Privacy-Handbuch

Spurenarm surfen mit Mozilla Firefox,
E-Mail mit Thunderbird,
chatten und verschlüsselt telefonieren,
Anonymisierungsdienste nutzen
und Daten verschlüsseln
für WINDOWS + Linux

7. April 2024

Inhaltsverzeichnis

Kapitel 1

Scroogled

Greg landete abends um acht auf dem internationalen Flughafen von San Francisco, doch bis er in der Schlange am Zoll ganz vorn ankam, war es nach Mitternacht. Er war der ersten Klasse nussbraun, unrasiert und drahtig entstiegen, nachdem er einen Monat am Strand von Cabo verbracht hatte, um drei Tage pro Woche zu tauchen und sich in der übrigen Zeit mit der Verführung französischer Studentinnen zu beschäftigen. Vor vier Wochen hatte er die Stadt als hängeschultriges, kullerbäuchiges Wrack verlassen. Nun war er ein bronzener Gott, der bewundernde Blicke der Stewardessen vorn in der Kabine auf sich zog.

Vier Stunden später war in der Schlange am Zoll aus dem Gott wieder ein Mensch geworden. Sein Elan war ermattet, Schweiß rann ihm bis hinunter zum Po, und Schultern und Nacken waren so verspannt, dass sein Rücken sich anfühlte wie ein Tennisschläger. Sein iPod-Akku hatte schon längst den Geist aufgegeben, sodass ihm keine andere Ablenkung blieb, als dem Gespräch des Pärchens mittleren Alters vor ihm zu lauschen.

„Die Wunder moderner Technik“, sagte die Frau mit Blick auf ein Schild in seiner Nähe: Einwanderung – mit Unterstützung von Google.

„Ich dachte, das sollte erst nächsten Monat losgehen?“ Der Mann setzte seinen Riesen-Sombrero immer wieder auf und ab.

Googeln an der Grenze – Allmächtiger. Greg hatte sich vor sechs Monaten von Google verabschiedet, nachdem er seine Aktienoptionen zu Barem gemacht hatte, um sich eine Auszeit zu gönnen, die dann allerdings nicht so befriedigend geworden war wie erhofft. Denn während der ersten fünf Monate hatte er kaum etwas anderes getan, als die Rechner seiner Freunde zu reparieren, tagsüber vorm Fernseher zu sitzen und zehn Pfund zuzunehmen –, was wohl darauf zurückzuführen gewesen war, dass er nun daheim herumgesessen war statt im Googleplex mit seinem gut ausgestatteten 24-Stunden-Fitnessclub.

Klar, er hätte es kommen sehen müssen. Die US-Regierung hatte 15 Milliarden Dollar daran verschwendet, Besucher an der Grenze zu fotografieren und ihre Fingerabdrücke zu nehmen –, und man hatte nicht einen einzigen Terroristen geschnappt. Augenscheinlich war die öffentliche Hand nicht in der Lage, richtig zu suchen.

Der DHS-Beamte hatte tiefe Ringe unter den Augen und blinzelte auf seinen Monitor, während er die Tastatur mit seinen Wurstfingern traktierte. Kein Wunder, dass es vier Stunden dauerte, aus dem verdammten Flughafen rauszukommen.

„n Abend“, sagte Greg und reichte dem Mann seinen schwitzigen Pass. Der Mann grunzte etwas und wischte ihn ab, dann starrte er auf den Bildschirm und tippte. Eine Menge. Ein kleiner Rest getrockneten Essens klebte ihm im Mundwinkel, und er bearbeitete ihn mit seiner Zunge.

„Möchten Sie mir was über Juni 1998 erzählen?“

Greg blickte vom Abflugplan hoch. „Pardon?“

„Sie haben am 17. Juni 1998 eine Nachricht auf alt.burningman über Ihre Absicht geschrieben, ein Festival zu besuchen. Und da fragten Sie: Sind Psychopilze wirklich so eine schlechte Idee?“

Der Interviewer im zweiten Befragungsraum war ein älterer Mann, nur Haut und Knochen, als sei er aus Holz geschnitzt. Seine Fragen gingen sehr viel tiefer als Psychopilze.

„Berichten Sie von Ihren Hobbys. Befassen Sie sich mit Raketenmodellen?“

„Womit?“

„Mit Raketenmodellen.“

„Nein“, sagte Greg, „überhaupt nicht“. Er ahnte, worauf das hinauslief.

Der Mann machte eine Notiz und klickte ein paarmal. „Ich frage nur, weil bei Ihren Suchanfragen und Ihrer Google-Mail ne Menge Werbung für Raketenzubehör auftaucht.“

Greg schluckte. „Sie blättern durch meine Suchanfragen und Mails?“ Er hatte nun seit einem Monat keine Tastatur mehr angefasst, aber er wusste: Was er in die Suchleiste eintippte, war wahrscheinlich aussagekräftiger als alles, was er seinem Psychiater erzählte.

„Sir, bleiben Sie bitte ruhig. Nein, ich schaue Ihre Suchanfragen nicht an“, sagte der Mann mit einem gespielten Seufzer. „Das wäre verfassungswidrig. Wir sehen nur, welche Anzeigen erscheinen, wenn Sie Ihre Mails lesen oder etwas suchen. Ich habe eine Broschüre, die das erklärt. Sie bekommen sie, sobald wir hier durch sind.“

„Aber die Anzeigen bedeuten nichts“, platzte Greg heraus. „Ich bekomme Anzeigen für Ann-Coulter-Klingeltöne, sooft ich eine Mail von meinem Freund in Coulter, Iowa, erhalte!“

Der Mann nickte. „Ich verstehe, Sir. Und genau deshalb spreche ich jetzt hier mit Ihnen. Können Sie sich erklären, weshalb bei Ihnen so häufig Modellraketen-Werbung erscheint?“

Greg grübelte. „Okay, probieren wir es mal. Suchen Sie nach coffee fanatics.“ Er war in der Gruppe mal ziemlich aktiv gewesen und hatte beim Aufbau der Website ihres Kaffee-des-Monats-Abodienstes geholfen. Die Bohnenmischung zum Start des Angebots hieß „Turbinen-Treibstoff“. Das plus „Start“, und schon würde Google ein paar Modellraketen-Anzeigen einblenden.

Die Sache schien gerade ausgestanden zu sein, als der geschnitzte Mann die Halloween-Fotos entdeckte – tief vergraben auf der dritten Seite der Suchergebnisse für Greg Lupinski.

„Es war eine Golfkriegs-Themenparty im Castro“, sagte er.

„Und Sie sind verkleidet als . . . ?“

„Selbstmordattentäter“, erwiderte er kläglich. Das Wort nur auszusprechen, verursachte ihm Übelkeit.

„Kommen Sie mit, Mr. Lupinski“, sagte der Mann.

Als er endlich gehen durfte, war es nach drei Uhr. Seine Koffer standen verloren am Gepäckkarussell. Er nahm sie und sah, dass sie geöffnet und nachlässig wieder geschlossen worden waren; hier und da lugten Kleidungsstücke heraus.

Daheim stellte er fest, dass all seine pseudopräkolumbianischen Statuen zerbrochen worden waren und dass mitten auf seinem brandneuen weißen mexikanischen Baumwollhemd ein ominöser Stiefelabdruck prangte. Seine Kleidung roch nun nicht mehr nach Mexiko – sie roch nach Flughafen.

An Schlaf war jetzt nicht mehr zu denken, er musste über die Sache reden. Es gab nur eine einzige Person, die all das begreifen würde. Zum Glück war sie normalerweise um diese Zeit noch wach.

Maya war zwei Jahre nach Greg zu Google gekommen. Sie war es, die ihn überzeugt hatte, nach dem Einlösen der Optionen nach Mexiko zu gehen: Wohin auch immer, hatte sie gesagt, solange er nur seinem Dasein einen Neustart verpasste.

Maya hatte zwei riesige schokobraune Labradore und eine überaus geduldige Freundin, Laurie, die mit allem einverstanden war, solange es nicht bedeutete, dass sie selbst morgens um sechs von 350 Pfund sabbernder Caniden durch Dolores Park geschleift wurde.

Maya griff nach ihrem Tränengas, als Greg auf sie zugelaufen kam; dann blickte sie ihn erstaunt an und breitete ihre Arme aus, während sie die Leinen fallen ließ und mit dem Schuh festhielt. „Wo ist der Rest von dir? Mann, siehst du heiß aus!“

Er erwiderte die Umarmung, plötzlich seines Aromas nach einer Nacht invasiven Googelns bewusst. „Maya“, sagte er, „was weißt du über Google und das DHS?“

Seine Frage ließ sie erstarren. Einer der Hunde begann zu jaulen. Sie blickte sich um, nickte dann hoch in Richtung der Tennisplätze. „Auf dem Laternenmast – nicht hinschauen“, sagte sie. „Da ist einer unserer lokalen Funknetz-Hotspots. Weitwinkel-Webcam. Guck in die andere Richtung, während du sprichst.“

Letztlich war es für Google gar nicht teuer gewesen, die Stadt mit Webcams zu überziehen – vor allem, wenn man bedachte, welche Möglichkeiten es bot, Menschen die passende Werbung zu ihrem jeweiligen Aufenthaltsort liefern zu können. Greg hatte seinerzeit kaum Notiz davon genommen, als die Kameras auf all den Hotspots ihren öffentlichen Betrieb aufgenommen hatten; es hatte einen Tag lang Aufruhr in der Blogosphäre gegeben, während die Leute mit dem neuen Allesseher zu spielen begonnen und an diverse Rotlichtviertel herangezoomt hatten, doch nach einer Weile war die Aufregung abgeebbt.

Greg kam sich albern vor, er murmelte: „Du machst Witze.“

„Komm mit“, erwiderte sie, nicht ohne sich dabei vom Laternenpfahl abzuwenden.

Die Hunde waren nicht einverstanden damit, den Spaziergang abzukürzen, und taten ihren Unmut in der Küche kund, wo Maya Kaffee zubereitete.

„Wir haben einen Kompromiss mit dem DHS ausgehandelt“, sagte sie und griff nach der Milch. „Sie haben sich damit einverstanden erklärt, nicht mehr unsere Suchprotokolle zu durchwühlen, und wir lassen sie im Gegenzug sehen, welcher Nutzer welche Anzeigen zu sehen bekommt.“

Greg fühlte sich elend. „Warum? Sag nicht, dass Yahoo es schon vorher gemacht hat . . . “

„N-nein. Doch, ja, sicher, Yahoo war schon dabei. Aber das war nicht der Grund für Google, mitzumachen. Du weißt doch, die Republikaner hassen Google. Wir sind größtenteils als Demokraten registriert, also tun wir unser Bestes, mit ihnen Frieden zu schließen, bevor sie anfangen, sich auf uns einzuschießen. Es geht ja auch nicht um P.I.I.“ – persönlich identifizierende Information, der toxische Smog der Informationsära – „sondern bloß um Metadaten. Also ist es bloß ein *bisschen* böse.“

„Warum dann all die Heimlichtuerei?“

Maya seufzte und umarmte den Labrador, dessen gewaltiger Kopf auf ihrem Knie ruhte. „Die Schlapphüte sind wie Läuse – die sind überall. Tauchen sogar in unseren Konferenzen auf, als wären wir in irgendeinem Sowjet-Ministerium. Und dann die Sicherheitseinstufungen – das spaltet uns in zwei Lager: solche mit Bescheinigung und solche ohne. Jeder von uns weiß, wer keine Freigabe hat, aber niemand weiß, warum. Ich bin als sicher eingestuft – zum Glück fällt man als

Lesbe nicht mehr gleich automatisch durch. Keine sichere Person würde sich herablassen, mit jemandem essen zu gehen, der keine Freigabe hat.“

Greg fühlte sich sehr müde. „Na, da kann ich von Glück reden, dass ich lebend aus dem Flughafen herausgekommen bin. Mit Pech wäre ich jetzt eine Vermisstenmeldung, was?“

Maya blickte ihn nachdenklich an. Er wartete auf eine Antwort.

„Was ist denn?“

„Ich werde dir jetzt was erzählen, aber du darfst es niemals weitergeben, o.k.?“

„Ähm, du bist nicht zufällig in einer terroristischen Vereinigung?“

„Wenn es so einfach wäre ... Die Sache ist die: Was das DHS am Flughafen treibt, ist eine Art Vorsortierung, die es den Schlapphüten erlaubt, ihre Suchkriterien enger zu fassen. Sobald du an der Grenze ins zweite Zimmerchen gebeten wirst, bist du *eine Person von Interesse* – und dann haben sie dich im Griff. Sie suchen über Webcams nach deinem Gesicht und Gang, lesen deine Mail, überwachen deine Suchanfragen.“

„Sagtest du nicht, die Gerichte würden das nicht erlauben?“

„Sie erlauben es nicht, jedermann undifferenziert auf blauen Dunst zu googeln. Aber sobald du im System bist, wird das eine selektive Suche. Alles legal. Und wenn sie dich erst mal googeln, finden sie garantiert irgendwas. Deine gesamten Daten werden auf *verdächtige Muster* abgegrast, und aus jeder Abweichung von der statistischen Norm drehen sie dir einen Strick.“

Greg fühlte Übelkeit in sich aufsteigen. „Wie zum Teufel konnte das passieren? Google war ein *guter* Ort. *Tu nichts Böses*, war da nicht was?“ Das war das Firmenmotto, und für Greg war es ein Hauptgrund dafür gewesen, seinen Stanford-Abschluss in Computerwissenschaften direkten Wegs nach Mountain View zu tragen.

Mayas Erwiderung war ein raues Lachen. *„Tu nichts Böses?* Ach komm, Greg. Unsere Lobbyistengruppe ist dieselbe Horde von Kryptofaschisten, die Kerry die Swift-Boat-Nummer anhängen wollte. Wir haben schon längst angefangen, vom Bösen zu naschen.“

Sie schwiegen eine Minute lang.

„Es ging in China los“, sagte sie schließlich. „Als wir unsere Server aufs Festland brachten, unterstellten wir sie damit chinesischem Recht.“

Greg seufzte. Er wusste nur zu gut um Googles Einfluss: Sooft man eine Webseite mit Google Ads besuchte, Google Maps oder Google Mail benutzte – ja sogar, wenn man nur Mail an einen Gmail-Nutzer sendete –, wurden diese Daten von der Firma penibel gesammelt. Neuerdings hatte Google sogar begonnen, die Suchseite auf Basis solcher Daten für die einzelnen Nutzer zu personalisieren. Dies hatte sich als revolutionäres Marketingwerkzeug erwiesen. Eine autoritäre Regierung würde damit andere Dinge anfangen wollen.

„Sie benutzten uns dazu, Profile von Menschen anzulegen“, fuhr sie fort. „Wenn sie jemanden einbuchten wollten, kamen sie zu uns und fanden einen Vorwand dafür. Schließlich gibt es kaum eine Aktivität im Internet, die in China nicht illegal ist.“

Greg schüttelte den Kopf. „Und warum mussten die Server in China stehen?“

„Die Regierung sagte, sie würde uns sonst blocken. Und Yahoo war schon da.“ Sie schnitten beide Grimassen. Irgendwann hatten die Google-Mitarbeiter eine Obsession für Yahoo entwickelt und sich mehr darum gekümmert, was die Konkurrenz trieb, als darum, wie es um das eigene Unternehmen stand. „Also taten wir es – obwohl viele von uns es nicht für eine gute Idee hielten.“

Maya schlürfte ihren Kaffee und senkte die Stimme. Einer ihrer Hunde schnupperte unablässig unter Gregs Stuhl.

„Die Chinesen forderten uns praktisch sofort auf, unsere Suchergebnisse zu zensieren“, sagte Maya. „Google kooperierte. Mit einer ziemlich bizarren Begründung: *Wir tun nichts Böses, sondern wir geben den Kunden Zugriff auf eine bessere Suchmaschine! Denn wenn wir ihnen Suchergebnisse präsentierten, die sie nicht aufrufen können, würde sie das doch nur frustrieren – das wäre ein mieses Nutzererlebnis.*“

„Und jetzt?“ Greg schubste einen Hund beiseite. Maya wirkte gekränkt.

„Jetzt bist du eine Person von Interesse, Greg. Du wirst googlebelauert. Du lebst jetzt ein Leben, in dem dir permanent jemand über die Schulter blickt. Denk an die Firmen-Mission: *Die Information der Welt organisieren.* Alles. Lass fünf Jahre ins Land gehen, und wir wissen, wie viele Haufen in der Schüssel waren, bevor du sie gespült hast. Nimm dazu die automatisierte Verdächtigung von jedem, der Übereinstimmungen mit dem statistischen Bild eines Schurken aufweist, und du bist . . . “

„. . . verraten und vergoogelt.“

„Voll und ganz“, nickte sie.

Maya brachte beide Labradors zum Schlafzimmer. Eine gedämpfte Diskussion mit ihrer Freundin war zu hören, dann kam sie allein zurück.

„Ich kann die Sache in Ordnung bringen“, presste sie flüsternd hervor. „Als die Chinesen mit den Verhaftungen anfingen, machten ein paar Kollegen und ich es zu unserem 20-Prozent-Projekt, ihnen in die Suppe zu spucken.“ (Eine von Googles unternehmerischen Innovationen war die Regel, dass alle Angestellten 20 Prozent ihrer Arbeitszeit in anspruchsvolle Projekte nach eigenem Gusto zu investieren hatten.) „Wir nennen es den Googleputzer. Er greift tief in die Datenbanken ein und normalisiert dich statistisch. Deine Suchanfragen, Gmail-Histogramme, Surfmuster. Alles. Greg, ich kann dich googleputzen. Eine andere Möglichkeit hast du nicht.“

„Ich will nicht, dass du meinetwegen Ärger bekommst.“

Sie schüttelte den Kopf. „Ich bin ohnehin schon geliefert. Jeder Tag, seit ich das verdammte Ding programmiert habe, ist geschenkte Zeit. Ich warte bloß noch drauf, dass jemand dem DHS meinen Background steckt, und dann . . . tja, ich weiß auch nicht. Was auch immer sie mit Menschen wie mir machen in ihrem Krieg gegen abstrakte Begriffe.“

Greg dachte an den Flughafen, an die Durchsuchung, an sein Hemd mit dem Stiefelabdruck.

„Tu es“, sagte er.

Der Googleputzer wirkte Wunder. Greg erkannte es daran, welche Anzeigen am Rand seiner Suchseiten erschienen, Anzeigen, die offensichtlich für jemand anderen gedacht waren. Fakten zum Intelligent Design, Abschluss im Online-Seminar, ein terrorfreies Morgen, Pornografieblocker, die homosexuelle Agenda, billige Toby-Keith-Tickets. Es war offensichtlich, dass Googles neue personalisierte Suche ihn für einen völlig anderen hielt: einen gottesfürchtigen Rechten mit einer Schwäche für Cowboy-Musik.

Nun gut, das sollte ihm recht sein.

Dann klickte er sein Adressbuch an und stellte fest, dass die Hälfte seiner Kontakte fehlte. Sein Gmail-Posteingang war wie von Termiten ausgehöhlt, sein Orkut-Profil normalisiert. Sein Kalender, Familienfotos, Lesezeichen: alles leer. Bis zu diesem Moment war ihm nicht klar gewesen, wie viel seiner selbst ins Web migriert war und seinen Platz in Googles Serverfarmen gefunden hatte – seine gesamte Online-Identität. Maya hatte ihn auf Hochglanz poliert; er war jetzt *Der Unsichtbare.*

Greg tippte schläfrig auf die Tastatur seines Laptops neben dem Bett und erweckte den Monitor zum Leben. Er blinzelte die Uhr in der Toolbar an. 4:13 Uhr morgens! Allmächtiger, wer hämmerte denn um diese Zeit gegen seine Tür?

Er rief mit nuscheliger Stimme „Komm ja schon“ und schlüpfte in Morgenmantel und Pantoffeln. Dann schlurfte er den Flur entlang und knipste unterwegs die Lichter an. Durch den Türspion blickte ihm düster Maya entgegen.

Er entfernte Kette und Riegel und öffnete die Tür. Maya huschte an ihm vorbei, gefolgt von den Hunden und ihrer Freundin. Sie war schweißüberströmt, ihr normalerweise gekämmtes Haar hing strähnig in die Stirn. Sie rieb sich die rot geränderten Augen.

„Pack deine Sachen“, stieß sie heiser hervor.

„Was?“

Sie packte ihn bei den Schultern. „Mach schon“, sagte sie.

„Wohin willst . . . “

„Mexiko wahrscheinlich. Weiß noch nicht. Nun pack schon, verdammt.“ Sie drängte sich an ihm vorbei ins Schlafzimmer und begann, Schubladen zu öffnen.

„Maya“, sagte er scharf, „ich gehe nirgendwohin, solange du mir nicht sagst, was los ist.“

Sie starrte ihn an und wischte ihre Haare aus dem Gesicht. „Der Googleputzer lebt. Nachdem ich dich gesäubert hatte, habe ich ihn runtergefahren und bin verschwunden. Zu riskant, ihn noch weiter zu benutzen. Aber er schickt mir Mailprotokolle, sooft er läuft. Und jemand hat ihn sechs Mal verwendet, um drei verschiedene Benutzerkonten zu schrubben – und die gehören zufällig alle Mitgliedern des Senats-Wirtschaftskomitees, die vor Neuwahlen stehen.“

„Googler frisieren die Profile von Senatoren?“

„Keine Google-Leute. Das kommt von außerhalb; die IP-Blöcke sind in D.C. registriert. Und alle IPs werden von Gmail-Nutzern verwendet. Rate mal, wem diese Konten gehören.“

„Du schnüffelst in Gmail-Konten?“

„Hm, ja. Ich habe durch ihre E-Mails geschaut. Jeder macht das mal, und mit weitaus übleren Motiven als ich. Aber stell dir vor, all diese Aktivität geht von unserer Lobbyistenfirma aus. Machen nur ihren Job, dienen den Interessen des Unternehmens.“

Greg fühlte das Blut in seinen Schläfen pulsieren. „Wir sollten es jemandem erzählen.“

„Das bringt nichts. Die wissen alles über uns. Sehen jede Suchanfrage, jede Mail, jedes Mal, wenn uns die Webcams erfassen. Wer zu unserem sozialen Netzwerk gehört . . . Wusstest du das? Wenn du 15 Orkut-Freunde hast, ist es statistisch gesehen sicher, dass du höchstens drei Schritte entfernt bist von jemandem, der schon mal Geld für *terroristische Zwecke* gespendet hat. Denk an den Flughafen – das war erst der Anfang für dich.“

„Maya“, sagte Greg, der nun seine Fassung wiedergewann, „übertreibst du es nicht mit Mexiko? Du könntest doch kündigen, und wir ziehen ein Start-up auf. Aber das ist doch bescheuert.“

„Sie kamen heute zu Besuch“, entgegnete sie. „Zwei politische Beamte vom DHS. Blieben stundenlang und stellten eine Menge verdammt harter Fragen.“

„Über den Googleputzer?“

„Über meine Freunde und Familie. Meine Such-Geschichte. Meine persönliche Geschichte.“

„Jesus.“

„Das war eine Botschaft für mich. Die beobachten mich – jeden Klick, jede Suche. Zeit zu verschwinden, jedenfalls aus ihrer Reichweite.“

„In Mexiko gibt es auch eine Google-Niederlassung.“

„Wir müssen jetzt los“, beharrte sie.

„Laurie, was hältst du davon?“, fragte Greg.

Laurie stupste die Hunde zwischen die Schultern. „Meine Eltern sind ?65 aus Ostdeutschland weggegangen. Sie haben mir immer von der Stasi erzählt. Die Geheimpolizei hat alles über dich in deiner Akte gesammelt: ob du vaterlandsfeindliche Witze erzählst, all so?n Zeug. Ob sie es nun wollten oder nicht, Google hat inzwischen das Gleiche aufgezogen.“

„Greg, kommst du nun?“

Er blickte die Hunde an und schüttelte den Kopf. „Ich habe ein paar Pesos übrig“, sagte er. „Nehmt sie mit. Und passt auf euch auf, ja?“

Maya zog ein Gesicht, als wolle sie ihm eine runterhauen. Dann entspannte sie sich und umarmte ihn heftig.

„Pass du auf dich auf“, flüsterte sie ihm ins Ohr.

Eine Woche später kamen sie zu ihm. Nach Hause, mitten in der Nacht, genau wie er es sich vorgestellt hatte. Es war kurz nach zwei Uhr morgens, als zwei Männer vor seiner Tür standen.

Einer blieb schweigend dort stehen. Der andere war ein Lächler, klein und faltig, mit einem Fleck auf dem einen Mantelrevers und einer amerikanischen Flagge auf dem anderen. „Greg Lupinski, es besteht der begründete Verdacht, dass Sie gegen das Gesetz über Computerbetrug und -missbrauch verstoßen haben“, sagte er, ohne sich vorzustellen. „Insbesondere, dass Sie Bereiche autorisierten Zugangs überschritten und sich dadurch Informationen verschafft haben. Zehn Jahre für Ersttäter. Außerdem gilt das, was Sie und Ihre Freundin mit Ihren Google-Daten gemacht haben, als schweres Verbrechen. Und was dann noch in der Verhandlung zutage kommen wird . . . angefangen mit all den Dingen, um die Sie Ihr Profil bereinigt haben.“

Greg hatte diese Szene eine Woche lang im Geist durchgespielt, und er hatte sich allerlei mutige Dinge zurechtgelegt, die er hatte sagen wollen. Es war eine willkommene Beschäftigung gewesen, während er auf Mayas Anruf gewartet hatte. Der Anruf war nie gekommen.

„Ich möchte einen Anwalt sprechen“, war alles, was er herausbrachte.

„Das können Sie tun“, sagte der kleine Mann. „Aber vielleicht können wir zu einer besseren Einigung kommen.“

Greg fand seine Stimme wieder. „Darf ich mal Ihre Marke sehen?“

Das Basset-Gesicht des Mannes hellte sich kurz auf, als er ein amüsiertes Glucksen unterdrückte. „Kumpel, ich bin kein Bulle“, entgegnete er. „Ich bin Berater. Google beschäftigt mich – meine Firma vertritt ihre Interessen in Washington –, um Beziehungen aufzubauen. Selbstverständlich würden wir niemals die Polizei hinzuziehen, ohne zuerst mit Ihnen zu sprechen. Genau genommen möchte ich Ihnen ein Angebot unterbreiten.“

Greg wandte sich der Kaffeemaschine zu und entsorgte den alten Filter.

„Ich gehe zur Presse“, sagte er.

Der Mann nickte, als ob er darüber nachdenken müsse. „Na klar. Sie gehen eines Morgens zum Chronicle und breiten alles aus. Dort sucht man nach einer Quelle, die Ihre Story stützt; man wird aber keine finden. Und wenn sie danach suchen, werden wir sie finden. Also lassen Sie mich doch erst mal ausreden, Kumpel. Ich bin im Win-Win-Geschäft, und ich bin sehr gut darin.“

Er pausierte. „Sie haben da übrigens hervorragende Bohnen, aber wollen Sie sie nicht erst eine Weile wässern? Dann sind sie nicht mehr so bitter, und die Öle kommen besser zur Geltung. Reichen Sie mir mal ein Sieb?“

Greg beobachtete den Mann dabei, wie er schweigend seinen Mantel auszog und über den Küchenstuhl hängte, die Manschetten öffnete, die Ärmel sorgfältig hochrollte und eine billige Digitaluhr in die Tasche steckte. Er kippte die Bohnen aus der Mühle in Gregs Sieb und wässerte sie in der Spüle.

Er war ein wenig untersetzt und sehr bleich, mit all der sozialen Anmut eines Elektroingenieurs. Wie ein echter Googler auf seine Art, besessen von Kleinigkeiten. Mit Kaffeemühlen kannte er sich also auch aus.

„Wir stellen ein Team für Haus 49 zusammen . . . "

„Es gibt kein Haus 49", sagte Greg automatisch.

„Schon klar", entgegnete der andere mit verkniffenem Lächeln. „Es gibt kein Haus 49. Aber wir bauen ein Team auf, das den Googleputzer überarbeiten soll. Mayas Code ist nicht sonderlich schlank und steckt voller Fehler. Wir brauchen ein Upgrade. Sie wären der Richtige; und was Sie wissen, würde keine Rolle spielen, wenn Sie wieder an Bord sind."

„Unglaublich", sagte Greg spöttisch. „Wenn Sie denken, dass ich Ihnen helfe, im Austausch für Gefälligkeiten politische Kandidaten anzuschwärzen, sind Sie noch wahnsinniger, als ich dachte."

„Greg", sagte der Mann, „niemand wird angeschwärzt. Wir machen nur ein paar Dinge sauber. Für ausgewählte Leute. Sie verstehen mich doch? Genauer betrachtet gibt jedes Google-Profil Anlass zur Sorge. Und genaue Betrachtung ist der Tagesbefehl in der Politik. Eine Bewerbung um ein Amt ist wie eine öffentliche Darmspiegelung." Er befüllte die Kaffeemaschine und drückte mit vor Konzentration verzerrtem Gesicht den Kolben nieder. Greg holte zwei Kaffeetassen (Google-Becher natürlich) und reichte sie weiter.

„Wir tun für unsere Freunde das Gleiche, was Maya für Sie getan hat. Nur ein wenig aufräumen. Nur ihre Privatsphäre schützen – mehr nicht."

Greg nippte am Kaffee. „Was geschieht mit den Kandidaten, die Sie nicht putzen?"

„Na ja", sagte Gregs Gegenüber mit dünnem Grinsen, „tja, Sie haben Recht, für die wird es ein bisschen schwierig." Er kramte in der Innentasche seines Mantels und zog einige gefaltete Blätter Papier hervor, strich sie glatt und legte sie auf den Tisch. „Hier ist einer der Guten, der unsere Hilfe braucht." Es war das ausgedruckte Suchprotokoll eines Kandidaten, dessen Kampagne Greg während der letzten drei Wahlen unterstützt hatte.

„Der Typ kommt also nach einem brutalen Wahlkampf-Tag voller Klinkenputzen ins Hotel, fährt den Laptop hoch und tippt *knackige Ärsche* in die Suchleiste. Ist doch kein Drama, oder? Wir sehen es so: Wenn man wegen so was einen guten Mann daran hindert, weiterhin seinem Land zu dienen, wäre das schlichtweg unamerikanisch."

Greg nickte langsam.

„Sie werden ihm also helfen?", fragte der Mann.

„Ja."

„Gut. Da wäre dann noch was: Sie müssen uns helfen, Maya zu finden. Sie hat überhaupt nicht verstanden, worum es uns geht, und jetzt scheint sie sich verdrückt zu haben. Wenn sie uns bloß mal zuhört, kommt sie bestimmt wieder rum."

Er betrachtete das Suchprofil des Kandidaten.

„Denke ich auch", erwiderte Greg.

Der neue Kongress benötigte elf Tage, um das Gesetz zur Sicherung und Erfassung von Amerikas Kommunikation und Hypertext zu verabschieden. Es erlaubte dem DHS und der NSA, bis zu 80

Prozent der Aufklärungs- und Analysearbeit an Fremdfirmen auszulagern. Theoretisch wurden die Aufträge über offene Bietverfahren vergeben, aber in den sicheren Mauern von Googles Haus 49 zweifelte niemand daran, wer den Zuschlag erhalten würde. Wenn Google 15 Milliarden Dollar für ein Programm ausgegeben hätte, Übeltäter an den Grenzen abzufangen, dann hätte es sie garantiert erwischt – Regierungen sind einfach nicht in der Lage, richtig zu suchen.

Am Morgen darauf betrachtete Greg sich prüfend im Rasierspiegel (das Wachpersonal mochte keine Hacker-Stoppelbärte und hatte auch keine Hemmungen, das deutlich zu sagen), als ihm klar wurde, dass heute sein erster Arbeitstag als De-facto-Agent der US-Regierung begann. Wie schlimm mochte es werden? Und war es nicht besser, dass Google die Sache machte, als irgendein ungeschickter DHS-Schreibtischtäter?

Als er am Googleplex zwischen all den Hybridautos und überquellenden Fahrradständern parkte, hatte er sich selbst überzeugt. Während er sich noch fragte, welche Sorte Bio-Fruchtshake er heute in der Kantine bestellen würde, verweigerte seine Codekarte den Zugang zu Haus 49. Die rote LED blinkte immer nur blöde vor sich hin, wenn er seine Karte durchzog. In jedem anderen Gebäude würde immer mal jemand raus- und wieder reinkommen, dem man sich anschließen könnte. Aber die Googler in 49 kamen höchstens zum Essen raus, und manchmal nicht einmal dann.

Ziehen, ziehen, ziehen. Plötzlich hörte er eine Stimme neben sich.

„Greg, kann ich Sie bitte sprechen?“

Der verschrumpelte Mann legte einen Arm um seine Schulter, und Greg atmete den Duft seines Zitrus-Rasierwassers ein. So hatte sein Tauchlehrer in Baja geduftet, wenn sie abends durch die Kneipen gezogen waren. Greg konnte sich nicht an seinen Namen erinnern: Juan Carlos? Juan Luis?

Der Mann hielt seine Schulter fest im Griff, lotste ihn weg von der Tür, über den tadellos getrimmten Rasen und vorbei am Kräutergarten vor der Küche. „Wir geben Ihnen ein paar Tage frei“, sagte er.

Greg durchschoss eine Panikattacke. „Warum?“ Hatte er irgendetwas falsch gemacht? Würden sie ihn einbuchten?

„Es ist wegen Maya.“ Der Mann drehte ihn zu sich und begegnete ihm mit einem Blick endloser Tiefe. „Sie hat sich umgebracht. In Guatemala. Es tut mir Leid, Greg.“

Greg spürte, wie der Boden unter seinen Füßen verschwand und wie er meilenweit emporgezogen wurde. In einer Google-Earth-Ansicht des Googleplex sah er sich und den verschrumpelten Mann als Punktepaar, zwei Pixel, winzig und belanglos. Er wünschte, er könnte sich die Haare ausreißen, auf die Knie fallen und weinen.

Von weit, weit weg hörte er sich sagen: „Ich brauche keine Auszeit. Ich bin okay.“

Von weit, weit weg hörte er den verschrumpelten Mann darauf bestehen.

Die Diskussion dauerte eine ganze Weile, dann gingen die beiden Pixel in Haus 49 hinein, und die Tür schloss sich hinter ihnen.

Ich danke dem Autor Cory Doctorow und dem Übersetzer Christian Wöhrl dafür, dass sie den Text unter einer Creative-Commons-Lizenz zur Nutzung durch Dritte bereitstellen.

Kapitel 2

Angriffe auf die Privatsphäre

Im realen Leben ist Anonymität die tagtäglich erlebte Erfahrung. Wir gehen eine Straße entlang, kaufen eine Zeitung, ohne uns ausweisen zu müssen, beim Lesen der Zeitung schaut uns niemand zu. Das Aufgeben von Anonymität (z. B. mit Rabattkarten) ist eine aktive Entscheidung.

Im Internet ist es umgekehrt. Von jedem Nutzer werden Profile erstellt. Webseitenbetreiber sammeln Informationen (Surfverhalten, E-Mail-Adressen), um mit dem Verkauf der gesammelten Daten ihr Angebot zu finanzieren. Betreiber von Werbe-Servern nutzen die Möglichkeiten, das Surfverhalten Webseiten-übergreifend zu erfassen.

Verglichen mit dem Beispiel *Zeitunglesen* läuft es auf dem Datenhighway so, dass uns Zeitungen in großer Zahl kostenlos aufgedrängt werden. Beim Lesen schaut uns ständig jemand über die Schulter, um unser Interessen- und Persönlichkeitsprofil für die Einblendung passender Werbung zu analysieren oder um es zu verkaufen (z. B. an zukünftige Arbeitgeber). Außerdem werden unsere Kontakte zu Freunden ausgewertet, Kommunikation wird gescannt, Geheimdienste sammeln kompromittierendes Material usw.

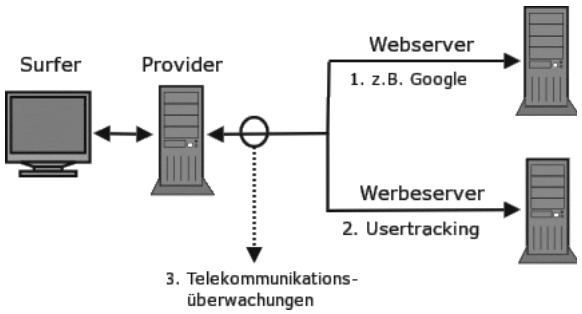


Abbildung 2.1: Möglichkeiten zur Überwachung im WWW

Neben den Big-Data-Firmen werden auch staatliche Maßnahmen zur Überwachung immer weiter ausgebaut und müssen von Internet-Providern unterstützt werden. Nicht immer sind die vorgesehenen Maßnahmen rechtlich unbedenklich.

> *Eine zukünftige Regierung könnte eine technische Infrastruktur erben, die für Zwecke der Überwachung bestens geeignet ist. Sie kann Bewegungen der politischen Gegner, jede finanzielle Transaktion, jede Kommunikation, jede einzelne E-Mail, jedes Telefongespräch überwachen. Alle Mitteilungen könnten gefiltert und gescannt, automatisch zugeordnet und protokolliert werden. Es ist an der Zeit, dass die Kryptografie von uns allen genutzt wird.* P. Zimmermann (Entwickler von PGP, ZRTP und Blackphone)

Das hier zur Verfügung gestellte Privacy Handbuch wendet sich primär an private Nutzer, die sich etwas tiefer mit dem Thema befassen wollen. Eine Erweiterung auf Firmen würde einerseits den Themenumfang endlos ausdehnen und anderseits können Firmen professionelle IT Fachleute einstellen, die die nötige Kompetenz mitbringen und im Rahmen von Weiterbildungen entwickeln.

2.1 Big Data – Kunde ist der, der bezahlt

Viele Nutzer dieser Dienste sehen sich in der Rolle von *Kunden*. Das ist falsch. Kunde ist der, der bezahlt. Kommerzielle Unternehmen (insbesondere börsennotierte Unternehmen) optimieren ihre Webangebote, um den zahlenden Kunden zu gefallen und den Gewinn zu maximieren. Die vielen Freibier-Nutzer sind bestenfalls *glückliche Hamster im Laufrad*, die die verkaufte Ware produzieren.

2.1.1 Google

Das Beispiel Google wurde aufgrund der Bekanntheit gewählt. Auch andere Firmen gehören zu den Big Data Companies und versuchen, mit ähnlichen Geschäftsmodellen Gewinne zu erzielen. Im Gegensatz zu Facebook, Twitter usw. verkauft Google die gesammelten Informationen über Nutzer nicht an Dritte, sondern verwendet sie intern für die Optimierung der Werbung. Nur an die NSA werden nach Informationen des Whistleblowers W. Binney zukünftig Daten weitergegeben.

Wirtschaftliche Zahlen

Google hat einen jährlichen Umsatz von 37 Mrd. Dollar, der ca. 9,4 Mrd. Dollar Gewinn abwirft. 90 % des Umsatzes erzielt Google mit personalisierter Werbung. Die Infrastruktur kostet ca. 2 Mrd. Dollar jährlich. (Stand: 2011) Im Jahr 2017 betrug der Umsatz fast 80 Mrd. Dollar.

Google Web Search

Googles Websuche ist in Deutschland die Nummer Eins. 89 % der Suchanfragen gehen direkt an *google.de*. Mit den Diensten wie Ixquick, Metager2 oder Web.de, die indirekt Anfragen an Google weiterleiten, beantwortet der Primus ca. 95 % der deutschen Suchanfragen (2008).

1. Laut Einschätzung der Electronic Frontier Foundation werden alle Suchanfragen protokolliert und die meisten durch Cookies, IP-Adressen und Informationen von Google-Accounts einzelnen Nutzern zugeordnet.

   In den Datenschutzbestimmungen von Google kann man nachlesen, dass diese Informationen (in anonymisierter Form) auch an Dritte weitergegeben werden. Eine Einwilligung der Nutzer in die Datenweitergabe liegt nach Ansicht der Verantwortlichen vor, da mit der Nutzung des Dienstes auch die AGBs akzeptiert wurden. Sie sind schließlich auf der Website öffentlich einsehbar.

2. Nicht nur die Daten der Nutzer werden analysiert. Jede Suchanfrage und die Reaktionen auf die angezeigten Ergebnisse werden protokolliert und ausgewertet.

   Google Flu Trends zeigte, wie gut diese Analyse der Suchanfragen arbeitet. Anhand der Such-Protokolle wird eine Ausbreitung der Grippe um 1–2 Wochen schneller erkannt, als es bisher dem U.S. Center for Disease Control and Prevention möglich war.

   Die mathematischen Grundlagen für diese Analysen wurden im Rahmen der Bewertung von Googles 20 %-Projekten entwickelt. Bis 2008 konnten Entwickler bei Google 20 % ihrer Arbeitszeit für eigene Ideen verwenden. Interessante Ansätze aus diesem Umfeld gingen als Beta-Version online (z. B. Orkut). Die Reaktionen der Surfer auf diese Angebote wurde genau beobachtet. Projekte wurden wieder abgeschaltet, wenn sie die harten Erfolgskriterien nicht erfüllten (z. B. Google Video).

Inzwischen hat Google die 20%-Klausel abgeschafft. Die Kreativität der eigenen Mitarbeiter ist nicht mehr notwendig und zu teuer. Diese Änderung der Firmenpolitik wird von einer Fluktuation des Personals begleitet. 30 % des kreativen Stammpersonals von 2000 haben der Firma inzwischen den Rücken zugekehrt (Stand 2008).

Die entwickelten Bewertungsverfahren werden zur Beobachtung der Trends im Web eingesetzt. Der Primus unter den Suchmaschinen ist damit in der Lage, erfolgversprechende Ideen und Angebote schneller als andere Mitbewerber zu erkennen und darauf zu reagieren. Die Ideen werden nicht mehr selbst entwickelt, sondern aufgekauft und in das Imperium integriert. Seit 2004 wurden 60 Firmen übernommen, welche zuvor die Basis für die meisten aktuellen Angebote von Google entwickelt hatten: YouTube, Google Docs, Google Maps, Google Earth, Google Analytics, Picasa, SketchUp, die Blogger-Plattformen u. v. m.

Das weitere Wachstum des Imperiums scheint langfristig gesichert.

Zu spät hat die Konkurrenz erkannt, welches enorme Potenzial die Auswertung von Suchanfragen darstellt. Mit dem Börsengang 2004 musste Google seine Geheimniskrämerei etwas lockern und für die Börsenaufsicht Geschäftsdaten veröffentlichen. Microsoft hat daraufhin Milliarden Dollar in *MSN Live Search, Bing* versenkt und Amazon, ein weiterer Global-Player im Web, der verniedlichend als Online-Buchhändler bezeichnet wird, versuchte mit *A9*, auch eine Suchmaschine zu etablieren.

Adsense, DoubleClick, Analytics & Co.

Werbung ist die Haupteinnahmequelle von Google. Im dritten Quartal 2010 erwirtschaftete Google 7,3 Milliarden Dollar und damit 97 % der Einnahmen aus Werbung. Zielgenaue Werbung basierend auf umfassenden Informationen über Surfer bringt wesentlich höhere Einkünfte als einfache Bannerschaltung. Deshalb sammeln Werbetreibende im Netz umfangreiche Daten über Surfer. Es wird beispielsweise verfolgt, welche Webseiten ein Surfer besucht, und daraus ein Interessenprofil abgeleitet. Die Browser werden mit geeigneten Mitteln markiert (Cookies u. Ä.), um Nutzer leichter wiederzuerkennen.

Inzwischen lehnen 84 % der Internetnutzer dieses Behavioral Tracking ab. Von den Unternehmen im Internet wird es aber stetig ausgebaut. Google ist auf diesem Gebiet führend und wird dabei (unwissentlich?) von vielen Website-Betreibern unterstützt.

97 % der TOP100-Websites und ca. 80 % der deutschsprachigen Webangebote sind mit verschiedenen Elementen von Google für die Einblendung kontextsensitiver Werbung und Traffic-Analyse infiziert.[1] Jeder Aufruf einer derart präparierten Website wird bei Google registriert, ausgewertet und einem Surfer zugeordnet. Neben kommerziellen Verkaufswebsites, Informationsangeboten professioneller Journalisten und Online-Redaktionen gehören die Websites politischer Parteien genauso dazu wie unabhängige Blogger auf den Plattformen *blogger.com* und *blogspot.com* sowie private Websites, die sich über ein paar Groschen aus dem Adsense-Werbeprogramm freuen.

Untragbar wird diese Datenspionage, wenn politische Parteien wie die CSU ihre Spender überwachen lassen. Die CSU bietet ausschließlich die Möglichkeit, via Paypal zu spenden. Die Daten stehen damit inklusive Wohnanschrift und Kontonummer einem amerikanischen Großunternehmen zur Verfügung. Außerdem lässt die CSU ihre Spender mit Google-Analytics beobachten. Der Datenkrake erhält damit eindeutige Informationen über politische Anschauungen. Diese Details können im Informationskrieg wichtig sein.

Damit kennt das Imperium nicht nur den Inhalt der Websites, die vom Google-Bot für den Index der Suchmaschine abgeklappert wurden. Auch Traffic und Besucher der meisten Websites sind bekannt. Diese Daten werden Werbetreibenden anonymisiert zur Verfügung gestellt.

[1] Lars Reppesgaard, Das Google Imperium, (2008)

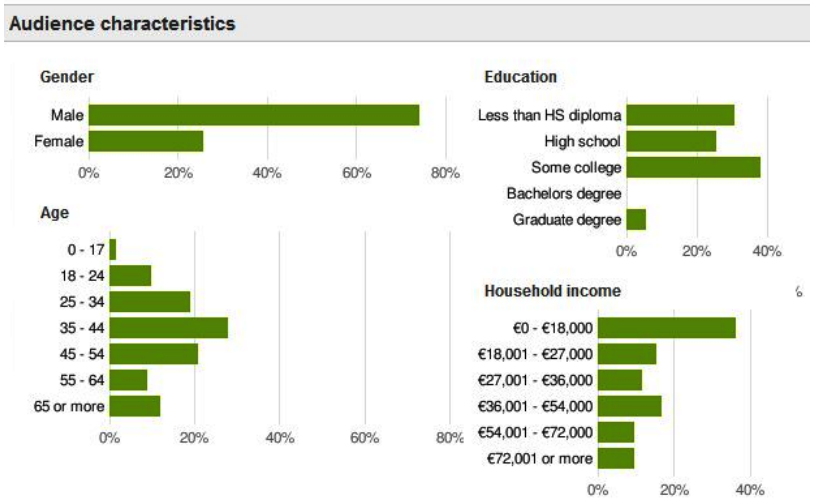


Abbildung 2.2: Ad-Planner-Besucherstatistik (Beispiel)

Die Grafik in Abb. 2.2 zur Besucherstatistik wurde vom Google Ad-Planner für eine (hier nicht genannte) Website erstellt. Man erkennt, dass der überwiegende Anteil der Besucher männlich und zwischen 35 und 44 Jahren alt ist. Die Informationen zu Bildung und Haushaltseinkommen müssen im Vergleich zu allgemeinen Statistiken der Bevölkerung bewertet werden, was hier mal entfällt.

Wie kommt das Imperium zu diesen Daten? Es gibt so gut wie keine Möglichkeit, diese Daten irgendwo einzugeben. Google fragt NICHT nach diesen Daten, sie werden in erster Linie aus der Analyse des Surf- und Suchverhaltens gewonnen. Zusätzlich kauft Google bei Marktforschungsunternehmen große Mengen an Informationen, die in die Kalkulation einfließen.

Wenn jemand mit dem iPhone auf der Website von BMW die Preise von Neuwagen studiert, kann Google diese Person einer Einkommensgruppe zuordnen. Wird der Surfer später beim Besuch von Spiegel-Online durch Einblendung von Werbung wiedererkannt, kommt ein entsprechender Vermerk in die Datenbank. Außerdem kann die Werbung passend zu seinen Interessen und Finanzen präsentiert werden. Die Realität ist natürlich etwas komplexer.

Mit dem im April 2010 eingeführtem **Retargeting** geht Google noch weiter. Mit Hilfe spezieller Cookies werden detaillierte Informationen über Surfer gesammelt. Die Informationen sollen sehr genau sein, bis hin zu Bekleidungsgrößen, für die man sich in einem Webshop interessiert hat. Die gesammelten Informationen sollen die Basis für punktgenaue Werbung bieten. Beispielsweise soll nach dem Besuch eines Webshops für Bekleidung ohne Kaufabschluss permanent alternative Werbung zu diesem Thema eingeblendet werden.

Google Attribution

Der Dienst *Google Attribution* wurde im Frühjahr 2017 gestartet. Mit diesem Dienst möchte Google Werbetreibenden Informationen liefern, wie sich personalisierte Online-Werbekampagnen auf Einkäufe in der realen Welt auswirken.

Basis für diese Auswertung sind neben den Daten aus dem Surfverhalten usw. auch Daten aus der realen Welt. Die 2014 eingeführte *Ladenbesuchsmessung* wird genutzt und Informationen aus Kreditkartenzahlungen werden einbezogen.

- Die *Ladenbesuchsmessung* basiert auf der genauen Lokalisierung von Android-Smartphones und liefert Informationen, welche Geschäfte der Besitzer eines Smartphones besucht.
- Durch Partnerschaften hat Google in den USA Zugriff auf 70 % der Kreditkartenzahlungen. Für Europa sind ähnliche Partnerschaften in Vorbereitung.
- Außerdem wird viel Voodoo Magic (KI) für die Auswertung genutzt.

Google hat errechnet, dass Kunden beim Besuch eines Geschäftes in der realen Welt mit 25 % höherer Wahrscheinlichkeit etwas kaufen und 10 % mehr ausgeben, wenn sie zuvor Online-Werbung zu dessen Angebot gesehen haben.

Google Mail, Talk, News usw. und Google+ (personalisierte Dienste)

Mit einem einheitlichem Google-Konto können verschiedene personalisierte Angebote genutzt werden. (Google Mail, News, Talk, Calendar, Alert, YouTube, Börsennachrichten usw.)

Bei der Anmeldung ist das Imperium weniger wissbegierig als vergleichbare kommerzielle Anbieter. Vor- und Nachname, Login-Name und Passwort reichen aus. Es ist nicht unbedingt nötig, seinen realen Namen anzugeben. Auch ein Pseudonym wird akzeptiert. Die Accounts ermöglichen es, aus dem Surf- und Suchverhalten, den zusammengestellten Nachrichtenquellen, dem Inhalt der E-Mails usw. ein Profil zu erstellen. Die unsichere Zuordnung über Cookies, IP-Adressen und andere Merkmale ist nicht nötig. Außerdem dienen die Dienste als Flächen für personalisierte und gut bezahlte Werbung.

Patente aus dem Umfeld von Google Mail zeigen, dass dabei nicht nur Profile über die Inhaber der Accounts erstellt werden, sondern auch die Kommunikationspartner unter die Lupe genommen werden. Wer an einen Google-Mail-Account eine E-Mail sendet, landet in der Falle des Datenkraken.

Die Einrichtung eines Google-Accounts ermöglicht es aber auch, gezielt die gesammelten Daten in gewissem Umfang zu beeinflussen. Man kann Einträge aus der Such- und Surf-Historie löschen u. Ä. (Besser ist es sicher, die Einträge von vornherein zu vermeiden.)

Smartphones und Android

2005 hat Google die Firma Android Inc. für 50 Mio. Dollar gekauft und sucht mit dem Smartphone-Betriebssystem Android auf dem Markt der mobilen Kommunikation ähnliche Erfolge wie im Web.

Bei der Nutzung von Android-Smartphones sollen alle E-Mails über Google Mail laufen, Termine mit dem Google Calendar abgeglichen werden, die Kontaktdaten sollen bei Google landen usw. Die Standortdaten werden ständig an Google übertragen, um sogenannte Mehrwertdienste bereitzustellen (genau wie das iPhone die Standortdaten an Apple sendet). Smartphones sind als Lifestyle-Gadget getarnte Tracking-Devices.

> *Wir wissen, wo du bist. Wir wissen, wo du warst. Wir können mehr oder weniger wissen, was du gerade denkst.* (Google-Chef Eric Schmidt, 2010)

Mozilla Firefox

Google ist der Hauptsponsor der Firefox-Entwickler. Seit 2012 zahlt Google jährlich 300 Mio. Dollar an die Mozilla Foundation, um die voreingestellte Standardsuchmaschine in diesem Browser zu sein. Das ist natürlich in erster Linie ein Angriff auf Microsoft. Die Entwickler von Firefox kommen ihrem Daten sammelnden Hauptsponsor jedoch in vielen Punkten deutlich entgegen:

- Die Default-Startseite ermöglicht es Google, ein langlebiges Cookie im First-Party-Context zu setzen und den Browser damit praktisch zu personalisieren. Die standardmäßig aktive Richtlinie für Cookies ermöglicht es Google exklusiv, auch als Drittseite das Surfverhalten zu verfolgen, da mit dem Start ein Cookie vorhanden ist.
- Sollte die Startseite modifiziert worden sein, erfolgt die „Personalisierung“ des Browsers wenige Minuten später durch Aktualisierung der Phishing-Datenbank.
- Diese „Personalisierung“ ermöglicht es Google, den Nutzer auf allen Webseiten zu erkennen, die mit Werbeanzeigen aus dem Imperium oder Google-Analytics verschmutzt sind. Im deutschsprachigen Web hat sich diese Verschmutzung auf 4/5 der relevanten Webseiten ausgebreitet.

(Trotzdem ist Mozilla Firefox ein guter Browser. Mit wenigen Anpassungen und Erweiterungen von unabhängigen Entwicklern kann man ihm die Macken austreiben und spurenarm durchs Web surfen.)

Google DNS

Mit dem DNS-Service versucht Google, die Digital Natives zu erreichen. Der Service spricht Nerds an, die in der Lage sind, Cookies zu blockieren, Werbung auszublenden und die natürlich einen DNS-Server konfigurieren können.

Google verspricht, dass die DNS-Server unter den IP-Adressen 8.8.8.8 und 8.8.4.4 nicht kompromittiert oder zensiert werden, und bemüht sich erfolgreich um schnelle DNS-Antworten. Die Google-Server sind etwa 1/10 bis 1/100 Sekunden schneller als andere unzensierte DNS-Server.

Natürlich werden alle Anfragen gespeichert und ausgewertet. Ziel ist es, die von erfahrenen Nutzern besuchten Websites zu erfassen und in das Monitoring des Web besser einzubeziehen. Positiv an dieser Initiative ist, dass es sich kaum jemand leisten kann, die Wirtschaftsmacht Google zu blockieren. Damit wird auch die Sperrung alternativer DNS-Server, wie es in Deutschland im Rahmen der Einführung der Zensur geplant war, etwas erschwert.

Kooperation mit Geheimdiensten (NSA, CIA)

Es wäre verwunderlich, wenn die gesammelten Datenbestände nicht das Interesse der Geheimdienste wecken würden. Das EPIC bemühte sich jahrelang auf Basis des Freedom of Information Act, Licht in diese Kooperation zu bringen. Die Anfragen wurden nicht beantwortet.[2]

Erst durch die von Snowden/Greenwald veröffentlichten Dokumente wurde mehr bekannt. Google ist seit 2009 einer der ersten PRISM-Partner der NSA. Das bedeutet, dass der US-Geheimdienst vollen Zugriff auf die Daten der Nutzer hat. Von allen auf der Folie genannten PRISM-Firmen wurden über-spezifische Dementis veröffentlicht, dass sie nie von einem Programm mit dem Namen

[2] https://epic.org/2010/09/epic-files-suit-for-documents.html

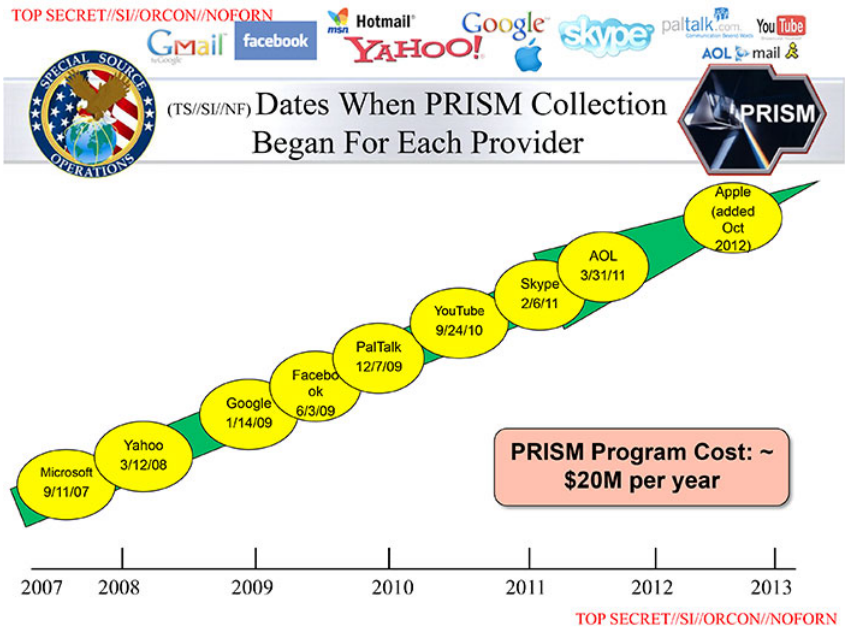


Abbildung 2.3: NSA-Folie zu den PRISM-Partnern

PRISM gehört hätten und demzufolge nicht wissentlich mit der NSA im Rahmen von PRISM kooperieren würden. Rajesh De, Leiter der Rechtsabteilung der NSA, dementierte die Dementis[3] und stellte klar, dass die Internetfirmen zwar den intern verwendetet Namen PRISM nicht kannten, dass die Datensammlung aber mit *voller Kenntnis und Unterstützung* der Unternehmen erfolgte.

Das Dementi von Google ist außerdem aufgrund der Informationen des Whistleblowers W. Binney unglaubwürdig. W. Binney war 30 Jahre in führenden Positionen der NSA tätig und veröffentlichte 2012, dass Google Kopien des gesamten E-Mail-Verkehrs von GMail und sämtliche Suchanfragen dem neuen Datacenter der NSA in Bluffdale zur Verfügung stellen wird:

> *It will store all Google search queries, e-mail and fax traffic.*

Wenn Googles Verwaltungsratschef Eric Schmidt auf der SXSW-Konferenz 2014 behauptet, durch Einführung der SSL-Verschlüsselung zwischen Datacentern seien die Daten der Google-Nutzer jetzt vor der NSA sicher[4], dann kann man dies als PR-Gag abtun. Google ist aufgrund geltender Gesetze zur Kooperation mit den weitreichenden Späh-Programmen der NSA verpflichtet.

Außerdem kooperiert Google mit der CIA bei der Auswertung der Datenbestände im Rahmen des Projekts Future of Web Monitoring, um Trends zu erkennen und für die Geheimdienste der USA zu erschließen.

Kooperation mit Behörden

Auf Anfrage stellt Google den Behörden der Länder die angeforderten Daten zur Verfügung. Dabei agiert Google auf Grundlage der nationalen Gesetze. Bei daten-speicherung.de findet man

[3] http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google-yahoo-co-nsa-anwalt-internetfirmen-wussten-von-ausspaehaktionen-12855553.html

[4] https://www.heise.de/-2138499

Zahlen zur Kooperationswilligkeit des Imperiums. Durchschnittlich beantwortet Google Anfragen mit folgender Häufigkeit:

- 3mal täglich von deutschen Stellen,
- 20mal täglich von US-amerikanischen Stellen,
- 6mal täglich von britischen Stellen.

In den drei Jahren von 2009–2012 haben sich die Auskünfte von Google an staatliche Behörden und Geheimdienste verdoppelt, wie die Grafik in Abb. 2.4 der EFF.org zeigt.

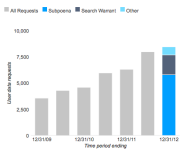


Abbildung 2.4: Steigerung der Auskünfte von Google an Behörden

Die (virtuelle) Welt ist eine „Google“ – oder?

Die vernetzten Rechenzentren von Google bilden den mit Abstand größten Supercomputer der Welt. Dieser Superrechner taucht in keiner TOP500-Liste auf. Es gibt kaum Daten, da das Imperium sich bemüht, diese Informationen geheim zu halten. Die Datenzentren werden von (selbstständigen?) Gesellschaften wie Exaflop LLC betrieben.

Neugierige Journalisten, Blogger und Technologieanalysten tragen laufend neues Material über diese Maschine zusammen. In den Materialsammlungen findet man 12 bedeutende Anlagen in den USA und 5 in Europa, die als wesentliche Knotenpunkte des Datenuniversums eingeschätzt werden. Weitere kleinere Rechenzentren stehen in Dublin, Paris, Mailand, Berlin, München Frankfurt und Zürich. In Council Bluffs (USA), Thailand, Malaysia und Litauen werden neue Rechenzentren gebaut, die dem Imperium zuzurechnen sind. Das größte aktuelle Bauprojekt vermuten Journalisten in Indien (2008).

Experten schätzen, dass ca. 1 Mio. PCs in den Rechenzentren für Google laufen (Stand 2007). Alle drei Monate kommen etwa 100.000 weitere PCs hinzu. Es werden billige Standard-Komponenten verwendet, die zu Clustern zusammengefasst und global mit dem *Google File System (GFS)* vernetzt werden. Das GFS gewährleistet dreifache Redundanz bei der Datenspeicherung.

Die Kosten für diese Infrastruktur belaufen sich auf mehr als 2 Milliarden Dollar jährlich (2007).

Die Videos von YouTube sollen für 10 % des gesamten Traffics im Internet verantwortlich sein. Über den Anteil aller Dienste des Imperiums am Internet-Traffic kann man nur spekulieren.

Google dominiert unser (virtuelles) Leben.

Dabei geht es nicht um ein paar Cookies, sondern um eine riesige Maschinerie.

2.1.2 Weitere Datensammler

Die Datensammler (Facebook, Amazon, Twitter, TikTok, Onlineshops usw.) verkaufen Informationen über Nutzer an Datenhändler (z. B. Acxiom, KaiBlue, RapLeaf u. a.), welche die Daten anreichern, zusammenfassen und umfassende Profile den eigentlichen Endnutzern wie Kreditkartenfirmen, Personalabteilungen großer Unternehmen und Marketingabteilungen von Microsoft bis Blockbuster verkaufen.

Facebook, Twitter, TikTok... hat E. Snowden sehr schön beschrieben:

> Businesses that make money by collecting and selling detailed records of private lives were once described as surveillance companies. Their rebranding as social media is the most successful deception since the Department of War became the Department of Defense.

Es ist nicht nur die Datensammlung, die mich von Jahrmarkt der Eitelkeiten auf den Sozialen Medien fernhält, sondern auch der Lärm der *Großen Clowns* (m/w/d), die nur ihre Selbstdarstellungsshow präsentieren wollen (immer auf der Jagd nach Likes) und der Hass in den giftigen Bissen der surrenden Fliegen, die sich für die Guten halten und mit Eifer ihre religiöse Ideologie verbreiten. Und mein Arm taugt nicht als Fliegenwedel.

Das ist kein Phänomen des Internetzeitalters. F. Nitzsche hat es schon in dem Buch *Also sprach Zarathustra* im Kapitel 14 *Von den Fliegen des Marktes* anschaulich beschrieben.

Acxiom konnte bereits 2001, noch bevor Facebook als Datenquelle zur Verfügung stand, auf umfangreiche Datenbestände verweisen. Als das FBI die Namen der angeblichen 9/1-Attentäter veröffentlichte (von denen noch heute einige quicklebendig sind), lieferte Acxiom mehr Daten zu diesen Personen, als alle Geheimdienste zusammen – inklusive früherer und aktueller Adressen, Namen der Mitbewohner usw. Das war der Beginn einer Zusammenarbeit. Im Rahmen der Zusammenarbeit mit FBI und CIA führten die Daten von Acxiom mehrfach zu Anklagen und Abschiebungen.

Acxiom protzt damit, präzise Daten über 96 % der amerikanischen Bevölkerung zu haben. In Deutschland bietet Acxiom Daten zu 44 Mio. aktiven Konsumenten an. Jeder Datensatz hat 1.500 Datenpunkte. Die Konsumenten werden in 14 Hauptgruppen unterteilt, z. B. *Alleinerziehend & statusarm, gut situierter Midlife-Single* oder *Goldener Ruhestand & aktiv* usw. Diese Hauptgruppen werden nach Lifestyle-Aktivitäten (z. B. *Garten, Haustiere, Sport, Mode, Diät* usw.), Konsumverhalten, Milieuzuordnung (z. B. *intellektuell, statusorientiert-bürgerlich, traditionelles Arbeitermilieu, hedonistisch, konsummaterialistisch usw.*) in bis zu 214 Untergruppen unterteilt.

> *Sie können sich Acxiom wie eine automatisierte Fabrik vorstellen, wobei das Produkt, das wir herstellen, Daten sind.* (Aussage eines Technikers von Acxiom)

Oracle ist eine ehemalige IT-Firma. Früher wurde Software entwickelt und neuerdings wird das Sammeln und Verknüpfen von Daten als profitabler Geschäftszweig entdeckt. Oracle wirbt mit folgenden Datenbeständen:

> *3 Milliarden Verbraucherprofile aus 700 Millionen täglichen Social-Media-Nachrichten, Daten über die Nutzung von 15 Millionen Webseiten und Einkäufe bei 1.500 Händlern.*

Das Tracking des Surfverhaltens wird mit der Auswertung des tagtäglichen Social-Media-Gedöhns und den Einkäufen in Online-Shops kombiniert.

BlueKai ist seit 2014 eine Tochterfirma von Oracle. Ein Datenleck im Juni 2020 zeigte, wie gigantisch und detailliert die Datenbestände von BlueKai sind. Die personenbezogenen Datensätze enthalten folgende Angaben:

- realen Namen, genutzte E-Mail-Adressen, Telefonnummern und Kreditkarten;
- Historie von Online- und Offline-Einkäufen;
- Historie des Surfverhaltens im Internet.

In den Datensätzen konnte beispielsweise nachvollzogen werden, dass ein namentlich bekannter Deutscher für 10 Euro auf einer Webseite für E-Sports-Wetten ein Angebot mit einer Prepaid-Kreditkarte platziert hatte. Auch die E-Mail-Adressen und Telefonnummern des Deutschen waren in der Datenbank zu finden.

Gemäß Eigenwerbung kann BlueKai 1,2 % des Internet-Traffics beobachten, inklusive der Besucher bekannter Porno-Webseiten. Daten von Offline-Einkäufen werden von Firmen gekauft, die als Payment-Prozessoren Kreditkarten-Transaktionen abwickeln.

Match Group monopolisiert den Online-Datingmarkt. Zur Match Group gehören die Dating-Portale Tinder, OkCupid, Plenty of Fish, Meetic, LoveScout24, OurTimes, Pairs, Meetic, Match, Twoo, Neu.de und weitere Partnerportale. In den Datenschutzerklärungen der Portale kann man nachlesen, dass die sensiblen Persönlichkeitsdaten der Nutzer innerhalb der Match Group zwischen Portalen ausgetauscht werden.

Ein Beispiel: Laut der Datenschutz-Policy von Tinder[5] werden folgende Daten gesammelt:

- Informationen, die der Nutzer selbst angibt über Name, Ort, Alter, Geschlecht, sexuelle Vorlieben, Fotos, Videos usw.;
- Informationen über die Nutzung des Dienstes wie Login/Logout-Zeitpunkt, Suchanfragen, Klicks auf interne Seiten und auf Werbung, Kontakte und die Interaktionen mit den Kontakten, versendete und empfangene Nachrichten usw.;
- Informationen über verwendete Geräte (Hardware, Software, IP-Adressen, individuelle Geräte-IDs wie IMEI/UDID oder MAC-Adressen, gerätespezifische Werbe-IDs wie AAID von Google oder IDFA von Apple, Informationen zur Mobilfunkverbindung wie Dienstanbieter und Signalstärke sowie Information der Gerätesensoren wie Beschleunigungssensor, Kompass oder Gyroskope)
- Daten zu Geolocation werden via GPS, Bluetooth, oder WiFi-Verbindungen ermittelt, die Ermittlung der Geolocation kann auch im Hintergrund erfolgen, wenn man die Dienste von Tinder nicht nutzt.
- Falls man *Do Not Track* (DNT) im Browser aktiviert hat, wird es ignoriert.

> *Wir teilen Ihre Daten mit anderen Unternehmen der Match Group. [...] Die Unterstützung kann technische Verarbeitungsvorgänge wie Datenhosting und -wartung, Kundenbetreuung, Marketing und gezielte Werbung [...] umfassen.*
> *Wir dürfen Ihre Daten auch an Partner weitergeben, die uns bei der Verbreitung und Vermarktung unserer Dienste unterstützen.*

Das ist ein Freibrief, um sehr private Details an beliebige Dritte zu verkaufen.

Big Data Scoring aus Estland bewertet die Kreditwürdigkeit von Personen im Auftrag von Banken und anderen Kreditgebern sowie für Kunden aus der Immobilienbranche anhand der Facebook-Profile und der Aktivitäten bei anderen Social-Media-Sites. Das Ergebnis der Bewertung ist eine Zahl von 0 bis 10.

[5] https://www.gotinder.com/privacy

AtData sammelt die Informationen anhand von E-Mail-Adressen. Jeder kann auf der Website eine Liste von E-Mail-Adressen hochladen, bezahlen und nach Zahlungseingang die Daten abrufen. Ein kleiner Auszug aus der Preisliste soll den Wert persönlicher Informationen zeigen:

- Alter, Geschlecht und Ort: 1 Cent pro E-Mail-Adresse
- Haushaltseinkommen: 1 Cent pro E-Mail-Adresse
- Ehestand: 1 Cent pro E-Mail-Adresse
- vorhandene Kinder: 1 Cent pro E-Mail-Adresse
- Wert des bewohnten Hauses: 1 Cent pro E-Mail-Adresse
- Relation von Krediten zum Vermögen: 1 Cent pro E-Mail-Adresse
- vorhandene Kreditkarten: 1 Cent pro E-Mail-Adresse
- Fahrzeuge im Haushalt: 1 Cent pro E-Mail-Adresse
- Smartphone Nutzung: 1 Cent pro E-Mail-Adresse
- Beruf und Ausbildung: 2 Cent pro E-Mail-Adresse
- Tätigkeit als Blogger: 1 Cent pro E-Mail-Adresse
- wohltätige Spenden: 1 Cent pro E-Mail-Adresse
- Präferenzen für hochwertige Marken: 1 Cent pro E-Mail-Adresse
- Präferenzen für Bücher, Zeitschriften: 1 Cent pro E-Mail-Adresse
- ...

Present-Service Ullrich GmbH hat sich auf die Erkennung von Schwangerschaften und Geburten spezialisiert. Von den jährlich 650.000 Geburten in Deutschland kann die Present-Service Ullrich GmbH nach eigenen Angaben 50 % erkennen und ist der Marktführer in Deutschland (Stand: 2014). Die Daten werden zusammen mit Informationen über die finanzielle Situation der Eltern für das Direktmarketing genutzt und verkauft.

Für das Direktmarketing nutzt die Firma 10.000 aktive Partner im Gesundheitswesen (Frauenärzte, Hebammen, Krankenschwestern) und verspricht den Kunden:

> *Ihre Werbebotschaft wird durch den Frauenarzt, die Hebammen bei der Geburtsvorbereitung oder Krankenschwestern bei der Geburt übergeben. Sie erzielen Customer-Touchpoints in einmalig glaubwürdiger Szenerie. So wird ihre Marke von Anfang an Teil der Familie.*

2.2 Techniken der Datensammler

Viele Dienste im Web nutzen die Möglichkeiten, das Surfverhalten und unsere private Kommunikation zu verfolgen, zu analysieren und die gesammelten Daten zu versilbern. Die dabei entstehenden Nutzerprofile sind inzwischen sehr aussagekräftig. Es können das Einkommen, Alter, politische Orientierung, Zufriedenheit mit dem Job, Wahrscheinlichkeit einer Kreditrückzahlung, erotische Liebesbeziehungen und sexuelle Vorlieben, Schwangerschaften u. a. m. eingeschätzt werden. Ein Online-Versand von Brautkleidern möchte bspw. gezielt Frauen im Alter von 24-30 Jahren ansprechen, die verlobt sind. Ein Anbieter von hochwertiger Babyausstattung möchte gezielt finanziell gut situierte Schwangere ansprechen. Das und vieles mehr ist heute schon möglich.

Es geht aber längst nicht nur um die Einblendung von Werbung. Sarah Downey warnt [6] vor wachsenden realen Schäden durch das Online-Tracking. Die gesammelten Informationen können den Abschluss von Versicherungen und Arbeitsverträgen beeinflussen oder sie können zur Preisdiskriminierung genutzt werden. Ganz einfaches Beispiel: das US-Reiseportal Orbitz bietet z. B. Surfern mit MacOS Hotelzimmer an, die 20–30 Dollar teurer sind als die Zimmer, die Windows-Nutzern angeboten werden.[7]

Techniken zum Tracking des Surfverhaltens

Das Surfverhalten liefert die meisten Informationen über unsere Vorlieben. Dabei werden folgende Techniken eingesetzt:

Cookies sind noch immer das am häufigsten eingesetzte Mittel, um Browser zu markieren und das Surfverhalten zu verfolgen.

Blockieren der Cookies von Drittseiten schützt nur teilweise vor dem Tracking mit Cookies. Die Datensammler haben Methoden entwickelt, um Tracking-Cookies als First-Party-Content zu platzieren.[8] Empirische Studien zeigen, dass es 160 Trackingdienste gibt, die mehr als 40 % des Surfverhaltens verfolgen können, wenn das Setzen von Cookies für Drittseiten möglich ist. Wenn man Cookies von Drittseiten verbietet, dann können immer noch 44 Trackingdienste mehr als 40 % des Surfverhaltens verfolgen. Dazu zählen:

- Google Analytics, Chartbeat.com oder AudienceScience.com schreiben die Tracking-Cookies mit JavaScript als First-Party-Content.
- WebTrekk nutzt DNS-Aliases, um eigene Server als Subdomain der aufgerufenen Webseite zu deklarieren und sich First-Party-Status zu erschleichen.
- Yahoo! Web Analytics protzt damit, dass sie ebenfalls ihre Tracking-Cookies als First-Party-Content einsetzen können.

Mit diesen First-Party-Cookies wird das Surfverhalten innerhalb einer Website beobachtet. Zusätzlich werden weitere Methoden wie Browser-Fingerprinting eingesetzt, die eine Verknüpfung der gesammelten Daten über mehrere Webseiten hinweg ermöglichen.

Google hat im Nov. 2023 angekündigt, die Unterstützung für Drittseitencookies bis Ende 2024 aus dem Browser Chrome zu entfernen. Damit wird sich die Trackingbranche endgültig umstellen müssen und es werden dann auch die letzten Cookies von Drittseiten verschwinden.[9]

IP-Adresse wird wieder bedeutsamer für das Tracking, da aufgrund der Cookiekalypse das Tracking mit Cooies immer schwieriger wird. Allerdings wird nicht einfach die IP-Adresse verwendet, die insbesondere bei Smartphones ständig wechselt, sobald man die Komfortzone des heimischen WLANs verlässt. Statt dessen besteht das Ziel, anhand der IP-Adresse ein Gerät oder zumindest einen Haushalt zu identifzieren. Um die Funktionsweise zu verschleiern, nennt man es in der Fachsprache oft *Netzwerk-Cookies*.

Das Verfahren funktioniert folgendermaßen:

[6] https://www.heise.de/-1628313
[7] https://www.heise.de/-1626368
[8] https://anonymous-proxy-servers.net/blog/index.php?/archives/377-Tracking-mit-Cookies.html
[9] https://www.bleepingcomputer.com/news/google/google-shares-plans-for-blocking-third-party-cookies-in-chrome/

1. Wenn ein Surfer eine verseuchte Webseite besucht, sendet der Webserver die IP-Adresse und die aufgerufene Webseite zu einer Marketingplatform.
2. Die Marketingplatform ermittelt den Telekommunikationsprovider und schickt die IP dorthin.
3. Der Telekommunikationsprovider weiß, welchem Smartphone (SIM Karte) oder welchem Haushalt (Router) diese IP-Adresse aktuell zugeteilt ist und liefert eine pseudonyme ID zurück, die für diese SIM Karte oder den Router konstant bleibt, auch wenn die IP-Adresse wechselt.
4. Die Marketingplatform ermittelt aus dem gesammelten Surfverhalten für diese pseudonyme ID die passende Werbung für die Zielperson oder Personengruppe (Haushalt).
5. Der Webserver baut diese individualisierte Werbung in die ausgelieferte Webseite ein.
6. Die angezeigte Werbung könnte man mit uBlock Origin oder ähnlichen Werbeblockern blockieren, aber das Tracking verhindert man damit nicht.

Die erste Marketingplattform dieser Art (Klartext: ein großer, europäischer Trackingprovider) heißt Utiq SA/NV und soll Webservern die Auslieferung von individualisierter Werbung auf Basis einer pseudonymen ID ermöglichen, die aus dem Mobilfunkvertrag des Kunden abgeleitet wird. Utiq SA/NV versucht in erster Linie, Smartphones zu tracken - aber das muss nicht so bleiben.

Im Juni 2023 hat Utiq SA/NV erste Ergebnisse dieser neuen Trackingmethode vorgestellt. Das Tracking anhand der IP-Adresse in Kooperation mit Telcos kann 4x mehr Surfer verfolgen als es mit Third-Party-Cookies möglich ist und ist um 25% besser als Tracking mit First-Party Cookies.

HTML-Wanzen (sogenannte Webbugs) sind 1x1-Pixel große transparente Bildchen, die in den HTML-Code einer Webseite eingebettet werden. Sie sind für den Nutzer unsichtbar. Beim Laden einer Webseite werden sie von einem externen Server geladen und hinterlassen Einträge in den Logdaten. Außerdem können sie Cookies transportieren.

Werbebanner und Like-Buttons können einerseits in der gleichen Weise wie HTML-Wanzen für das Tracking verwendet werden. Außerdem verrät man mit Klicks auf Werbung oder Like-Buttons mehr private Informationen, als man eigentlich veröffentlichen möchte. S. Guha von Microsoft sowie B. Cheng und P. Francis vom Max-Planck-Institut für Software-Systeme haben ein Paper veröffentlicht, wie man homosexuelle Männer anhand der Klicks auf Werbung erkennen kann.[10] Das Verfahren kann für verschiedene Fragestellungen angepasst werden. Die Klicks auf Facebook-Like-Buttons können in der gleichen Weise ausgewertet werden. Forscher der Universität Cambridge (Großbritannien) konnten bei einer Untersuchung die sexuelle Orientierung und politische Einstellung der Nutzer anhand der Klicks auf Like-Buttons vorhersagen.[11]

Immer häufiger nutzen Kriminelle die großen Werbenetzwerke, um mit ihrer Schadsoftware möglichst viele Rechner anzugreifen. Sie kaufen passende Werbeplätze und lassen bösartige Werbebanner ausliefern oder locken die Surfer mit Anzeigen auf Malware-Webseiten. Diese Angriffe werden als *Malvertising* bezeichnet (abgeleitet von *malicious advertising*) und nehmen derzeit stark zu. Die Sicherheitsexperten von Cyphort registrierten 2015 einen Anstieg von 325 % und erwarten eine Fortsetzung dieses Trends für 2016.[12]

[10] http://arstechnica.com/tech-policy/news/2010/10/more-privacy-headaches-for-facebook-gay-users-outed-to-advertisers.ars

[11] https://www.heise.de/-1820638

[12] http://www.cyphort.com/about/news-and-events/press-releases/cyphort-labs-issues-special-report-on-the-rise-in-malvertising-cyber-attacks/

EverCookies nutzen moderne HTML5-Techniken wie DomStorage, ETags aus dem Cache u. A. als Ersatz für Cookies, um den Surfer zu markieren und ihn später anhand dieser Markierungen wiederzuerkennen. Der polnische Informatiker Samy Kamkar hat eine Webseite zur Demonstration von EverCookie-Techniken erstellt.[13] 38 % der populären Webseiten nutzen bereits verschiedene EverCookie-Techniken (Stand: Oktober 2012).

Browser-Fingerprinting nutzt verschiedene Merkmale des Browsers wie z. B. Browserversion, installierte Schriftarten, Bildschirmgröße, bevorzugte Sprachen und weitere Daten, um einen Fingerprint zu berechnen. Dieser Fingerprint ist für viele Surfer eindeutig. Das Projekt Panopticlick[14] der EFF.org zeigte, dass mehr als 80 % der Surfer damit eindeutig erkennbar sind. Die Erkennungsrate stieg auf 94 %, wenn Flash- oder Java-Applets zusätzlich genutzt werden konnten.

Für das Fingerprinting des Browsers werden verschiedene Techniken eingesetzt:

1. HTTP-Header: Es werden die Informationen ausgewertet, die der Browser bei jedem Aufruf sendet (Sprache, Browsername und -version, Betriebssystem und -version, unterstützte Zeichensätze, Dateitypen, Kodierungen).
2. JavaScript-basiert: Informationen werden per JavaScript ausgelesen (installierte Schriften, Bildschirmgröße, Größe des Browserfensters).
3. Canvas-basiert: In einem HTML5-Canvas-Element wird ein Text gerendert, das Ergebnis via JavaScript als Bild ausgelesen und ein Hash über alle Pixel als individuelles Merkmal berechnet. Das Ergebnis unterscheidet sich von Browser zu Browser aufgrund installierter Schriften, Software für das Rendering usw. Das Tracking-Verfahren wurde 2012 in der wissenschaftlichen Arbeit *Perfect Pixel: Fingerprinting Canvas in HTML5*[15] beschrieben.

   Mittels Canvas-Font-Fingerprinting können die installierten Schriftarten ermittelt werden. Das Verfahren wurde 2016 in dem *OpenWPM Paper* beschrieben.
4. Plug-in-basiert: Informationen werden per Flash- oder Java-Plugin ausgelesen (Schriftarten, Betriebssystem, Kernel, Multi-Monitor Setups, Bildschirmgröße).
5. Add-on-basiert: Durch Seiteneffekte werden evtl. vorhandene Browser Add-ons analysiert (NoScript-Whitelist, AdBlock-Blacklist, User-Agent-Spoofing).
6. Hardware-basiert: Informationen über die Hardware des genutzten Rechners werden gesammelt (Vibrator-API, Zugriff auf Mikrofon und Webcam, Performance der Grafikhardware und Besonderheiten im Soundsystem).
7. CSS Fingerprinting verwendet trickreiche CSS Hacks statt Javascript, um Informationen über den Computer zu sammeln und daraus einen möglichst eindeutigen Fingerprint zu berechnen, der eine Wiedererkennung des Browsers ermöglichen soll. Man kann die installierten Schriftarten ermitteln, mit Mediaqueries die Bildschirmgröße schätzen (was ein alter Hut ist) u.v.a.m.

   In dem Paper *Web Browser Fingerprinting Using Only Cascading Style Sheets*[16] (2015) wurde ein erstes Konzept dafür vorgeschlagen. Allerdings wurde bisher nicht die gleiche Qualität wie beim Javascript Fingerprinting erreicht.

Die Studien *Dusting the Web for Fingerprinters*[17] (2013) und *The web never forgets*[18]

[13] https://samy.pl/evercookie/
[14] https://panopticlick.eff.org/browser-uniqueness.pdf
[15] http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf
[16] https://ieeexplore.ieee.org/document/7424801
[17] http://www.cosic.esat.kuleuven.be/publications/article-2334.pdf
[18] https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf

(2014) der KU Leuven (Belgien) und OpenWPN.[19] (2016) der Princeton University haben nachgewiesen, das Fingerprinting für das Tracking genutzt wird. Mit dem *FP-Insector* haben US-amerikanische Forscher 2020 nachgewiesen, dass das Browser-Fingerprinting als Trackingtechnik bei fast einem Viertel der Top-10.000-Webseiten eingesetzt wird, insbesondere bei News- und Shopping-Webseiten.[20]

- *Bluecava* nutzt ausschließlich Browser-Fingerprinting und protzt mit 30 % besseren Ergebnissen als Cookie-basierte Techniken.[21]
- *Zanox.com* nutzt den Fingerprint des Browsers, wenn Cookies gelöscht oder per Browser-Einstellung blockiert werden.[22]
- *WebTrekk* berechnet einen Fingerprint auf Grundlage von Geolocation und anhand von IP-Adresse, Bildschirmgröße und Farbtiefe des Monitors, innerer Größe des Browserfensters, bevorzugter Sprache, User-Agent des Browsers, Version des Betriebssystems sowie Einstellungen für Java, JavaScript und Cookies.[23]
- *Multicounter* nutzt den Fingerprint zusätzlich zu Cookies oder EverCookies zur Verbesserung der Erkennungsraten.[24]
- *Anonymizer Inc.* verwendet Browser Fingerprinting auf sämtlichen Webseiten, verschweigt es aber im Privacy Statement. (Eine seltsame Auffassung für jemanden, der Anonymität verkaufen will.)
- *Yahoo! Web Analytics* nutzt Fingerprinting, wenn Cookies blockiert werden.
- Canvas-Fingerprinting wird u. a. von den Trackingdiensten *doubleverify.com, lijit.com* und *alicdn.com* genutzt. Auf 14.371 Webseiten wurden Trackingscripte mit Canvas-Fingerprinting nachgewiesen (Stand: 2016).
- AudioContext-Fingerprinting wurde bei drei Trackingdiensten nachgewiesen, die jedoch nur eine geringe Reichweite haben und nur auf wenigen Webseiten eingebunden sind.

Da Browser-Fingerprinting keine Markierungen einsetzt, die man löschen könnte, ist eine Verteidigung besonders schwer realisierbar. Wichtigste Verteidigungsmaßnahmen sind das Blockieren von JavaScript (vor allem für Drittseiten), blockieren von Flash und die Nutzung von AdBlock, um Tracking-Scripte zu blockieren.

Keystroke-Biometrics verwendet das Schreibverhalten der Nutzer auf der Tastatur als Identifizierungsmerkmal. Der HTML5-Standard definiert eine API, um auf Tastaturereignisse reagieren zu können. In Firefox 38.0 wurden erste Teile der API standardmäßig aktiviert. In Kombination mit hoch-genauen Timern können Webapplikationen das Schreibverhalten der Surfer in Webformularen analysieren und als biometrischen Login (z. B. von der Firma KeyTrac angeboten) oder als Trackingfeature verwenden.

Mit Windows 10 hat Microsoft begonnen, das Schreibverhalten der Anwender im Hintergrund durch das Betriebssystem analysieren zu lassen und die erstellten biometrischen Profile an die Firma BehavioSec zu senden, die mit der DARPA und Microsoft kooperiert. Laut Eigenwerbung kann BehavioSec 99 % der Nutzer korrekt erkennen. Die dabei entstehende umfangreiche Sammlung der biometrischen Profile kann zukünftig zum Tracking und zur Deanonymisierung genutzt werden.

[19] https://www.privacy-handbuch.de/download/OpenWPM_1_million_site_tracking_measurement.pdf
[20] https://www.golem.de/news/browser-fingerprinting-neue-methoden-gegen-cookie-loses-tracking-2008-150518.html
[21] http://www.bluecava.com/visitor-insight-campaign-measurement
[22] http://blog.zanox.com/de/zanox/2013/09/11/zanox-stellt-tpv-fingerprint-tracking-vor/
[23] http://www.webtrekk.com/de/index/datenschutzerklaerung.html
[24] http://www.multicounter.de/features.html

Wischen, Tippen, Zoomen sind die üblichen Gesten für die Bedienung der Touchscreens auf Smartphones. Ein australisches Forschungsteam präsentierte auf der PETS 2018 das Paper *Quantifying the Uniqueness of Touch Gestures for Tracking*,[25] in dem gezeigt wird, dass diese Touch-Gesten individuell unterschiedlich und dadurch für die Wiedererkennung von Smartphone-Nutzern geeignet sind.

> *Im Vergleich zu üblichen Tracking-Mechanismen, z. B. basierend auf Cookies, Browser-Fingerprints, Browser-User-Agents, Log-Ins und IP-Adressen, gibt es mehrere Faktoren, die das Tracking basierend auf Touch-Informationen potenziell riskanter machen. Während die anderen Mechanismen virtuelle Identitäten wie Online-Profile tracken, birgt touch-based tracking das Potenzial, die eigentliche (physische) Person am Gerät zu tracken und zu identifizieren.*

Die Touch-Daten können über APIs von allen Smartphone-Apps ausgelesen werden.

Tracking von E-Mail-Newslettern

Die Markierung von E-Mail-Newslettern ist weit verbreitet. Es geht dabei darum, das Öffnen der E-Mails zu beobachten und die Klicks auf Links in den Newslettern zu verfolgen.

- Wie beim Tracking des Surfverhaltens werden kleine 1x1-Pixel-große Bildchen in die E-Mail eingebettet, die beim Lesen im HTML-Format von einem externen Server geladen werden. Durch eine individuelle, nutzerspezifische URL kann die Wanze eindeutig einer E-Mail-Adresse zugeordnet werden. Ein Beispiel aus dem E-Mail-Newsletter von Paysafecard, das einen externen Trackingservice nutzt:

  ```
  <IMG src="http://links.mkt3907.com/open/log/43.../1/0">
  ```

  Easyjet.com (ein Billigflieger) kann offenbar die Aufrufe seiner Newsletter selbst zählen und auswerten. In den E-Mails mit Informationen zu gebuchten Flügen findet man folgende kleine Wanze am Ende der Mail:

  ```
  <IMG src="http://mail.easyjet.com/log/bEAS001/mH9..." height=0 width=0
  ↪ border=0>
  ```

  Bei kommerziellen E-Mail-Newslettern kann man fast sicher davon ausgehen, dass sie Wanzen enthalten. Ich habe diese Trackingelemente in so gut wie allen kommerziellen Newslettern von *PayPal.com, Easyjet, AirBerlin, Paysafecard, UKash* usw. gefunden. Sie werden aber nicht nur im kommerziellen Bereich verwendet. Die CDU Brandenburg markierte ihre Newsletter über einen längeren Zeitraum, um zu überprüfen, wann und wo sie gelesen wurden. *ACCESS Now* und *Abgeordnetenwatch* sind weitere Beispiele.

- Neben kleinen Bildern können weitere HTML-Elemente wie CSS-Stylesheets, Media-Dateien oder Link-Prefetching in einer E-Mail genutzt werden. Der E-Mail Privacy Test[26] zeigt eine umfangreiche Liste. Diese Elemente werden in der Praxis aber kaum genutzt.

- Die Links in den E-Mails führen oft nicht direkt zum Ziel. Sie werden über einen Trackingservice geleitet, der jeden Klick individuell für jede Empfängeradresse protokolliert und danach zur richtigen Seite weiterleitet. Als Beispiel soll ein Link aus dem Paysafecard-Newsletter dienen, der zu einem Gewinnspiel auf der Paysafecard-Webseite führen soll:

[25] https://petsymposium.org/2018/files/papers/issue2/popets-2018-0016.pdf
[26] https://emailprivacytester.com//

```
<a href="http://links.mkt3907.com/ctt?kn=28&ms=3N...">Gewinne Preise
↪  im Wert von 10.000 Euro</a>
```

Als Schutzmaßnahme gegen dieses Tracking sollte man Mails als Text lesen.

Tracking von Dokumenten (PDF, Word usw.)

Die Firma ReadNotify bietet bspw. einen Service, der Word-Dokumente und PDF-Dateien mit speziellen unsichtbaren Elementen versieht. Diese werden beim Öffnen des Dokumentes vom Server der Firma nachgeladen und erlauben somit eine Kontrolle, wer wann welches Dokument öffnet. Via Geo-Location ermittelt ReadNotify auch den ungefähren Standort des Lesers. Aus der Werbung von ReadNotify:[27]

> *We not only let you know when your document or PDF was opened, but we will also endeavor to let you know:*
>
> - *Date, time, location, ISP, etc regarding each reading*
> - *Recipient/reader details*
> - *When applicable, details showing when your document was Printed out (on paper) or Saved (a copy made to disk)*
> - *Details on whether or not it was forwarded (and where possible; to whom)*
> - *Which pages of your PDF were read*
> - *Length of time read*
> - *How many times it was opened and re-opened (with optional instant notifications each time)*

2.3 Tendenzen auf dem Gebiet des Tracking

Obwohl 80 % der Internetnutzer das Tracking des Surfverhaltens ablehnen, wird es stetig ausweitet. Dabei wird es sowohl technisch durch die großen Datensammler immer weiter ausgebaut als auch durch politische Entscheidungen bezüglich der Datensammlung erleichtert.

1. Mehr Trackingelemente werden auf den Webseiten eingesetzt. Das Projekt *Web Privacy Census* der University of California verfolgt seit mehreren Jahren die Entwicklung und dokumentiert einen stetigen Anstieg von Trackingelementen bei den meistbesuchten Webseiten (Top-100, Top-1000 und Top-25.000). Als Beispiel soll die Anzahl der Cookies dienen, die beim Besuch der 100 populärsten Webseiten gesetzt werden (ohne Login, nur beim Betrachten der Webseiten):

	Anzahl der Cookies
2009	3.602
2011	5.675
2012	6.485
2015	12.857

[27] https://ssl1.readnotify.com/readnotify/pmdoctrack.asp

2. Das Projekt registriert eine überproportionale Zunahme schwer blockierbarer Trackingfeatures (EverCookies). Immer mehr Webseiten verwenden HTML5-DomStorage, IE_userdata oder ETags aus dem Cache für die Verfolgung des Surfverhaltens. Für die meistbesuchten Webseiten wurden folgende Zahlen zur Nutzung von EverCookies ermittelt:

	Nutzung von EverCookies
2011	19 % der Webseiten
2012	34 % der Webseiten
2015	76 % der Webseiten

3. Durch den Aufkauf kleinerer Anbieter durch die Großen der Branche erfolgt eine Marktbereinigung. Es bilden sich sogenannte Tracking-Familien, die die Daten untereinander austauschen und somit eine große Reichweite bei der Beobachtung des Surfverhaltens haben. Die größten Tracking-Familien sind:

   (a) Die Google-Familie ist unangefochten die Nummer Eins. 44 % der weltweiten Umsätze in der Onlinewerbung werden durch diese Gruppe erzielt. Das Google-Imperium hat in den letzten Jahren die Firmen *YouTube, DoubleClick mit falkad.net, FeedBurner, Springs, Adscape, AdMob, Teracent, Invite Media, Admeld, Adelphic, Wildfire Interactive* u. a. m. aufgekauft. Nach dem OpenWPM-Report von 2016 gehören die TOP-5-Trackingdienste alle zur Google-Familie und von den TOP-20-Trackingdiensten gehören 12 zum Google-Imperium. Die folgende Tabelle zeigt, wie das Google Imperium dadurch seine Präsenz auf den 1000 populärsten Webseiten in den letzten Jahren ausbauen konnte:

	Trackingelemente der Google-Familie
2005	auf 7 % der Webseiten
2006	auf 16 % der Webseiten
2008	auf 55 % der Webseiten
2012	auf 74 % der Webseiten
2015	auf 92 % der Webseiten

   (b) Auf den Plätzen 2 und 3 folgen Facebook und Twitter, die vor allem mit Like-Buttons und ähnlichem Social-Media-Kram tracken und 2016 eine Abdeckung von mehr als 10 % der 1-Million-Top-Sites erreichten. Die Kooperation von Facebook mit den eigenständigen Trackingdiensten BlueKai und Epsilon ist dabei noch nicht enthalten.

   (c) Auf den folgenden Plätzen liegen etwas abgeschlagen die Tracking-Familien von Microsoft (u. a. mit den Trackingdiensten *atdmt.com, adbureau.com, aquantive.com*), die Yahoo!-Familie (mit den Trackingdiensten *adrevolver, yieldmanager, overture*), die AOL-Familie (mit *adsonar.com, tacoda.net, advertising.com*) und die Oracle Data Cloud (mit *BlueKai, Datalogix, AddThis*) mit einem Marktanteil von jeweils 3–8 %.

4. Die Beobachtung des Surfverhaltens und der Online-Einkäufe liefert nur ein unvollständiges Bild unserer Interessen. Durch Einbeziehung von Daten aus dem realen Leben sollen die Profile verbessert werden.

   - Im Februar 2013 gab Facebook eine Kooperation mit den Datenhändlern *Axciom* und *Datalogix* bekannt. Diese Firmen werten umfangreiche Daten aus der realen Welt aus (Kreditkartenzahlungen, Rabattkarten usw.). Damit sollen die Werbeeinblendungen bei Facebook individueller und zielgerichteter auf die Interessen der Mitglieder zugeschnitten werden.

- PayPal.com will sein Bezahlsystem auch offline in der realen Welt anbieten und verspricht den teilnehmenden Geschäften, dass sie mehr über die Vorlieben ihrer Kunden erfahren werden. Natürlich wird auch PayPal.com mehr über die realen Interessen der Kunden erfahren.
- Google hat 2014 die *Ladenbesuchsmessung* eingeführt und beobachtet anhand der Geolocation der Android-Smartphones, welche Geschäfte der Besitzer des Smartphones in der realen Welt besucht.
- Patentanmeldungen von Google und Firmen-Akquisitionen zeigen, dass das Imperium zukünftig auch Daten in der realen Welt sammeln möchte. Anfang 2014 kaufte Google z. B. mit Nest einen Hersteller von Thermostaten und Rauchmeldern für 3,1 Milliarden Dollar. Die Thermostate von Nest sind in Millionen Haushalten eingebaut und mit Temperatur-, Helligkeits- sowie Luftfeuchtigkeitssensoren ausgerüstet, die via Internet ausgelesen werden können.

  > *Dank Nests eingebauter Sensoren weiß Google jetzt, wann Sie zuhause sind, in welchem Raum Sie sich aufhalten und dank der Feuchtigkeitssensoren im Schlafzimmer auch, wie oft, wie lange und wie leidenschaftlich Sie Sex haben.* (M. Morgenroth)

- Außerdem interessiert sich Google für die Offline-Einkäufe mit Kreditkarten. Über Partnerschaften kennt Google 70 % der Zahlungen mit Kreditkarten in den USA (Stand: Mai 2017). Ähnliche Partnerschaften in Europa sind in Vorbereitung.[28]

5. Alle Datensammlungen wecken natürlich Begehrlichkeiten bei den Geheimdiensten und Strafverfolgern. Leider ist wenig konkretes darüber bekannt. Bei der Anhörung des US Senate Commerce Committee zu den Problemen von Online-Tracking im Juni 2012 sagte B. Liodice als Vertreter der Werbeindustrie, dass das Tracking des Surfverhaltens der Internetnutzer für die Sicherheit der USA wichtig und notwendig ist.

   Die EFF.org kommentierte:

   > *In yesterday's Senate hearing, we heard the advertising industry admit that their near-ubiquitous online tracking program is being used for issues that are the purview of law enforcement.*

   Durch die Snowden-Dokumente wurden konkrete Beispiele bekannt.[29]

   - Die NSA beobachtet den Datenverkehr und nutzt die Tracking-Cookies der Datensammler zur Beobachtung der Surfer und zur Identifikation von Targets, deren Computer mit Trojanern infiziert werden sollen. Insbesondere Das PREF-Cookie von Google wird von der NSA gern genutzt.
   - Außerdem nutzt die NSA die Standortinformationen, die von Smartphone Apps an Datensammler (Service-Provider, Entwickler) gesendet werden, um Personen zu lokalisieren (HAPPYFOOT).

6. Von der Politik ist wenig Unterstützung für Datenschutz zu erwarten. Wie unsere Bundeskanzlerin mehrfach betont hat, leben wir in einer *marktkonformen Demokratie*. Die Demokratie hat sich also marktkonform anzupassen und in erster Linie den sogenannten Wertschöpfungen nicht im Wege zu stehen. Neben den *Finanzprodukten* aus dem Bankensektor (die nichts weiter sind als eine Umverteilung von Geld) gilt jetzt auch das Sammeln und

[28] http://www.latimes.com/business/technology/la-fi-tn-google-ads-tracking-20170523-story.html
[29] https://www.eff.org/deeplinks/2013/12/nsa-turns-cookies-and-more-surveillance-beacons

Auswerten von privaten Daten als eine Art Wertschöpfung, die neue Produkte ermöglicht, über die die Kunden mehrheitlich erfreut sein sollen.

Auf dem Wirtschaftstag 2015 positionierte sich Bundeskanzlerin Merkel gegen den Datenschutz und für diese neue Art der Wertschöpfung. Ihrer Meinung nach sind Daten der bedeutendste Rohstoff dieses Jahrhunderts und die Ausbeutung dieses Rohstoffes sollte nicht durch strenge Datenschutzrichtlinien beeinträchtigt werden.

> *Die eigentliche Musik wird stattfinden jetzt in der Debatte um die Datenschutzgrundverordnung, um das Big Data Management, und da müssen wir aufpassen, dass wir in Europa nicht ein klein wenig schizophren sind. Wir haben das schöne Safe Harbor Abkommen mit den Vereinigten Staaten von Amerika, das heißt, es können alle Daten aus Europa nach Amerika geschickt werden und dort zu neuen Produkten verarbeitet werden, und der europäische Kunde ist froh, mit diesen Produkten dann hantieren zu können. Wir müssen es schaffen, ein solches Big Data Management zu machen, dass Wertschöpfung hier auch in Europa stattfinden kann.*

Auf dem IT-Gipfel 2016 in Saarbrücken bekräftigte Bundeskanzlerin Merkel diese Linie der Bundesregierung nochmal und verabschiedete und sich vom Grundprinzip der Datensparsamkeit als Leitlinie. Sie sagte wörtlich:

> *Denn das Prinzip der Datensparsamkeit, wie wir es vor vielen Jahren hatten, kann heute nicht die generelle Leitschnur sein für die Entwicklung neuer Produkte.*

Wir werden also zukünftig mehr auf Selbstschutz angewiesen sein. Dieser Selbstschutz könnte zukünftig aber schwieriger werden. In der Auseinandersetzung zwischen Werbewirtschaft und AdBlockern stellen sich Bundestag und Bundesrat auf die Seite der Werbewirtschaft. In dem *Abschlussbericht der Bund-Länder-Kommission zur Medienkonvergenz* vom Juni 2016 befasst sich ein eigenes Kapitel damit, wie sich Medien gegen den zunehmenden Einsatz von Werbeblockern schützen können. Ein gesetzliches Verbot von Werbeblockern wird diskutiert:

> *. . . eine zeitnahe Prüfung durch Bund und Länder klären, ob im Hinblick auf die wirtschaftlichen Auswirkungen und damit verbundenen medienpolitischen Risiken gegebenenfalls eine gesetzliche Flankierung geboten ist.*

Unklar ist, wie ein solches Verbot umgesetzt und durchgesetzt werden kann. Nach Ansicht der Interessenvertreter der Werbeindustrie gibt es aber *einen rechts- und medienpolitischen Bedarf für ein gesetzliches Verbot von Ad-Blockern* und sie werden darin von führenden Regierungsmitgliedern unterstützt.

7. Der *Point of no Return* ist längst überschritten. Am 6. Oktober 2015 erklärte der Europäische Gerichtshof (EuGH) das Safe-Habour-Abkommen für ungültig,[30] das bisher den Datentransfer in die USA erlaubte. Die Verquickung von Facebook mit den US-Geheimdiensten im Rahmen von PRISM spielte eine wesentliche Rolle bei der Urteilsfindung.

   Google und Facebook erklärten daraufhin, dass sie auch ohne Safe-Habour-Abkommen wie bisher weitermachen, die Daten europäischer Nutzer in die USA transferieren und dort verarbeiten werden.[31] Sie sehen die EU-Standardvertragsklauseln nach Artikel 26, Absatz 2

[30] https://www.heise.de/tp/artikel/46/46186/1.html

[31] https://www.golem.de/news/safe-harbor-urteil-google-und-microsoft-suchen-neue-wege-des-datentransfers-1510-116945.html

der EU-Datenschutzrichtlinie von 1995 (EC95/46) als ausreichende Grundlage an. In dieser Ansicht werden sie von der EU-Kommission unterstützt.[32]

Meiner Meinung nach haben die europäischen Regierungen und die EU keine andere Möglichkeit, als vor der Marktmacht der US-Konzerne zu kapitulieren. Wenn man Google & Co. das Sammeln von Daten über europäische Nutzer verbieten würde, dann könnten die US-Konzerne im Gegenzug den Zugriff auf ihre Dienste für europäische Nutzer sperren, da sie nicht mehr mit ihren Daten zur Finanzierung der Dienste beitragen. (Im kleineren Maßstab hat es Google beim Leistungsschutzrecht schon einmal demonstriert.)

Die Mehrheit der europäischen Nutzer würde es nicht akzeptieren, auf Facebook, Google, Youporn und Twitter, Microsoft Windows, Apples MacOS und iPhones sowie Android Smartphones usw. verzichten zu müssen. DAS wäre ein hinreichender Grund für einen Aufstand. Somit muss die EU-Kommission dem gemeinsamen Druck der US-Regierung und der US-Firmen nachgeben und ein Konstrukt finden, dass das Sammeln von Daten zur Finanzierung der Services und zur Auswertung durch die US-Geheimdienste (z. B. im Rahmen von PRISM) weiterhin erlaubt.

Dass das neue *Privacy-Shield*-Abkommen (der Nachfolger von *Safe Habour*) eine Kapitulation der EU beim Thema Datenschutz gleichkommt, konnte man erwarten und ist keine Überraschung.

8. Die zukünftige Entwicklung könnte durch folgende Eckpunkte gekennzeichnet sein:

   - Weitere Ausweitung des Marktes auf die zwischenmenschliche Kommunikation;
   - Vereinzelung der Individuen durch Pseudogemeinschaften in der virtuellen Welt;
   - Kontrolle aller digitalen Aktivitäten durch die *smarte Diktatur*.

2.4 Crypto War 3.0

Im Januar 2015 eröffnete der britische Premierminister Cameron den **crypto war 3.0** mit der Forderung, dass **jede Kommunikation für Geheimdienste einsehbar sein muss**. Weitere Politiker wie Obama, der damalige Bundesinnenminister de Maizière oder der australische Justizminister Keenan assistierten. Als hinreichender Grund wird der allgegenwärtige TERRORISMUS kolportiert, der unsere demokratischen Werte bedroht, und immer wieder Pornografie von und mit Minderjährigen (vulgo: Kinderpornografie).

Ein generelles Verbot starker Kryptografie wird nicht ernsthaft diskutiert. Es wäre nicht durchsetzbar und eine kommerzielle Nutzung des Internets wäre praktisch tot. Damit sind nicht Googles Werbeeinnahmen gemeint sondern industrielle Anwendungen, mit denen richtig viel Geld umgesetzt wird (z. B. im Bereich Banken, Börsen usw.).

Ein Schwerpunkt der aktuellen Angriffe auf Verschlüsselung richtet sich gegen Krypto-Messenger-Apps. Dabei sind zwei Angriffsmuster erkennbar:

Forderung nach Backdoors in der Verschlüsselung: Diese Strategie ist nicht neu und wurde schon mehrfach gegen Kommunikationsdienste erfolgreich eingesetzt, sobald diese Dienste eine nennenswerte Popularität erreichten.

- Skype wurde 2005 durch Anwendung des CALEA Act. gezwungen, Schnittstellen für die Überwachung bereitzustellen. Diese Überwachung wurde ständig weiter ausgebaut und heute liest auch Microsoft als Betreiber des Dienstes mit.

[32] http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm

- Blackberry wurde in Kanada, in Indien und in anderen Ländern gezwungen, den Behörden die Schlüssel für die Entschlüsselung zur Verfügung zu stellen.

Mit Gesetzen wird versucht, diese Praxis auf alle Krypto-Messenger auszudehnen:

- Ein Anti-Terror-Gesetz sollte alle Anbieter von Messaging-Diensten in Russland zwingen, dem Geheimdienst FSB die Möglichkeit zur Entschlüsselung der Kommunikation zu geben. Außerdem sollen die Inhalte der Kommunikation für sechs Monate und die Metadaten für drei Jahre gespeichert werden. Der Versuch der Durchsetzung dieses Gesetztes gegenüber dem Messenger Telegram endete in einem Fiasko.[33] Gegenwärtig wird die Durchsetzung des Gesetzes nicht verfolgt.
- In Australien wurde im Dezember 2018 das *Assistance and Access Bill* verabschiedet, welches ebenfalls die Anbieter von Messaging-Diensten zur Hinterlegung eines Generalschlüssels bei den Strafverfolgungsbehörden verpflichtet, um verschlüsselte Kommunikation entschlüsseln zu können. Anbieter von Messaging-Diensten wie Signal haben es abgelehnt, dem Gesetz Folge zu leisten. Die Durchsetzung des Gesetzes wird ebenfalls nicht verfolgt.
- In Deutschland hat Bundesinnenminister Seehofer im Mai 2019 ähnliche Vorstellungen geäußert. Demgemäß sollten alle Messaging-Dienste gezwungen werden, die gewünschten Kommunikationsdaten selbst zu entschlüsseln und in entschlüsselter Form den Strafverfolgungsbehörden zur Verfügung zu stellen. Die vehemente Kritik des Bundesverbandes für IT-Sicherheit, eco-Verband der Internetwirtschaft, CCC, Digitale Gesellschaft u. a. m. verhinderte die Umsetzung dieser Pläne.
- Ende November 2020 wurde der deutsche Vorschlag für einen Beschluss des EU-Rates verabschiedet, der die Betreiber von Messaging-Diensten zur Kooperation mit Behörden und Geheimdiensten verpflichten soll. Es werden darin keine konkreten Verfahren zur Zusammenarbeit vorgegeben. Den Betreibern wird die magische Hausaufgabe der Quadratur des Kreises gestellt, eine sichere Verschlüsselung zu entwickeln und gleichzeitig den Behörden auf Wunsch die entschlüsselten Inhalte zur Verfügung zu stellen. Konkrete Gesetze sollen folgen.

  Die Datenschutzkonferenz von Bund und Ländern hat die Pläne zurückgewiesen. Die *Aushöhlung der Verschlüsselung*, wie vom EU-Rat gefordert, sei kontraproduktiv und könne von Kriminellen und Terroristen umgangen werden.

Moderne Krypto-Messenger sind gegen diese Angriffe robust. Technisch ist es den Betreibern von Messaging-Diensten wie Signal, Wire, Threema oder Telegram nicht möglich, die Ende-zu-Ende-Verschlüsselung nachträglich mit einem Master-Key zu knacken. Daher sind die genannten gesetzlichen Initiativen nicht durchsetzbar.

Seit Mitte 2018 ist daher ein Umdenken bei den Befürwortern der Überwachung erkennbar. Es wird keine Entschlüsselung der Kommunikation gefordert, aber die Betreiber von Messaging-Diensten sollen Behörden dabei unterstützen, sich als „stille Teilnehmer“ in eine verschlüsselte Kommunikation einzuklinken und so Chats bzw. Gruppenchats live und unbemerkt belauschen zu können:

> *It's relatively easy for a service provider to silently add a law enforcement participant to a group chat or call [. . .]*
>
> *We're not talking about weakening encryption or defeating the end-to-end nature of the service. In a solution like this, we're normally talking about suppressing a*

33 https://www.golem.de/news/zensur-russland-zensiert-15-millionen-ips-fuer-telegram-sperre-1804-133895.html

> *notification on a target's device, and only on the device of the target and possibly those they communicate with. That's a very different proposition to discuss and you don't even have to touch the encryption.*

Salopp gesagt: Die Dienste möchten also den Multi-Device-Support moderner Krypto-Protokolle exploiten und dabei nicht erwischt werden. Sie möchten die Möglichkeit haben, ein neues Gerät im Namen eines Benutzers zu registrieren, ohne dass der Benutzer eine Warnmeldung bekommt, und mit diesem Gerät alles mitlesen. (Vereinzelt waren Polizeibehörden mit der Methode bereits erfolgreich, weil Kriminelle mögliche Schutzfunktionen dagegen nicht aktivierten oder Warnungen ignorierten.)

Die Befürworter dieses Ansatzes argumentieren, dass diese Überwachung nicht anders wäre als der Einsatz von Krokodilklemmen bei der alten Telefonie und dass damit die Sicherheit der Verschlüsselung nicht generell geschwächt werden muss.

Frontdoor Diskussion: Auf dem Grünen Polizeikongress im November 2019 haben Conztanze Kurz (Sprecherin des CCC) und Konstantin v. Notz (Grüne) den Vorschlag unterstützt, dass Anbieter von Messaging-Diensten eine modifizierte Version der App bereitstellen könnten, in der die Ende-zu-Ende-Verschlüsselung zugunsten der Strafverfolgung kompromittiert wurde. Diese Version könnte in Kooperation mit Google bzw. Apple auf den Smartphones der Zielpersonen verteilt werden. Diese *Frontdoor* genannte Option hätte einige Vorteile gegenüber einer *Backdoor*, die die Krypto aller Messaging-Apps kompromittiert, oder gegenüber Bundestrojanern, die den Schwarzmarkt für Exploits anheizen werden.[34]

Aufhebung der Haftungsprivilegierung: Mit dem Earn IT Act wurde im März 2020 von einigen Senatoren in den USA der Vorschlag eingebracht, dass sich Krypto-Messenger nicht mehr auf die Haftungsprivilegierung für den Transport verschlüsselter Inhalte berufen können, wenn sie keine Möglichkeit haben, die verschlüsselten Inhalte im Auftrag der Behörden zu scannen.

Aufgrund starken Widerstandes wurde das Gesetz in einer verwässerten Form verabschiedet, die einzelnen US-Bundesstaaten den Erlass einer entsprechenden Verordnung ermöglicht, aber auf US-Bundesebene nicht erzwingt.

Im August 2020 bestätigte der für digitale Dienste zuständige EU-Binnenmarktkommissar T. Breton, dass auch die EU Maßnahmen ergreifen will, um Anbieter von Messengerdiensten in die Pflicht zu nehmen. Diese Dienste müssten sich das Privileg der Haftungsfreistellung für transportierte Inhalte erst verdienen, indem sie ihrerseits das technisch Mögliche tun, um illegale Inhalte zu erkennen und zu blockieren.

Im Vorfeld hatte Kommissarin Ylva Johansson (Inneres) angekündigt, dass Anbieter von Krypto-Messengern zukünftig ihre Plattformen routinemäßig nach pädokriminellen Inhalten durchsuchen müssten. Als Begründung nannte sie den explosionsartigen Anstieg der gemeldeten pädokriminellen Videos von 300.000 zwischen 2015 und 2017 auf über 3,5 Millionen aktuell in den USA. (Für Europa nannte sie keine Zahlen.)

In ihrer Argumentation verschweigt Kommissarin Johansson die Gründe für den Anstieg. Einerseits gibt es in dieser ekligen Branche den gleichen starken Trend weg von Fotos hin zu Videos wie im gesamten Internet. Außerdem wurden seit 2018 mit Microsofts PhotoDNA und vergleichbaren Produkten von Google, Facebook u. a. technische Lösungen ausgerollt, die die automatisierte Erkennung dieser illegalen Inhalte stark verbesserten und somit die Erkennungsraten drastisch steigern konnten. Bei den von Facebook oder Microsoft erkannten Videos handelt es sich in der Regel nur um Lockangebote. Die echt harte Ware wird nicht auf Social-Media-Plattformen angeboten, sondern auf Marktplätzen im Darknet.

[34] https://heise.de/-4595181

Der Verlust der Haftungsprivilegierung würde für den Betrieb von Messengern mit Ende-zu-Ende-Verschlüsselung ohne eine Backdoor, mit der Betreiber verschlüsselte Inhalte scannen könnten, in der EU ein erhebliches Risiko bedeuten. Sollte bei Ermittlungen nachgewiesen werden, dass der Messengerdienst für die Verteilung illegaler Inhalte genutzt wurde, könnte der Betreiber als *Störer* in Haftung genommen werden.

Das betrifft nicht nur kommerzielle, zentralisierte Dienste. Der Betrieb eines [matrix]-Homeservers mit offener Registrierung für unbekannte Dritte könnte damit zum ähnlich unkalkulierbarem Risiko werden wie der Betrieb eines Tor-Exit-Nodes.

Client-Side Scanning: Diese Idee beruht auf der irrwitzigen Annahme, dass die Ende-zu-Ende Verschlüsselung eines Messengers nicht kompromittiert werden würde, wenn der Messenger Client die Daten vor der Verschlüsselung lokal auf dem Smartphone scannt und bei suspekten Nachrichten im Hintergrund eine Kopie an die Behörden sendete, die sich das dann mal genauer ansehen können.

Die Argumentation ist Bullshit[35]. Wenn alle privaten Nachrichten irgendwo auf dem Transportweg automatisiert gelesen, auf Konformität mit geltendem Gesetzen geprüft und Verstöße automatisiert den Behörden gemeldet werden, dann ist es anlasslose Massenüberwachung und E-2-E Verschlüsselung soll gegen diese Massenüberwachung schützen.

(Dabei ist es egal ob unverschlüsselte Nachrichten an den Internetknoten gescannt werden, ob die die Nachrichten beim Provider entschlüsselt und gescannt werden oder lokal auf dem Smartphone vor dem Verschlüsseln.)

Anlasslose Massenüberwachung ist nicht mit unseren Werten vereinbar (sagte der EuGH).

Im September 2023 hat das britische Parlament das *Online Safity Bill* verabschiedet, welches von allen Messenger mit Ende-zu Ende ein Client-Side Scanning nach kinderpronografischen Bildern fordert. Die diesbezüglichen Bestimmungen des Gesetzen sollen aber (noch) nicht durchgesetzt werden, bis jemand eine Idee für die magische Quadratur des Kreises findet, einserseits alle Nachrichten zu scannen und gleichzeitig eine Privasphäre zu gewähreilsten.

In der EU wird gleichfalls darüber diskutiert, Messenger mit starker Ende-zu-Ende Verschlüsselung zum lokalen Scannen nach KiPo in allen Nachrichten vor dem Verschlüsseln zu zwingen. Die Zivilgesellschaft protestiert, aber die Diskussion in der EU ist noch nicht entschieden.

Staatliches Hacking und Einsatz von Trojanern: Da Hintertüren in der Verschlüsselung von Kommunikation zur Zeit in der EU und den USA nicht populär sind, versucht man es mehr mit staatlichen Hackerangriffen, die gesetzlich legitimiert und personell besser ausgestattet werden sollen.

- In Deutschland nimmt die im November 2015 angekündigte Bundes-Hacker-Behörde zur Unterstützung von Geheimdiensten und Strafverfolgung beim Brechen von Verschlüsselung langsam Gestalt an. Die *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* (Zitis) soll seit 2017 mit 60 Mitarbeitern einsatzbereit sein und dann schrittweise auf 400 Mitarbeiter ausgebaut werden.

  Der bis 2015 vom BKA eingesetzte *Bundestrojaner* der Firma DigiTask wurde vom CCC nach nur 11 Einsätzen enttarnt. In den Folgejahren gab es technische Probleme mit der selbst entwickelten RCIS 1.0 (*Remote Control Interception Software*), die in der Praxis unbrauchbar war. Seit Mitte 2018 ist eine Software von FinFischer für Quellen-TKÜ und die Online-Durchsuchung verfügbar. Außerdem kommt der Pegasus Trojaner der NSO Group bei BKA und BND zum Einsatz und Anfang 2023 wurde

[35] Bullshit (engl.): Kot von einem männlich gelesenen Rindvieh mit Zeugungsfägigkeit

bekannt, dass sich das BKA auch für den Predator Trojaner der griechischen Firma Intellexa interessiert.

Neben dem BKA möchte auch der Verfassungsschutz dieses Spielzeug einsetzen, bspw. wenn mal wieder die Beobachtung einer „terroristischen Vereinigung“ nach §129a konstruiert wurde. Das würde die Einsatzzahlen in Zukunft deutlich nach oben treiben.

- In den USA soll *Rule 41 of the US Federal Rules of Criminal Procedure* ab Dezember 2016 das staatliche Hacken von Tor- und VPN-Nutzern für das FBI massiv erleichtern, unabhängig davon, in welchem Land die Tor-Nutzer sich befinden.[36]

  Dass das FBI den TorBrowser knacken und installieren kann, haben sie 2013 und 2015 bewiesen. Der 2015 verwendete Exploit schien auch 2016 noch zu funktionieren. TorProject.org und die Mozilla Foundation haben sich um eine Veröffentlichung des Exploits bemüht, aber das Wissen um diese Schwachstelle wurde unter Hinweis auf die *Nationale Sicherheit* als geheim klassifiziert.

  Die Kompetenzen der NSA im Rahmen des Programms BULLRUN wurden durch die Dokumente von Snowden/Greenwald bekannt. EGOTISTICALGIRAFFE heißt das Programm, welches Methoden zum offensiven Angriff auf Tor entwickelt.

- In Schweden darf die Polizei ab März 2020 Bundestrojaner einsetzen. In der Begründung für das Gesetz wird darauf verwiesen, das 90 % der Kommunikation, für die die Polizei eine Lizenz zur Überwachung hat, verschlüsselt über Messenger wie Signal App erfolgt.

2.5 Fake-News-Debatte

Manche nennen es *Fake News*, andere sprechen von *alternativen Fakten*, umgangssprachlich nennt man es *Lügen* und in den wundersamen Geschichten des Barons von Münchhausen erlangte das Phänomen literarischen Weltruhm.

Als 2016 die Ergebnisse des Brexit-Votums und der US-Wahlen nicht mehr der Meinungsvorgabe der Mainstream-Medien entsprachen, schrillten Alarmglocken. Ende November 2016 deklarierte Bundeskanzlerin Merkel das Thema Fake News als ernste Bedrohung für den Ausgang der Wahlen in Deutschland.

2.5.1 Der Kampf gegen Fake News

Alternative Medien und Diskussionen in abgeschotteten Facebook-Gruppen sollen eine Gefahr für die Demokratie sein, die die Informationshoheit der etablierten Mainstream-Medien in Frage stellen und mit Falschmeldungen untergraben. Um uns vor Fake News zu schützen wurden hektisch Maßnahmen diskutiert:

1. Es wurden *Faktenchecker* wie Correctiv oder die ARD/ZDF Faktenchecker eingerichtet, die das Vertrauen genießen und Fake News entlarven sollten. Da diese *Faktenchecker* aber selbst eine politische Agenda verfolgen, hat sich schnell gezeigt, dass sie für eine neutrale Bewertung von News und Wahrheitsfindung ungeeignet sind.

2. Mit dem Netzwerkdurchsetzungsgesetz (NetzDG) werden stärkere Geschütze aufgefahren. Betreiber von Social-Media-Plattformen sollen Fake News entfernen, bevor sie viral werden und eine größere Reichweite erlangen. Dafür wird Facebook im deutschsprachigem Raum

[36] https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government

vom Recherchekollektiv Correctiv unterstützt, die selbst schon Fake News verbreitet haben, um ihre politische Agenda zu verfolgen.

Viele Rechtsexperten halten das NetzDG für verfassungswidrig, da es die Meinungs- und Pressefreiheit unzulässig stark einschränkt. Auch der UN-Sonderberichterstatter für Meinungsfreiheit rügt das NetzDG. Das Gesetz gefährdet die Menschenrechte auf Meinungsfreiheit und Privatsphäre. Im Zweifel würden Internetfirmen auch legale Inhalte löschen, um die Gefahr von Bußgeldzahlungen zu minimieren. Eine passendere Bezeichnung für das Gesetz wäre *Meinungsbeschränkungsgesetz* (neusprech.org).[37]

3. Um die Deutungshoheit westlicher Mainstream-Medien zu sichern und die Reichweite von Alternativen einzuschränken, überarbeitete Google seinen Suchalgorithmus:

   - Ende April 2017 gab Google eine Änderung seines Suchalgorithmus bekannt, um den Zugang zu minderwertigen Informationen wie Verschwörungstheorien und Fake News zu erschweren. Es werden jetzt die Mainstream-Meinungen bevorzugt und Webseiten mit abweichenden Meinungen abgewertet, wenn die Such-Historie eines Nutzers nicht darauf schließen lässt, dass er gezielt nach alternativen Meinungen sucht.
     Einige Webseiten wie z. B. die World Socialist Web Site der 4. Internationale berichten von einem Rückgang der Besucher bis zu 70 % durch diese Änderung.[38] [39]
   - Im November 2017 gab Google-CEO Erich Schmidt bekannt, dass die russische Nachrichtenseite RT.com und das Portal *Sputnik News* im Google News Service benachteiligt werden sollen, um die Reichweite zu reduzieren.[40]

     > *We are working on detecting and de-ranking those kinds of sites – it's basically RT and Sputnik.* [...] *But we don't want to ban the sites – that's not how we operate.*

   - Im August 2023 hat die Google News Initiative (GNI) eine Änderung des Google Fact Checking Tools bekannt gegeben, welche auch das Ranking von Webseiten beeinflusst. Einige Richtlinien für die Erkennung von Fake News bei Google Fact Checking:
     - Wer der WHO widerspricht (egal welches Thema), verbreitet Fake News.
     - Wer die Aussagen des IPCC zum menschengemachten Klimawandel in Frage stellt oder relativiert, verbreitet Fake News.
     - Die UNO Datenbank zur Statistik über CO2 Emmisionen ist die wahre Quelle.
     - Außerdem gelten für Googles Fact Checking das FBI und die Weltbank als Quellen der reinen Wahrheit, die nicht hinterfragt werden dürfen.

4. Während man in Deutschland (und im Rest der EU) fordert, dass Big Tech (Google, Facebook usw.) die alternative Medien möglichst klein halten und staatstragende Medien bevorzugt behandeln soll, fordert die EU, dass es in Belarus genau umgekehrt gehandhabt wird. Die EU fordert bei Google Bevorzugung von oppositionellen Medien in Belarus.[41]

(Die *Verschwörungstheorien* von heute sind oft die Wahrheiten von morgen. In allen unten genannten Beispielen würde die neue Bewertung von Google die Fake News gegenüber der Wahrheit mehr und mehr bevorzugen.)

[37] https://neusprech.org/netzwerkdurchsetzungsgesetz/
[38] https://www.wsws.org/de/articles/2017/07/28/goog-j28.html
[39] https://www.wsws.org/de/articles/2017/08/05/goog-a05.html
[40] https://www.rt.com/news/410444-google-alphabet-derank-rt/
[41] https://www.heise.de/news/EU-Kommissarin-Google-Co-sollen-oppositionelle-Medien-in-Belarus-bevorzugen-9590323.html

2.5.2 Fake-News-Beispiele

Mir fallen spontan folgende Fake News aus den letzten 400 Jahren ein, die teilweise schwerwiegendere Folgen hatten als ein Wahlergebnis in Deutschland:

- Im Jahr 1616 wiesen die damaligen Faktenchecker nachdrücklich darauf hin, dass Herr Galileo Galilei Fake News verbreitet.
- FAKE: *Im Januar 1999 massakrierten serbische Soldaten beim Massaker von Racak Zivilisten aus dem Kosovo.*

  WAHR: Nach dem Vormarsch der UCK im Kosovo ging die serbische Armee zum Gegenangriff über und es kam bei der Ortschaft Racak zu Gefechten zwischen der UCK-Brigade 161 und der serbischen Armee.

  Die rot-grüne Bundesregierung brauchte Propagandabilder zur Begründung des ersten Kriegseinsatzes der Bundeswehr im Ausland und verwendete Fotos der OSZE-KVM und KDOM nach einem Kampf zwischen UCK und serbischer Armee ein bisschen zweckentfremdet. Die gefallenen UCK-Kämpfer wurden als Zivilisten bezeichnet, die Fotos von ihren Waffen und Ausweisdokumenten wurden unterschlagen.

  Das *Massaker von Racak* war die Begründung für die NATO, um an der Seite der UCK in den Bürgerkrieg einzugreifen und Belgrad zu bombardieren. Auch Deutschland beteiligte sich an diesem völkerrechtswidrigen Angriff.
- FAKE: *Irakische Soldaten haben beim Überfall auf Kuwait frühgeborene Säuglinge aus den Brutkästen gerissen und auf dem Boden des Krankenhauses liegen gelassen, wo die Säuglinge starben.* (Brutkastenlüge, vom damaligen US-Präsidenten George H. W. Bush und von Menschenrechtsorganisationen vielfach zitiert.)

  WAHR: Die *Brutkastenlüge* wurde völlig faktenfrei von der PR-Agentur Hill & Knowlton im Auftrag der kuwaitischen Exil-Regierung erfunden. Die „Krankenschwester“, die als Zeugin aussagte, war die Tochter des kuwaitischen Botschafters in den USA.
- FAKE: *Der Irak hat Massenvernichtungswaffen! Insbesondere verfügt Diktator Saddam Hussein über mobile Biowaffen-Labore, die hoch-beweglich und auf Tiefladern montiert sind.* (US-Verteidigungsminister Rumsfeld und US-Außenminister C. Powell)

  WAHR: Alles komplett erlogen, die Story wurde unter Mithilfe des BND produziert und in der UNO als Grund für einen Überfall auf den Irak präsentiert. Nach dem Bericht der Iraq Survey Group (ISG) besaß der Irak 2003 keine ABC-Waffen.[42]
- FAKE: *Whistleblower Edward Snowden könnte ein russischer Spion sein.* (G. Maaßen, Chef des BfV) oder *Snowden ist ein Russen-Agent.* (J. R. Schindler)

  WAHR: E. Snowden ist gegen seinen Willen in Russland gestrandet, weil der US-Geheimdienst CIA unprofessionell arbeitete und unfähig war, Snowden festzusetzen. Russland hat ihm in ausweglosser Situation Asyl gewährt.
- FAKE: *Es wird ein No-Spy-Abkommen mit den USA geben.* (Bundeskanzlerin A. Merkel, Innenminister H.-P. Friedrich, Kanzleramtsminister R. Pofalla, S. Seibert)

  WAHR: Nach Berichten von NDR und WDR war der Bundesregierung bereits 2013 bekannt, dass die US-Regierung nie ein No-Spy-Abkommen angeboten hatte und zu einem solchen Abkommen auch keine Zustimmung von der US-Regierung zu erwarten war. Man brauchte aber etwas Gegengift zu den Snowden-Enthüllungen.

[42] http://www.faz.net/aktuell/politik/ausland/irak-krieg-keine-massenvernichtungswaffen-1175499.html

- FAKE: *Die AfD ist eine rechts-populistische Partei der Geringverdiener und ein Sammelbecken für die sozial Abgehängten der Gesellschaft.*

  WAHR: Die Mitglieder der AfD gehören überwiegend zur Mittelschicht. Der Anteil der Geringverdiener (unter 2.000 Euro Netto) unter den AfD-Anhängern entspricht mit 27 % der Anhängerschaft der CDU (28 % Geringverdiener) und ist geringer als bei SPD (32 %) und Linke (37 %).[43]

- FAKE: *Steckt Russland hinter der Attacke auf Telekom-Router?* Bundeskanzlerin Merkel und BND-Präsident Kahl warnen angesichts des Telekom-Hacks vor Cyber-Angriffen aus Russland, denn *nach den Erkenntnissen des BND wollen russische Hacker die Demokratie zerstören!*

  WAHR: Es gab keinen Angriff auf die Telekom, der Ausfall der Router war nur ein Kollateralschaden. Die kriminellen Betreiber des Mirai-Botnetzes wollten Zyxel-Router angreifen, die der irische Provider Eir an seine Kunden verteilte und die einen Security-Bug im TR-069 Interface haben. Die Telekom-Router hatten sich bei den automatisierten Tests des Mirai-Botnetzes auf Verwundbarkeit selbst abgeschaltet.[44]

  Der für den schrecklichen Angriff auf die Telekom-Router verantwortliche Hacker wurde vom LG Köln zu eine Bewährungsstrafe(!) von 20 Monaten verurteilt.[45]

- FAKE: *Russische Hacker griffen 2016 die Wahlen in der USA ein und verhalfen Donald Trump zum Wahlsieg, indem interne E-Mails des DNC, die die Korruptheit von Hillary Clinton bewiesen, bei Wikileaks publiziert wurden.*

  WAHR: Laut Aussage von Assange wurden die DNC-E-Mails, die Hillary Clintons Korruptheit bewiesen, von dem DNC-Mitarbeiter Seth Rich an Wikileaks geliefert, der im November 2016 beim Joggen erschossen wurde. Wikileaks versprach $20.000 Belohnung für Hinweise, die zur Verurteilung des Mörders von Seth Rich führen können.[46]

  Diese Aussage wird von der forensischen Analyse des DNC-Servers gestützt. Die Veteranen der US-Geheimdienste veröffentlichten in einem Memorandum an den US-Präsidenten die folgenden Schlussfolgerungen aus der Analyse:[47]

  > *Forensic studies of Russian hacking into Democratic National Committee computers last year reveal that on July 5, 2016, data was leaked (not hacked) by a person with physical access to DNC computer.*
  > [...]
  > *Key among the findings of the independent forensic investigations is the conclusion that the DNC data was copied onto a storage device at a speed that far exceeds an Internet capability for a remote hack.*
  > (Die Daten wurden mit einer mittleren Geschwindigkeit von 22,1 MB/s kopiert, Spitzenwert 49 MB/s. Das spricht für ein lokal angeschlossenes USB-Device.)

  Jack Matlock, ehemaliger US-Botschafter in Moskau und ehemaliges Mitglied im Nationalen Sicherheitsrat der USA, hält die Legende von russischer Wahleinmischung für politisch motiviert, um Präsident Trump zu delegitimieren.[48]

[43] https://www.zeit.de/politik/deutschland/2016-11/afd-waehler-geringverdiener-spd-die-linke-forsa-umfrage
[44] https://www.heise.de/-3520212
[45] https://www.golem.de/news/deutsche-telekom-router-hacker-bekommt-bewaehrungsstrafe-1707-129183.html
[46] https://twitter.com/wikileaks/status/763041804652539904
[47] https://consortiumnews.com/2017/07/24/intel-vets-challenge-russia-hack-evidence/
[48] https://consortiumnews.com/2018/07/03/former-us-envoy-to-moscow-calls-intelligence-report-on-alleged-russian-interference-politically-motivated/

- Die Corona-Krise 2020 war eine Blütezeit für Fake News. Es gab Meldungen zu Medikamenten, die gegen SARS-COV-2 helfen, wie Ibuprofen, Hydroxychloroquin oder Desinfektionsmittel (intravenös). Bill Gates will angeblich die Corona-Schutzimpfung nutzen, um uns allen Microchips zu implantieren (40 % der Trump-Wähler glauben das)[49] oder er hat heimlich die WHO und Bundesregierung gekapert (KenFM) usw.

  FAKE: Mein persönliches Fake-News-Highlight ist diese Meldung aus dem Bundesgesundheitsministerium vom 14. März 2020 (Twitter,[50] Facebook,[51] ZDF[52]):

  > ! Achtung Fake News !
  > Es wird behauptet und rasch verbreitet, das Bundesministerium für Gesundheit/die Bundesregierung würde bald massive weitere Einschränkungen des öffentlichen Lebens ankündigen. **Das stimmt NICHT!** Bitte helfen Sie mit, ihre Verbreitung zu stoppen.

  WAHR: Drei Tage später wurden die Lockdown-Maßnahmen verkündet, mit massiven Einschränkungen des öffentlichen Lebens, die ab 23. März 2020 in Deutschland in Kraft traten: Kontaktverbot, Schließung von Geschäften, Restaurants, Bars, Spielplätzen und des gesamten öffentlichen Lebens, Verbot von Reisen und Demonstrationen u. v. m.[53]

- FAKE: Das Gerede von der *Pandemie der Ungeimpften* war 2021 eine Fake-News-Kampagne von Lauterbach & Co. und die Faktenchecker bei allen Social-Media-Konzernen unterstützten dabei massiv, beispielsweise Twitter:

  > *Twitter will ban users that repeatedly claim vaccinated people can spread covid.*

  WAHR: Um die Fake-News-Kampagne mit Zahlen zu untermauern, wurden akrobatische mathematische Konstrukte bemüht. Bei der Auswertung der Infektionszahlen wurden bspw. Corona-Infizierte, deren Impfstatus nicht bekannt war, als ungeimpft gezählt. Marcus Söder twitterte im November 2021 die Fake-Statistik in Abb. 2.5, um die *Pandemie der Ungeimpften* zu beweisen.[54]

  Eine Nachfrage bei den zuständigen Behörden ergab, dass 81.782 Corona-Fälle im Beobachtungszeitraum gezählt wurden. 9.641 waren geimpft, 14.652 waren ungeimpft. Die 57.489 Fälle mit unbekanntem Impfstatus wurden als Ungeimpfte verrechnet.[55]

  Ein Jahr später lässt sich nicht mehr leugnen, dass die *Querdenker* recht hatten. Es ist Konsens, dass sich auch Geimpfte/Geboosterte mit dem Coronavirus infizieren und natürlich das Virus auch weiterverbreiten. Das RKI gibt offiziell zu, dass der Schutz der Impfung gegen eine Infektion nahe NULL liegt und es ist zweifelhaft, ob die Kosten/Nutzen-Bilanz der Impfung in der Gesamtrechnung unter Einbezug von Nebenwirkungen überhaupt noch positiv ist.[56]

[49] https://www.cnet.com/news/over-40-of-republicans-think-bill-gates-will-use-covid-19-vaccines-to-implant-microchips/
[50] https://twitter.com/bmg_bund/status/1238780849652465664
[51] https://www.facebook.com/bmg.bund/posts/1528002687362904
[52] https://www.zdf.de/nachrichten/panorama/coronavirus-deutschland-europa-usa-100.html
[53] https://www.berlin.de/corona/massnahmen/verordnung/
[54] https://twitter.com/Markus_Soeder/status/1461362183636279309
[55] https://www.welt.de/politik/deutschland/plus235442252/Fakten-zu-Inzidenzen-und-Patienten-Pandemie-der-Unwissenheit.html
[56] https://www.berliner-zeitung.de/gesundheit-oekologie/nebenwirkungen-wir-sehen-eine-absolute-risiko-erhoehung-durch-die-mrna-impfung-li.265003

Abbildung 2.5: Söders Fake-Inzidenzen für Geimpfte und Ungeimpfte im November 2021

- Zu personenbezogenen Fake News könnte man noch erwähnen, dass der GCHQ Rufmord im Internet gezielt plant und umsetzt (wahrscheinlich nicht nur der GCHQ). Zu den konkreten Methoden der JTRIG (Joint Threat Research Intelligence Group) gehört es, Personen mit Sex-Angeboten in kompromittierende Situationen zu locken, unter ihrem Namen Falschinformationen im Netz zu publizieren oder unter ihrer Identität Mails an Freunde und Kollegen zu verschicken. Eine weitere Taktik besteht darin, sich in Foren als Opfer einer Person auszugeben, die man schädigen möchte.

- Im Zeitalter von Twitter und Facebook ist es einfach, den gelangweilten Mob zu einem Shitstorm zu orchestrieren. Ein Beispiel ist Oberst Pedro Banos, der im Juni 2018 den Posten des Geheimdienstkoordinators in Spanien übernehmen sollte. Oberst Banos ist ein absoluter Experte auf dem Gebiet des islamischen Terrorismus. Er hat aber nie seine Meinung verschwiegen, dass die Politik der NATO-Staaten wesentlich mitverantwortlich dafür ist. In einer Twitter-Kampagne wurde er als *pro-russisch* abgestempelt. (Für einen NATO-Geheimdienstler der schlimmste Vorwurf.) Der Staatspräsident musste Oberst Banos wenige Tage nach der Ernennung aufgrund des Rummels wieder entlassen. General Miguel Ballesteros wurde zum neuen Geheimdienstchef ernannt, der ein Freund der NATO-Politik war. Ende 2018 wurde bekannt, dass die britische *Integrity Initiative* den Shitstorm gegen Banos orchestriert hatte.[57]

  Die Integrity Initiative ist eine britische Beeinflussungskampagne gegen Russland, deren Budget 2 Mio. Pfund jährlich beträgt (250.000 Pfund vom US-Außenministerium, 215.000 von der NATO usw.). Durch einen Leak von internen Dokumenten der Integrity Initiative wurden weitere Kampagnen in Großbritannien, Italien und Norwegen bekannt:

  - In Großbritannien wurde die bisher größte Kampagne der Integrity Initiative durchgeführt. Ziel war es, den Chef der Labour-Partei J. Corbyn zu diskreditieren. Auch Corbyn wurde als pro-russisch und als Gefahr für die Demokratie abgestempelt. Eine Analyse von ConsortiumNews[58] zeigt, dass jene namentlich in den Dokumenten genannten Journalisten, die sich an der Kampagne gegen Corbyn beteiligten, ein weiteres Ziel hatten: J. Assange.
  - In Italien folgte die Berichterstattung in den Medien über den Fall Skripal nicht dem vorgegebenen Narrativ aus GB. Der italienische Cluster der Integrity Initiative wurde aktiv, um die Berichterstattung im Mainstream auf Linie zu bringen.

[57] https://www.nachdenkseiten.de/?p=47955
[58] https://consortiumnews.com/2019/01/14/the-twitter-smearing-of-corbyn-and-assange/

  - Norwegen ist traditionell skeptischer gegenüber der US-Politik und zu wenig anti-russisch eingestellt. Norwegische Journalisten tendieren dazu, Informationen von russischer Seite die gleiche Gewichtung zuzusprechen wie Informationen aus westlichen NATO-Ländern oder den USA. Seit 2016 ist die Integrity Initative in Norwegen aktiv, um durch geeignete Maßnahmen etwas gegen diese gefährliche Starrköpfigkeit zu unternehmen.

  Für russische Medien war es *the biggest story of 2018*, in deutschen Medien habe ich mit Ausnahme von Telepolis[59] [60] [61] [62] fast nichts über die Integrity Initiative gelesen. Am gleichen Tag, als ANONYMOUS die Dokumente über den deutschen Cluster der Integrity Initiative veröffentlichte, machte der Spiegel einen Fake-News-Fall im eigenen Haus publik und alle deutschen Medien waren mit Claas Relotius[63] beschäftigt. Als am 03. Januar neue Dokumente zur Integrity Intiative veröffentlicht wurden, war in Deutschland der Promi-Leak[64] das große Ereignis, das andere Leaks überdeckte.

- Ein weiteres Phänomen im Zeitalter von Twitter und Facebook sind sogenannte *Influencer*, die sich in ihren emotional aufputschenden Berichten nur den Likes ihrer Follower verpflichtet sehen. Auf der Jagd nach mehr Likes und zur Bestätigung der vorherrschenden Meinung in der Echokammer der Follower werden oft Geschichten erfunden, die man klar in die Gruppe der Fake News einordnen kann.

  Ein typisches Beispiel dafür ist der 24-jährige Henryk Stöckl aus dem Umfeld der AfD. Auf seinen Accounts bei YouTube und Facebook veröffentlicht er emotionale, menschliche und scheinbar authentische, aber oft falsche Berichte. In Social-Media ist er zu einem der auffälligsten rechten Meinungsmacher in Deutschland geworden. Er selbst nennt sich Privat-Journalist, Kommentator, Aktivist oder Berichterstatter.

  In einem Interview mit BuzzFeed wurde er mit einigen seiner eigenen Aussagen konfrontiert und nach den Quellen gefragt. Seine Reaktion:[65]

  > *...ähm... also – ähm... ähmm... Diese Frage lassen wir mal besser aus.*

  An anderer Stelle nennt er Erzählungen von Dritten als Quelle seiner Fake News.

  Das viele seiner Berichte immer wieder als Lügen entlarvt werden, scheint seine Follower wenig zu interessieren. In den Antworten auf seine Beiträge steigern sie sich bis hin zu Mordaufrufen gegen Personen aus einem vermeintlich linken Spektrum hinein.

  Auch auf der linken Seite gibt es Spinner, die mit der massenweise Abschlachtung von Untermenschen eine neue Nazidiktatur verhindern wollen. Denken verboten?[66]

  Andere Beispiele sind falsche Politiker-Zitate, mit denen man hohe Klickraten und Likes erzielt, die aber leicht als Fake erkennbar sind, wie zum Beispiel das Zitat in Abb. 2.6

[59] https://www.heise.de/tp/features/Integrity-Initiative-Britische-Beeinflussungskampagne-gegen-Russland-4232365.html
[60] https://www.heise.de/tp/features/Infowar-oder-Absurdistan-Britisches-Aussenministerium-im-Strudel-der-Desinformation-4253994.html
[61] https://www.heise.de/tp/features/Neues-von-der-britischen-Beeinflussungskampagne-des-ominoesen-Institute-of-Statecraft-4266174.html
[62] https://www.heise.de/tp/features/Integrity-Initiative-taucht-ab-4286004.html
[63] http://www.spiegel.de/kultur/gesellschaft/fall-claas-relotius-spiegel-legt-betrug-im-eigenen-haus-offen-a-1244579.html
[64] https://www.heise.de/-4265180
[65] https://twitter.com/BuzzFeedNewsDE/status/1064538241880203264
[66] https://www.privacy-handbuch.de/diskussion.htm#08_01_19

aus dem Blog von Sven Liebich. In einem Spiegel-Interview sagte M. Schulz, dass man die Typen von der AfD bekämpfen muss, aber er sagte nichts von Lagern.[67]

Abbildung 2.6: Fake News: Falsches Zitat von M. Schulz mit hohen Klickraten

Im Gegensatz zu den Fake News, die von Medien und Journalisten verbreitet werden, sind diese Fakes leicht zu entlarven. Es wäre einfach, aus diesen Echokammern auszusteigen und von der Blindheit geheilt zu werden. Man muss es nur selbst wollen.

2.6 Geotagging

1. **Standortdaten** sind die wertvollsten Informationen für die Werbewirtschaft, um zukünftig den Markt zu vergrößern. Ein Online-Versand von Brautkleidern richtet seine Werbung an Frauen zwischen 24 und 30 Jahren, die verlobt sind. Ein Ladengeschäft stellt zusätzlich die Bedingung, dass sie sich häufig im Umkreis von xx aufhalten. Lokalisierte Werbung ist ein Markt, der durch die Verbreitung von Smartphones stark wächst.

2. Die Analyse des sozialen Umfeldes ist mit den Standortdaten ebenfalls möglich. Die Summe aller Standortdaten ist mehr als die Anhäufung der Standorte von Person A, B und C. Wie die Studie *Inferring social ties from geografic coincidences*[68] zeigt, ermöglicht diese Sammlung detaillierte Informationen über das soziale Umfeld, auch wenn man bei Facebook nicht befreundet ist. Die Standortdaten der Smartphones verraten, mit wem man regelmäßig ein Bier trinkt, mit wem man ins Bett steigt, ob man an Pegida-Demonstrationen teilnimmt oder sich in Antifa-Zirkeln trifft und vieles mehr.

3. Mit den Geofencing-Datensammlungen ist eine einfache **Überwachung** und **Einschüchterung** möglich. In der Ukraine wurden diese Daten bereits im Januar 2014 zur Einschüchterung von Demonstranten genutzt. Teilnehmer einer Demonstration gegen den damals amtierenden Präsidenten bekamen eine SMS mit dem Inhalt:

Sehr geehrter Kunde, sie sind als Teilnehmer eines Aufruhrs registriert.

[67] http://www.spiegel.de/politik/ausland/martin-schulz-ueber-afd-diese-typen-muss-man-bekaempfe-a-1078912.html
[68] http://www.pnas.org/content/107/52/22436.short

Die Firma Dataminr bietet Kunden via API Zugriff auf die Twitter-Postings und wirbt in einem Flyer am Beispiel eines Studentenprotestes in Südafrika damit, wie man das neue Geospatial Analyse Tool (Abb. 2.7) zum Monitoring von politischen Demonstrationen nutzen kann.

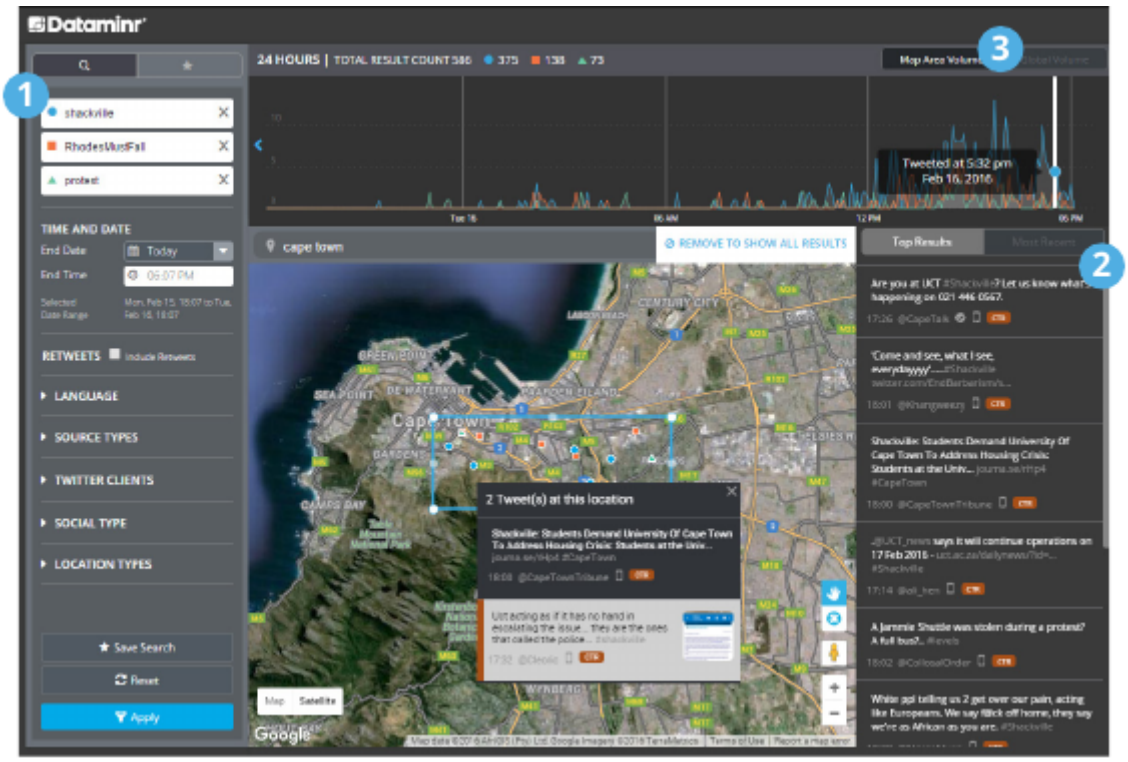


Abbildung 2.7: Auswertung der Twitter-Postings eines Studentenprotestes in Südafrika aufgrund der Geolocation der Postings

4. Die **Bewegungsanalyse** ermöglicht Aussagen über sehr private Details. Man kann z. B. durch die Analyse der Handybewegungen erkennen, ob jemand häufig als Geschäftsreisender unterwegs ist, ob man ein festes Arbeitsverhältnis hat, für welche Firma man tätig ist oder ob man arbeitslos ist. Die Firma Sense Networks ist ein Vorreiter auf dem Gebiet der Bewegungsanalyse. Im Interview mit *Technology Review* beschreibt Greg Skibiski seine Vision:

   > *Es entsteht ein fast vollständiges Modell. Mit der Beobachtung dieser Signale kann man ganze Firmen, ganze Städte, eine ganze Gesellschaft röntgen.*[69]

   Das Magazin *Wired* berichtete im Danger Room (Oktober 2011), dass das FBI Smartphones bereits seit Jahren mit der Zielstellung der „Durchleuchtung der Gesellschaft“ trackt. Muslimische Communitys werden systematisch analysiert, ohne dass die betroffenen Personen im Verdacht einer Straftat stehen. Das Geotracking von GPS-fähigen Smartphones und GPS-Modulen moderner Fahrzeuge durch das FBI erfolgt ohne richterlichen Beschluss.

   > *. . . the pushpins on the new FBI geo-maps indicate where people live, work, pray, eat and shop, not necessarily where they commit or plan crimes.*[70]

[69] https://www.heise.de/tr/artikel/Immer-im-Visier-276659.html
[70] https://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims/

Im September 2012 hat in den USA der Sixth Circuit Court of Appeals entschieden, das bezüglich Standortdaten keine Ansprüche auf Privatsphäre bestehen. Diese Entscheidung ermöglicht es US-Firmen, diese Daten hemmungslos zu sammeln. Die Dienste der USA dürfen ohne richterliche Prüfung Standortdaten von GPS-Geräten verfolgen.

Die Daten werden mit verschiedenen Methoden gesammelt:

- Hauptlieferanten für Geodaten sind Smartphones und Handys. Vor allem Apps können genutzt werden, um Geodaten zu sammeln. Über die Hälfte der in verschiedenen Stores downloadbaren Apps versenden Standortdaten unabhängig davon, ob sie für die Funktion der App nötig sind. Der Bundesdatenschutzbeauftragte erwähnt bspw. eine App, die das Smartphone zur Taschenlampe macht und dabei den Standort an den Entwickler der App sendet.

  Ein praktisches Beispiel für die Nutzung des Geotrackings ist die 2014 von Google eingeführte *Ladenbesuchsmessung*. Mit Hilfe der Android-Smartphones ermittelt Google, welche Geschäfte der Besitzer des Smartphones in der realen Welt besucht. Die Daten werden mit der Online-Werbung korreliert, die dem Besitzer am PC oder auf dem Smartphone angezeigt wurde, und sollen Werbetreibenden eine Rückmeldung darüber geben, wie erfolgreich ihre Online-Kampagnen in der realen Welt sind.

- Mit Einführung des iPhone 4 hat Apple seine Datenschutzbestimmungen geändert. Die gesamte Produktpalette von Apple (iPhones, Laptops, PCs usw.) wird in Zukunft den Standort des Nutzers laufend an Apple senden. Apple wird diese Daten Dritten zur Verfügung stellen. Wer Zugang zu diesen Daten hat, wird nicht näher spezifiziert.[71]

  Für die Datensammlungen rund um das iPhone wurde Apple mit dem BigBrother Award 2011 geehrt. Auszug aus der Laudatio von F. Rosengart und A. Bogk:

  > *Apples Firmenstrategie scheint darauf ausgelegt zu sein, möglichst viele Daten der Nutzer zu erfassen, ähnlich wie es soziale Netzwerke auch tun. Werbepartner freuen sich darauf, mit Hilfe von Apple möglichst zielgruppengerechte und standortbezogene Werbung auf dem Telefon anzeigen zu können.*

  Das chinesische Staatsfernsehen bezeichnete die Möglichkeit des Auslesens häufig besuchter Orte im iPhone als Risiko für die nationale Sicherheit,[72] da die Daten bei US-Firmen gespeichert werden, die im Rahmen von PRISM mit der NSA kooperieren.

- Millionen von Fotos werden über verschiedene Dienste im Internet veröffentlicht (Flickr, Twitter, Facebook usw.). Häufig enthalten diese Fotos in den EXIF-Attributen die GPS-Koordinaten der Aufnahme. Die Auswertung dieses Datenstromes steht erst am Anfang der Entwicklung. Ein Beispiel ist die mit Risikokapital ausgestattete Firma Heypic, die Fotos von Twitter durchsucht und auf einer Karte darstellt.

- Die ganz normale HTTP-Kommunikation liefert Standortinformationen anhand der IP-Adresse. Aktuelle Browser bieten zusätzlich eine Geolocation-API, die genauere Informationen zur Verfügung stellt. Als Facebook im Sommer 2010 die Funktion Places standardmäßig aktivierte, waren viele Nutzer überrascht, wie genau jede reale Bewegung im Sozialen Netz lokalisiert wird. Nicht nur Facebook kann das.

  Die Deaktivierung von Places scheint bei Facebook wirklich umständlich zu sein. Damit wird aber nicht die Erfassung der Daten deaktiviert, sondern nur die Sichtbarkeit für andere Nutzer!

[71] https://www.apple.com/chde/legal/privacy/
[72] https://www.heise.de/-2257924

Abbildung 2.8: Lokalisierung eines Smartphones durch Facebook

- Lokalisierungsdienste wie *Gowalla* oder *Foursquare* bieten öffentlich einsehbare Standortdaten und versuchen, durch Spiel-artigen Charakter neue Nutzer zu gewinnen. Im Gegensatz zu den oben genannten Datensammlungen kann man bei Gowalla oder Foursquare aber gut kontrollieren, welche Daten man veröffentlicht, oder die Dienste eben nicht nutzen.

Nichts zu verbergen?

Wer ein praktisches Beispiel braucht: Krankengeld gestrichen und Job verloren, weil er auf Facebook Urlaubsfotos veröffentlichte. Andreas H. litt an Depressionen. Er ging zum Arzt und wurde krankgeschrieben. Seine Ärzte rieten ihm zu einem Urlaub. Facebook-Fotos mit Surfbrett am Strand kosteten ihn erst das Krankengeld – und dann den Job.[73]

2.7 Kommunikationsanalyse

Geheimdienste verwenden seit Jahren die Kommunikationsanalyse (wer mit wem kommuniziert), um die Struktur von Organisationen aufzudecken. Damit gelingt es, automatisiert umfangreiche Informationen zu beschaffen, ohne die Verschlüsselung von Inhalten der Kommunikation knacken zu müssen.

> *Auch ohne Kenntnis der Gesprächs- oder Nachrichteninhalte – die nur durch Hineinhören zu erlangen wäre – lässt sich allein aus dem zeitlichen Kontext und der Reihenfolge des Kommunikationsflusses eine hohe Informationsgüte extrahieren, nahezu vollautomatisch.* (Frank Rieger)

Die Verwendung der Daten demonstriert das **Projekt Gegenwirken** der niederländischen Geheimdienste. In regierungskritischen Organisationen werden die Aktivisten identifiziert, deren Engagement für die Gruppe wesentlich ist. Für die Kommunikationsanalyse nötige Daten werden dabei u. a. systematisch mit illegalen Zugriffen gewonnen. Die identifizierten Aktivisten werden mit kleinen Schikanen beschäftigt, um die Arbeit der Gruppe zu schwächen. Das Spektrum reicht von ständigen Steuerprüfungen bis zu Hausdurchsuchungen bei harmlosen Bagatelldelikten.

Im Rahmen der Vorratsdatenspeicherung (VDS) werden genau die Datenbestände angelegt, die den Geheimdiensten und dem BKA eine umfassende Kommunikationsanalyse ermöglichen. Zur Kriminalitätsbekämpfung und -prävention taugt die Vorratsdatenspeicherung nicht, wie ein Vergleich der Kriminalitätsstatistik des BKA für die Jahre 2007, 2008, 2009 und 2010 zeigt.

[73] https://www.apotheke-adhoc.de/nachrichten/detail/pta-live/urlaub-trotz-krankengeld/

Zivile Kommunikationsanalyse

Zunehmend wird auch im zivilen Bereich diese Analyse eingesetzt. Das Ziel ist es, Meinungsmacher und kreative Köpfe in Gruppen zu identifizieren, gezielt mit Werbung anzusprechen und sie zu manipulieren. Im Gegensatz zu den Diensten haben Unternehmen meist keinen Zugriff auf Verbindungsdaten von Telefon und Mail. Es werden öffentlich zugängliche Daten gesammelt. Facebook und Twitter sowie Kommentare in Blogs und Foren bieten einen umfangreichen Datenpool. Teilweise werden von Unternehmen gezielt Blogs und Foren zu bestimmten Themen aufgesetzt, um Daten zu generieren.

Wie man die Freundschaftsbeziehungen in sozialen Netzen wie Facebook analysieren kann, um homosexuelle Orientierung zu erkennen, haben ehemalige Studenten des MIT mit *Gaydar – die Schwulenfalle* demonstriert. Die TU Berlin hat zusammen mit der Wirtschaftsuniversität Wien erfolgversprechende Ergebnisse zur *Rasterfahndung nach Meinungsmachern* veröffentlicht.

Ein Beispiel

Kommunikationsanalyse ist ein abstrakter Begriff. Anhand eines stark vereinfachten Beispiels soll eine Einführung erfolgen, ohne den Stand der Forschung zu präsentieren. Das Beispiel zeigt die Analyse einer subversiven Gruppe auf Basis einer Auswertung der Kommunikationsdaten von wenigen Mitgliedern. Die Kommunikationsdaten können aus verschiedenen Kanälen gewonnen werden: Telefon, E-Mail, Briefe, Instant-Messaging, Soziale Netze usw.

Als Beispiel nehmen wir eine Gruppe mit dem Namen *Muppet Group*, abgekürzt *mg*. Als Ausgangslage ist bekannt, dass *Anton* und *Beatrice* zur *mg* gehören.

Durch Auswertung aller zur Verfügung stehenden Kommunikationsdaten von *Anton* und *Beatrice* erhält man ein umfangreiches Netz ihrer sozialen Kontakte (Abb. 2.9). Dabei wird nicht nur die Anzahl der Kommunikationsprozesse ausgewertet, sondern auch die zeitliche Korrelation einbezogen.

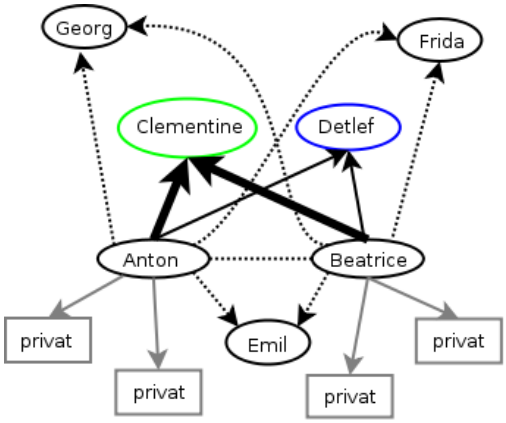


Abbildung 2.9: Soziales Netz von Anton und Beatrice

Besonders häufig haben beide (zeitlich korreliert) Kontakt zu *Clementine* und *Detlef*. Diese beiden Personen scheinen eine wesentliche Rolle innerhalb der Gruppe *mg* zu spielen. Einige Personen können als offensichtlich privat aus der weiteren Analyse entfernt werden, da nur einer von beiden Kontakt hält und keine zeitlichen Korrelationen erkennbar sind.

Ideal wäre es, an dieser Stelle die Kommunikation von *Clementine* und *Detlef* näher zu untersuchen. Beide sind aber vorsichtig und es besteht kein umfassender Zugriff auf die Kommunikationsdaten. Dann nimmt man als Ersatz vielleicht *Frida*, um das Modell zu präzisieren.

Frida unterhält vor allem einen engen Kontakt zu *Detlef*, was zu einer Umbewertung der Positionen von *Detlef* und *Clementine* führt (Abb. 2.10). Bei *Emil* handelt es sich evtl. um einen zufällig gemeinsamen Bekannten von *Anton* und *Beatrice*, der nicht in die *mg* eingebunden ist.

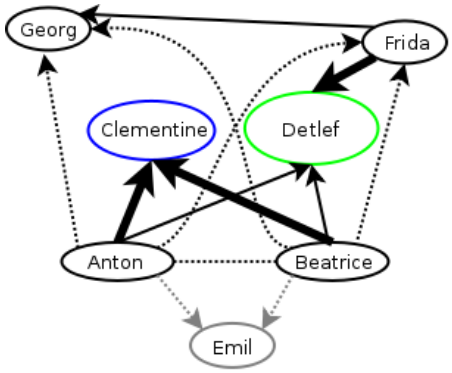


Abbildung 2.10: Präzisierte Struktur der „mg“

Reale Datenmmengen

Reale Kommunikationsnetzwerke sind wesentlich komplexer. Auf Grundlage der Daten, die von T-Mobile über den Politiker Malte Spitz gespeichert wurden, hat Michael Kreil von OpenDataCity die Grafik in Abb. 2.11 mit den Rohdaten erstellt.

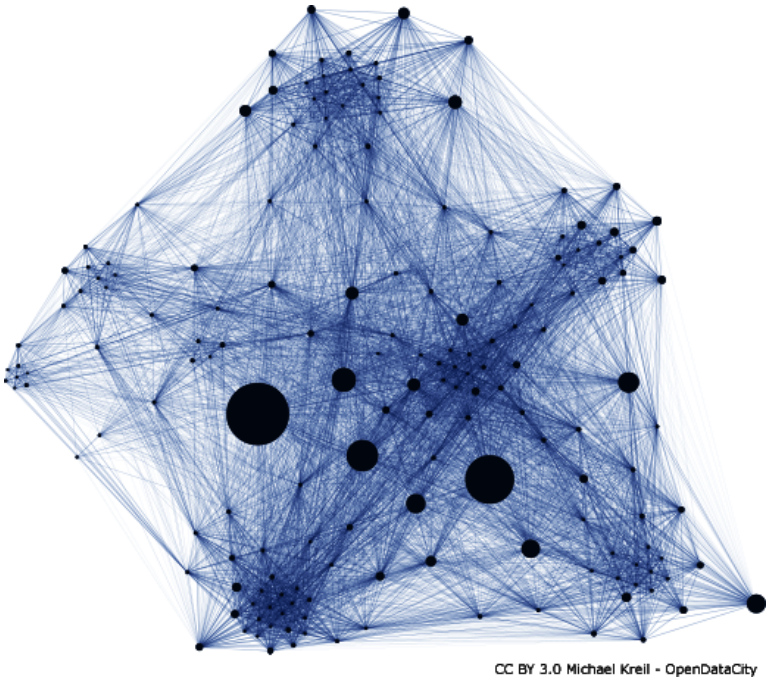


Abbildung 2.11: Kommunikationsnetzwerk von Malte Spitz

Etwas besser aufbereitete Daten visualisiert Abb. 2.12 mit den Kommunikationsdaten einer Woche von Ton Siedsmas.

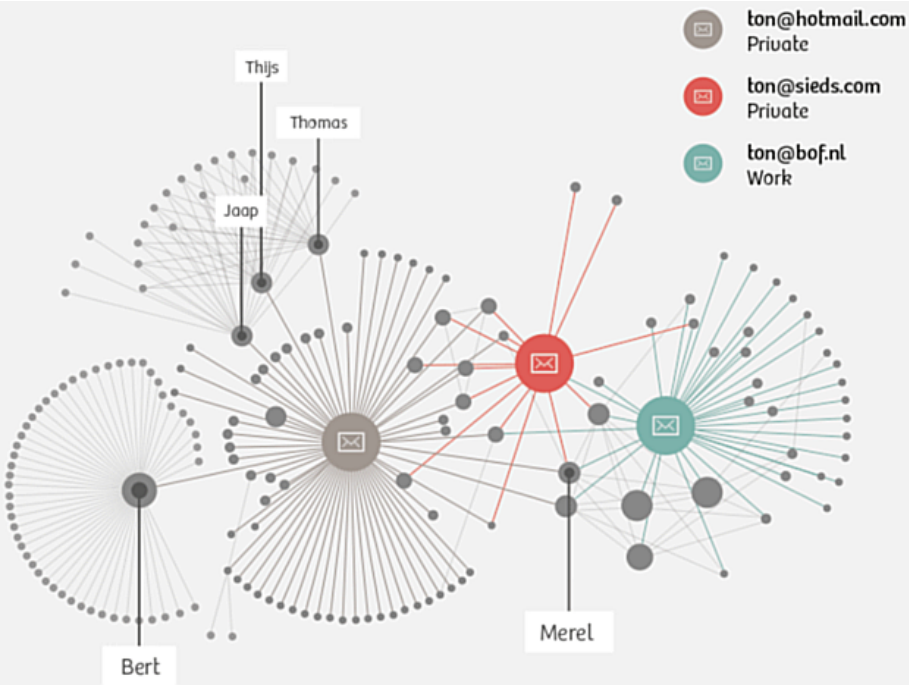


Abbildung 2.12: Aufbereitete Kommunikationsdaten von Ton Siedsmas

Wenn man auch die Standortdaten des Smartphones auswerten kann, werden die Informationen deutlich detaillierter. Abbildung 2.13 zeigt einen Tag von Ton Siedsmas.

Analysetools wie *i2 Analyst's Notebook* von IBM oder *rola rsCASE* können diese Daten hübsch aufbereiten und die Schlapphüte bei der Analyse effektiv unterstützen (Abb. 2.14).

2.8 Überwachungen im Internet

Eine umfassendere Übersicht zu verschiedenen Sicherheitsgesetzen der Jahre bis 2017 bietet www.daten-speicherung.de. Sehr schön erkennbar ist das Muster der Zustimmung durch die jeweiligen Regierungsparteien und meist Ablehnung durch die Opposition, von Böswilligen als Demokratie-Simulation bezeichnet. Unabhängig vom Wahlergebnis wird durch die jeweiligen Regierungsparteien die Überwachung ausgebaut.[74]

Identifizierungspflicht für nummernunabhängige Dienste Für Messenger, E-Mail-Provider und ähnliche Dienste, die unabhängig von der Telefonnummer nutzbar sind, soll eine Identifizierungspflicht der Nutzer eingeführt werden. Die Provider sollen Namen, Geburtsdatum und Adressen der Nutzer erfassen, verifizieren und den Behörden auf Abruf im Rahmen der Bestandsdatenauskunft zur Verfügung stellen.

Im Unterschied zum Klarnamen-Zwang können die Dienste weiterhin mit einem Pseudonym genutzt werden, aber die realen Identitäten hinter den Pseudonymen müssen der Strafverfolgung und Geheimdiensten zur Verfügung gestellt werden.

[74] https://www.daten-speicherung.de/index.php/ueberwachungsgesetze/

Abbildung 2.13: Standortdaten eines Tages von T. Siedsmas

- Auf der Innenministerkonferenz im Juni 2020 wurde diese Forderung mit der Notwendigkeit der Verfolgung von Kinderpornografie begründet.
- Die SPD nahm die Identifizierungspflicht für nummernunabhängige Dienste in den Entwurf des Wahlprogramms für die Bundestagswahl 2021 auf, um als möglicher Juniorpartner Bereitschaft zur Umsetzung weiterer Überwachungen zu signalisieren.
- Das Bundesinnenministerium unter H. Seehofer versuchte, die Identifizierungspflicht für E-Mail- und Messenger-Provider in der aktualisierten TKG-Novelle zu platzieren. Mit dem Vorschlag zur Novellierung des TKG vom Dezember 2020 sollten auch Over-the-Top-Dienste wie Messenger und E-Mail als TK-Dienste klassifiziert werden. Das würde diese Dienste zur TKÜ bei schweren Straftaten und außerdem zur Unterstützung beim Rollout von Trojanern zur Quellen-TKÜ und Online-Durchsuchung verpflichten.

Vorratsdatenspeicherung: (Neusprech: *Daten-Mindestspeicherfrist* oder ganz neu: *private Vorsorgespeicherung*)

Ohne jeglichen Verdacht sollen die Verbindungsdaten jeder E-Mail, jedes Telefonats, jeder SMS und Standortdaten der Handys gesammelt werden. Die Versuche zur Einführung sind nicht neu. Seit mehr als 18 Jahren versuchen unterschiedliche Regierungen, diese Überwachungsmaßnahme einzuführen, ohne die Notwendigkeit für die Strafverfolgung begründen zu können. Nutznießer sind in erster Linie die Geheimdienste.

- 1997 wurde die Vorratsdatenspeicherung aufgrund verfassungsrechtlicher Bedenken abgelehnt.
- 2002 wurde ein ähnlicher Gesetzentwurf vom Deutschen Bundestag abgelehnt und die Bundesregierung beauftragt, gegen einen entsprechenden Rahmenbeschluss auf EU-Ebene zu stimmen (Bundestag-Drucksache 14/9801).
- 2005 beschloss das EU-Parlament mit Mehrheit der christ- und sozialdemokratischen Fraktionen die Richtlinie zur sechsmonatigen Datenspeicherung der Verbindungs- und Standortdaten (VDS) (Directive 2006/24/EG). Um die Richtlinie mit einfacher Mehrheit in der EU-Kommission ohne Mitsprache des Parlamentes verabschieden zu können, wurde sie nicht als Sicherheits- und Polizeimaßnahme behandelt. Stattdessen

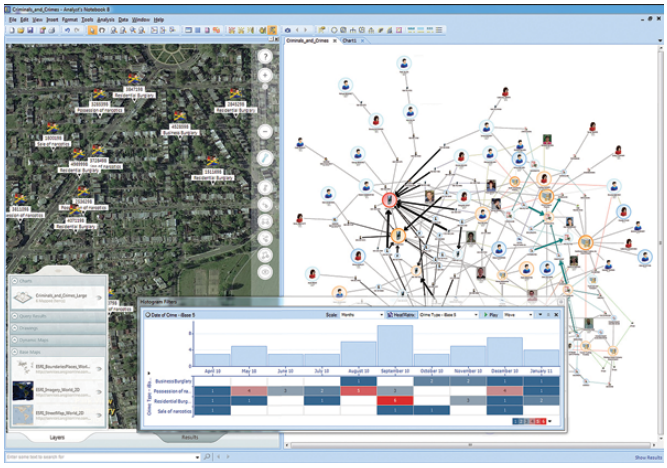


Abbildung 2.14: Screenshot von *i2 Analyst's Notebook* (IBM)

wurde sie als Maßnahme zur *Regulierung des Binnenmarktes* definiert, was außerdem die EU-Länder zu einer Umsetzung zwingt.

- 2006 legte der Wissenschaftliche Dienst des Bundestages ein Rechtsgutachten mit schweren Bedenken gegen die VDS vor.
- Ein Vergleich der Zahlen der Kriminalitätsstatistik des BKA für die Jahre 2007, 2008 und 2009 zeigt, dass die VDS im Jahr 2009 nicht zur einer Verbesserung der Aufklärungsrate von Straftaten im Internet führte und keinen Einfluss auf die Tendenz der Entwicklung hatte. Es gibt mehr Straftaten im Internet bei abnehmender Aufklärungsrate.

-	2008	2009	2010
-	(o. VDS)	(**mit VDS**)	(o. VDS)
Straftaten im Internet	167.451	206.909	223.642
Aufklärungsrate (Internet)	79.8 %	75.7 %	72,3 %

- 2010 erklärte das Bundesverfassungsgericht in einem Grundsatzurteil das Gesetz zur VDS als nicht vereinbar mit dem Grundgesetz (Az: 1 BvR 256/08).[75]
- 2012 zeigte das Max-Planck-Institut (MPI) für ausländisches und internationales Strafrecht in einer umfangreichen wissenschaftlichen Analyse, dass KEINE *Schutzlücke* ohne Vorratsdatenspeicherung besteht. Damit widersprach das Institut der Darstellung mehrerer Bundesinnenminister und des BKA-Chef Ziercke, wonach die VDS für die Kriminalitätsbekämpfung unbedingt nötig sei. Die in der Presse immer wieder herangezogenen Einzelbeispiele halten einer wissenschaftlichen Analyse nicht stand.[76]
- 2012 gab es einen erfolglosen Anlauf, die VDS international im Rahmen der UNODC als verpflichtende Richtlinie zu etablieren. Der Verfassungsschutz unterstützte diesen Versuch offensiv.
- 2014 wurde die Richtlinie 2006/24/EG vom EuGH als nicht vereinbar mit der Charta der Grundrechte der Europäischen Union gekippt (Urteil C-293/12 und C-594/12).
- 2015 wurde im Eilverfahren ein neues Gesetz zur *Speicherpflicht für Verkehrsdaten* verabschiedet. Bundesjustizminister H. Maas konnte auf der Pressekonferenz zur

[75] http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html

[76] https://www.ccc.de/de/updates/2012/mythos-schutzluecke

Verabschiedung des Gesetzentwurfes im Bundeskabinett auf Nachfrage keinen Grund nennen, warum die Vorratsdatenspeicherung notwendig sein soll:

> Frage: *Kann der Minister die Notwendigkeit der Vorratsdatenspeicherung beweisen (was eine Voraussetzung für Grundrechtseingriffe wäre)?*
> Antwort H. Maas: *Die Notwendigkeit kann ich nicht beweisen.*

Für die Bundesdatenschutzbeauftragte A. Voßhoff ist die VDS verfassungswidrig und widerspricht Urteilen von BVerfG und EuGH. Der ehemalige Bundesdatenschutzbeauftragte P. Schaar kommentierte:

> *Brauchen wir das überhaupt? Die Bundesregierung bleibt den Nachweis schuldig, dass dieser erhebliche Grundrechtseingriff unerlässlich ist.*

- Am 16.10.2015 beschloss der Bundestag erneut das neue Gesetz zur Vorratsdatenspeicherung. Verfassungsklagen wurden inzwischen eingereicht.
- 2017 legte der Wissenschaftliche Dienst zum wiederholten Mal ein Gutachten zur Vorratsdatenspeicherung vor, das zu dem Schluss kommt, dass das aktuelle Gesetz nicht mit geltendem EU-Recht vereinbar ist. In mehreren Punkten verstößt das Gesetz gegen die Vorgaben des Europäischen Gerichtshofes.

Warum bemüht man sich seit Jahren, eine Überwachungsmaßnahme einzuführen, die uns einige hundert Millionen Euro kosten wird, so gut wie keinen Beitrag zur Verbesserung der Strafverfolgung bietet und in erster Linie den Geheimdiensten (Neusprech: *Gefahrenabwehrdiensten*) neue Kompetenzen verschaffen wird?

Bestandsdatenauskunft Der IT-Sicherheitsforscher Pete Swire veröffentlichte im April 2012 ein Paper,[77] in dem er die aktuellen Tendenzen in der Überwachung aufzeigt. Weil das *Lauschen am Draht* in allen Variationen zunehmend ineffektiv wird, wollen Geheimdienste und Strafverfolger Zugriff auf die *Daten in der Cloud*. Dazu zählen auch E-Mail-Accounts. Die Hürden für den Zugriff sollen dabei gering sein.

Mit der Reform der Telekommunikationsüberwachung im Dezember 2012 kam der Gesetzgeber den Wünschen der Geheimdienste weit entgegen. Die Cloud- und Mail-Provider sollten automatisiert nutzbare Schnittstellen für die Abfrage von Bestandsdaten bereitstellen. Zu den Bestandsdaten zählen seit Dezember 2012 neben Name und Anschrift usw. auch folgende Daten, die im Gegensatz zu den allgemeinen Bestandsdaten aber nur mit Richtervorbehalt abgefragt werden sollen:

- Passworte für den Zugriff auf E-Mail-Konten und Cloud-Speicher;
- PINs zum Entsperren von Smartphones;
- Zugriff auf die Endgeräte (Router), die den Kunden vom DLS-Provider kostenlos bereitgestellt werden (TR-069 Schnittstelle).

Die PiratenPartei kommentierte den Gesetzentwurf kurz und bündig:

> *Der Entwurf der Bundesregierung ist schlicht verfassungswidrig.*

Zensur im Internet: Die Zensur sollte in Deutschland im Namen des Kampfes gegen Kinderpornografie im Internet eingeführt werden. Man wurde nicht müde zu behaupten, es gebe einen Millionen Euro schweren Massenmarkt, der durch Sperren von Webseiten empfindlich ausgetrocknet werden könne. Die Aussagen wurden geprüft und für falsch befunden.[78]

[77] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038871
[78] http://blog.odem.org/2009/05/quellenanalyse.html

1. In der ersten Stufe unterzeichneten im Frühjahr 2009 die fünf großen Provider freiwillig einen geheimen Vertrag mit dem BKA. Sie verpflichteten sich, eine Liste von Webseiten zu sperren, die vom BKA ohne nennenswerte Kontrolle erstellt werden sollte.
2. In der zweiten Stufe wurde am 18.06.09 das *Zugangserschwernisgesetz* verabschiedet. Alle Provider mit mehr als 10.000 Kunden sollten diese geheime Liste von Websites sperren. Neben den (ungeeigneten) DNS-Sperren sollten auch IP-Sperren und Filterung der Inhalte zum Einsatz kommen.
3. Die CDU/FDP-Regierung ging im Herbst 2009 einen halben Schritt zurück und schob mit einem Anwendungserlass die Umsetzung des Gesetzes für ein Jahr auf. Diese Regierung meinte also, über dem Parlament zu stehen und ein beschlossenes Gesetz nicht umsetzen zu müssen.
4. Im Rahmen der Evaluierung des Gesetzes ging das BKA nur halbherzig gegen dokumentierten Missbrauch vor, wie eine Veröffentlichung der AK-Zensur zeigte. Gleichzeitig wurde weiter Lobbyarbeit für das Zensurgesetz betrieben.[79]
5. Die Auswertung des eco-Verbands zeigt, dass Webseiten mit dokumentiertem Missbrauch effektiv gelöscht werden können. 2010 wurden 99,4 % der gemeldeten Webseiten gelöscht.[80] Auch 2011 und 2012 konnte das BKA 99 % aller gemeldeten KiPo-Webseiten löschen lassen. Warum also die Internet-Stoppschilder?
6. Im Herbst 2011 wurde das Gesetz offiziell beerdigt.

Der Aufbau einer Infrastruktur für Zensur im Internet wird auf vielen Wegen betrieben. Neben dem Popanz *Kinderpornografie* engagiert sich die Content-Mafia im Rahmen der geheimen ACTA-Verhandlungen für eine verbindliche Verpflichtung zum Aufbau der Infrastruktur für Websperren. Die CDU/CSU Bundestagsfraktion sieht die amerikanischen Gesetzesvorlagen SOPA und PIPA als richtungsweisend an. Beide Gesetzesvorlagen sehen umfangreiche Zensurmaßnahmen zum Schutz geistigen Eigentums vor.

Die verfassungsrechtlichen Bedenken gegen die Zensur hat der Wissenschaftliche Dienst des Bundestages in einem Gutachten zusammengefasst. Auch eine Abschätzung der EU-Kommission kommt zu dem Schluss, dass diese Sperrmaßnahmen **notwendigerweise eine Einschränkung der Menschenrechte voraussetzen**, beispielsweise der freien Meinungsäußerung.

BKA Gesetz: Mit dem BKA-Gesetz wurde eine Polizei mit den Kompetenzen eines Geheimdienstes geschaffen. Zu diesen Kompetenzen gehören neben der heimlichen Online-Durchsuchung von Computern der Lauschangriff außerhalb und innerhalb der Wohnung (incl. Video), Raster- und Schleierfahndung, weitgehende Abhörbefugnisse, Einsatz von V-Leuten, verdeckten Ermittlern, informellen Mitarbeitern usw.

Im Rahmen präventiver Ermittlungen (d. h. ohne konkreten Tatverdacht) soll das BKA die Berechtigung erhalten, in eigener Regie zu handeln und Abhörmaßnahmen auch auf Geistliche, Abgeordnete, Journalisten und Strafverteidiger auszudehnen. Im Rahmen dieser Vorfeldermittlungen unterliegt das BKA nicht der Leitungsbefugnis der Staatsanwaltschaft.

Damit wird sich das BKA bis zu einem gewissen Grad jeglicher Kontrolle, der justiziellen und erst recht der parlamentarischen, entziehen können.[81]

Telekommunikationsüberwachungsverordnung Auf richterliche Anordnung wird eine Kopie der gesamten Kommunikation an Strafverfolgungsbehörden weitergeleitet. Dieser Eingriff

[79] http://ak-zensur.de/2010/08/kapitulation.html
[80] http://www.eco.de/verband/202_8727.htm
[81] http://www.berlinonline.de/berliner-zeitung/print/politik/725127.html

in das verfassungsmäßig garantierte Recht auf unbeobachtete Kommunikation ist nicht nur bei Verdacht schwerer Verbrechen möglich, sondern auch bei einigen mit Geldstrafe bewährten Vergehen und sogar bei Fahrlässigkeitsdelikten (siehe §100a StPO).

Laut Gesetz kann die Überwachung auch ohne richterliche Genehmigung begonnen werden. Sie ist jedoch spätestens nach drei Tagen einzustellen, wenn bis dahin keine richterliche Genehmigung vorliegt.

Präventiv-polizeiliche Telekommunikationsüberwachung ermöglicht es den Strafverfolgungsbehörden der Länder Bayern, Thüringen, Niedersachsen, Hessen und Rheinland-Pfalz, den Telefon- und E-Mail-Verkehr von Menschen mitzuschneiden, die keiner(!) Straftat verdächtigt werden. Es reicht aus, in der Nähe eines Verdächtigten zu wohnen oder möglicherweise in Kontakt mit ihm zu stehen.

Die Anzahl der von dieser Maßnahme Betroffenen verdoppelt sich Jahr für Jahr. Gleichzeitig führen nur 17 % der Überwachungen zu Ergebnissen im Rahmen der Ermittlungen.

§129a StGB Auf Basis des §129a StGB (Bildung einer terroristischen Vereinigung) wurden in den letzten Jahren so gut wie keine Verurteilungen ausgesprochen. Die sehr weit gehenden Befugnisse für Ermittlungen nach diesem Paragraphen wurden jedoch mehrfach genutzt, um politische Aktivisten auszuforschen. Mehrfach haben verschiedene Gerichte die Anwendung des §129a StGB durch Ermittlungsbehörden für illegal erklärt.

- Doppeleinstellung in Sachen §129.[82]
- Razzien im Vorfeld des G8-Gipfels waren rechtswidrig.[83]
- Konstruieren und Schnüffeln mit §129a.[84]
- Durchsuchungen beim LabourNet waren rechtswidrig.[85]

Dieser Missbrauch der Anti-Terror-Befugnisse sollte gestoppt und evaluiert werden.

Datenbanken: Begleitet werden diese Polizei-Gesetze vom Aufbau umfangreicher staatlicher Datensammlungen. Von der Schwarzen Liste der Ausländerfreunde (Einlader-Datei) bis zur Antiterrordatei, die bereits 20.000 Personen enthält, obwohl es in Deutschland keinen Terroranschlag gibt. (Abgesehen von den Muppets aus dem Sauerland, deren Islamische Jihad-Union offensichtlich eine Erfindung der Geheimdienste ist.)

Elektronischer PA: Mit dem Elektronischen Personalausweis wird die biometrische Voll-Erfassung der Bevölkerung vorangetrieben. Außerdem werden die Grundlagen für eine eindeutige Identifizierung im Internet gelegt, begleitet von fragwürdigen Projekten wie De-Mail.

2.9 Terrorismus und der Ausbau der Überwachung

Nach den Anschlägen von Paris im November 2015 eskalierte der Ausbau der Überwachung und wird als die angeblich einzige Alternative zum Schutz der Bevölkerung diskutiert. Die EU erlaubte Frankreich sogar die Verletzung der Euro-Stabilitätskriterien,[86] weil durch den

[82] http://de.indymedia.org/2008/10/228421.shtml
[83] http://www.ag-friedensforschung.de/themen/Globalisierung/g8-2007/bgh.html
[84] http://www.neues-deutschland.de/artikel/175230.konstruieren-und-schnueffeln-mit-s-129a.html
[85] http://www.labournet.de/ueberuns/beschlagnahme/index.html
[86] http://www.faz.net/aktuell/wirtschaft/haushaltspolitik-schutz-der-buerger-wichtiger-als-defizitziele-13917723.html

notwendigen(?) Ausbau des Überwachungsapparates nach den Anschlägen außergewöhnliche finanzielle Belastungen entstanden. Die Medien schockierten uns mit einem einzelnen Ereignis. Wenn man Zeit und etwas Ruhe zum Nachdenken findet, dann relativiert sich der Schock.

Jemand hat die Toten durch Terroranschläge in Europa in den letzten Jahrzehnten aufgeschlüsselt. Die Grafik 2.15 auf Basis der Daten der *Global Terrorism Database*[87] zeigt, dass Europa hinsichtlich Terrorgefahr noch nie so sicher war wie heute.

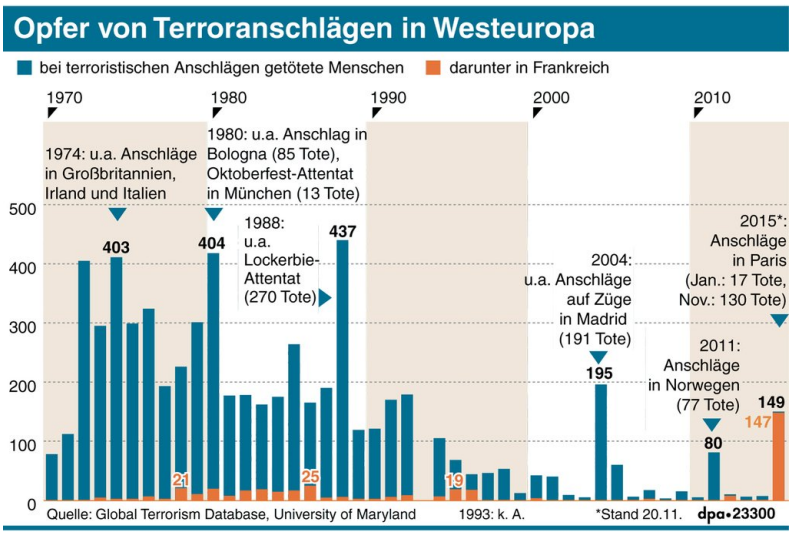


Abbildung 2.15: Opfer von Terroranschlägen in Westeuropa

Die jährlichen *EU Terrorism Reports* von Europol zeigen das gleiche Bild. In den Jahren 2005/2006 gab es fast 500 Terroranschläge pro Jahr in Europa, also mehr als einen Anschlag pro Tag und mehr als 700 Verhaftungen (siehe: TE-SAT Report für 2006.[88]) Hauptverantwortlich waren die ETA, die IRA und die italienischen Korsen. In dieser Zeit wurde ein Anschlag mit 191 Toten in Madrid zwar zur Kenntnis genommen, ein bisschen diskutiert und am nächsten Tag wieder vergessen.

Bis 2010 konnte durch politische Maßnahmen die Zahl der Terroranschläge im Vergleich zu 2006 halbiert werden, es gab nur noch 246 Anschläge.[89] Der Europol-Bericht TE-SAT 2014 listet noch 152 Terroranschläge mit sieben Toten auf, der niedrigste Stand.[90]

2015 wurde wieder ein Anstieg bei Terroranschlägen verzeichnet (insgesamt 211 Anschläge). Während sich linke und separatistische Anschläge weiter verringerten (nur noch 65), kam es zu einer Zunahme von dschihadistischen Anschlägen, vor allem in Frankreich. Dabei starben 148 Personen, da dschihadistische Selbstmordattentäter eine möglichst hohe Zahl von Todesopfern erzielen wollen. 687 potentielle islamistische Attentäter wurden verhaftet, davon wurden 98 % verurteilt.[91]

Von 2014 bis 2017 gab es in Europa 13 islamistische Anschläge von 24 Tätern. Alle Täter waren den Sicherheitsbehörden bekannt und als *gewaltbereite Gefährder* eingestuft. In 21–23 Fällen gab es außerdem eine Warnung von ausländischen Geheimdiensten.

[87] http://www.start.umd.edu/gtd/
[88] https://www.europol.europa.eu/sites/default/files/publications/tesat2007.pdf
[89] https://www.counterextremism.org/resources/details/id/229
[90] https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014
[91] https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014

In Deutschland gab es einen Anschlag in diesem Kontext: Der Terrorist Anis Amri fuhr im Dezember 2016 mit einem LKW in den Berliner Weihnachtsmarkt. Auch dieser Terrorist war den Sicherheitsbehörden bekannt. Er war in den Wochen vor dem Anschlag das Top-1-Thema der deutschen Terrorabwehr. Das BKA und der Verfassungsschutz waren über die Gefahr informiert, der marokkanische Geheimdienst hatte gewarnt und trotzdem ... [92]

Als Konsequenz aus dem Anschlag forderten Bundesinnenminister Thomas de Maizière (CDU) und andere Politiker reflexartig einen Ausbau der Überwachung. Insbesondere die Videoüberwachung stand auf der Wunschliste. C. Ströbele, ehemaliges Mitglied des Bundestages und der PKGr, zieht andere Konsequenzen aus dem Fall Amri:[93]

Wir können doch nicht dieselben Leute weitermachen lassen, die so versagt haben.

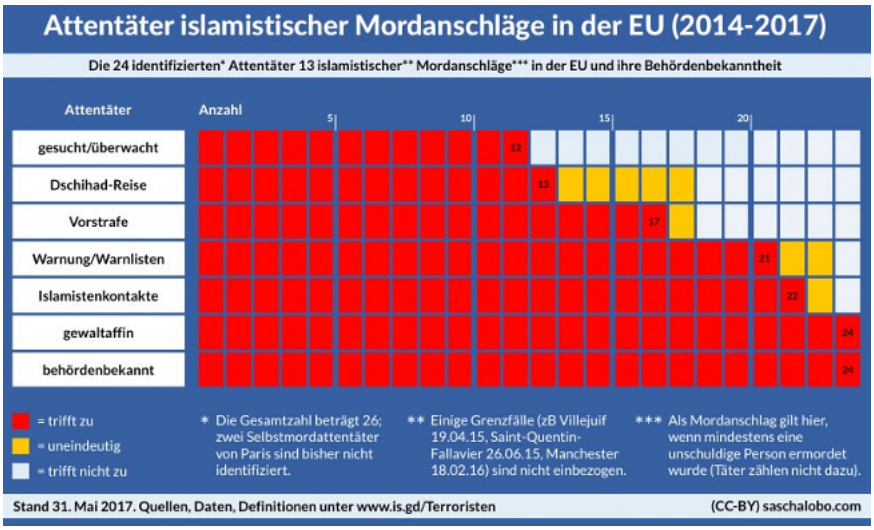


Abbildung 2.16: Alle 24 Terroristen mit islamistischem Hintergrund waren vor den Anschlägen als gewaltbereite Gefährder bekannt

Im Jahr 2019 gab es in Europa insgesamt drei erfolgreiche Terroranschläge mit dschihadistischem Hintergrund sowie einen rechtsextremen Terrorangriff. Zehn Personen starben dabei. Gegenüber den Vorjahren (2018: 7 Anschläge) und 2017 (10 Anschläge) ein Rückgang. In Europa wurden 1.004 Terroristen verhaftet. Dazu waren 115 geplante Terrorangriffe nicht erfolgreich und wurden verhindert. In Deutschland wurden drei Anschläge verhindert und 35 potentielle Terroristen verhaftet, davon 32 mit dschihadistischem Hintergrund.

Im Sommer 2020 wurden österreichische Sicherheitsbehörden vom slowakischen Geheimdienst informiert, dass ein vorbestrafter islamistischer Terrorist Munition kaufen wollte. Die Person hatte in Syrien gegen Assad gekämpft und war wegen der *Beteiligung an Terrorismus* zu einer Gefängnisstrafe verurteilt worden. Aufgrund erfolgreicher Teilnahme an einem De-Radikalisierungsprogramm wurde er vorzeitig aus der Haft entlassen. Die österreichischen Sicherheitsbehörden unternahmen nichts – bis der Terrorist im November 2020 ballernd durch Wien lief und mehrere Menschen tötete. Ein WEGA-Team (Wiener Sondereinheit) konnte den Attentäter nach neun Minuten außer Gefecht setzen.

Die Terrorgefahr in Europa wurde im letzten Jahrzehnt nicht durch den Ausbau der Überwachung reduziert, sondern durch einen politischen Integrationsprozess der separatistischen Gruppen.

[92] https://www.heise.de/tp/features/Amri-TOP-1-der-Terrorabwehr-3914967.html
[93] https://deutsch.rt.com/inland/61697-neue-vorwurfe-im-fall-amri-us-interessen/

Warum wird dieses erfolgreiche Konzept jetzt nicht mehr diskutiert? Dass Frankreich und Belgien auf diesem Gebiet der Integration massive Defizite haben, ist seit Jahren bekannt. Der vom französischen Präsidenten Hollande ausgerufenen *Krieg gegen den Islamismus* ist keine Lösung, auch nicht mit 5.000 Mann mehr Personal für die Dienste.

Eine wesentliche Rolle bei der Wahrnehmung von Terror spielen die Medien. Neben den redaktionell betreuten Medien wie die Mainstream-Presse und den qualitativ guten Blogs (bzw. alternativen Medien) haben sich Twitter und Facebook als sogenannte **Panik-Medien** etabliert. Schockierende Ereignisse verbreiten sich über diese Medien viral und schnell. Die etablierten, journalistischen Medien geraten unter Druck und müssen darauf reagieren. Neben dem *Terror* gab es in der Vergangenheit weitere Beispiele von Panikattacken wie *Schweinegrippe* oder *Ebola*. Das 700.000 Kinder in der Sahel-Zone verhungern, interessierte dagegen kaum jemanden.

Manchmal bin ich schockiert, wie stark die emotionale Wirkung der Panik-Medien geworden ist. Eine Mutter sprach einige Tage nach dem Anschlag in Paris in privater Runde über die Angst, dass ihre 17-jährige Tochter einem Terroranschlag zum Opfer fallen könnte, wenn sie abends allein in Berlin unterwegs ist. Ähmm – also ich würde eher auf Autounfall oder Unfall mit dem Fahrrad tippen, diese Gefahr ist unverändert hoch. Das Fahrrad vom Töchterchen hatte nämlich kein funktionierendes Rücklicht.

Die neuen Terroristen haben gelernt, die Panik-Medien immer besser für ihre Interessen zu nutzen. Auch die Apologeten der Überwachung nutzen die resultierende Angst für ihre eigenen Interessen und nicht für die Bekämpfung des Terrorismus. Der Schock durch die Anschläge wurde von der deutschen Regierung genutzt, um den bereits geplanten Ausbau der Geheimdienste um 475 Mitarbeiter anzukündigen. Noch nie war die Manipulation der Emotionen so stark und großflächig wie heute. *Der moderne Krieg ist kein Krieg um Territorien, sondern ein Krieg um die Köpfe.* Dieser Satz stammt aus der aktuellen Überarbeitung der NATO-Doktrin, er trifft aber auch beim Kampf gegen Terror zu.

Militärische Aktionen und geheimdienstliche Eskalation in den Überwachungsstaat sind keine Lösungen. Menschlichkeit und Integration sind Mittel, um Terror zu bekämpfen. In der globalen Politik müsste man jene konsequent ächten, die Terrorismus als Mittel zur Durchsetzung eigener Interessen fördern und anwenden. Die Grafik 2.17 zeigt die Länder, die seit 2010 Geld zur Finanzierung von Terrorismus bereitgestellt haben.

Ein konsequenter, politischer Druck auf Saudi-Arabien (der größte Finanzier des ISIS), die USA und die Türkei könnte im Kampf gegen Terrorismus mehr erreichen als alle Bomben zusammen. Das wird aber nicht diskutiert. Stattdessen werden die wirtschaftlichen Sanktionen gegen Syrien, Russland und den Iran aufrechterhalten.

Auch Frankreich ist seit Jahrzehnten als Förderer von staatlichem Terrorismus bekannt. In afrikanischen Ländern hat das Land mehrere blutige Putsche organisiert, weil die gewählten Regierungen nicht den neo-kolonialen Wirtschaftsinteressen von Frankreich folgten.[94]

2.10 Ich habe doch nichts zu verbergen!

Dieses Argument hört man oft. Haben wir wirklich nichts zu verbergen? Einige Beispiele für spezielle Detektoren und Einzelbeispiele sollen exemplarisch zeigen, wie tief Big Data in unser Leben eingreift und wie gravierend die willkürlich gesammelten Daten unser Leben beeinflussen können.

[94] https://www.heise.de/tp/artikel/46/46592/1.html

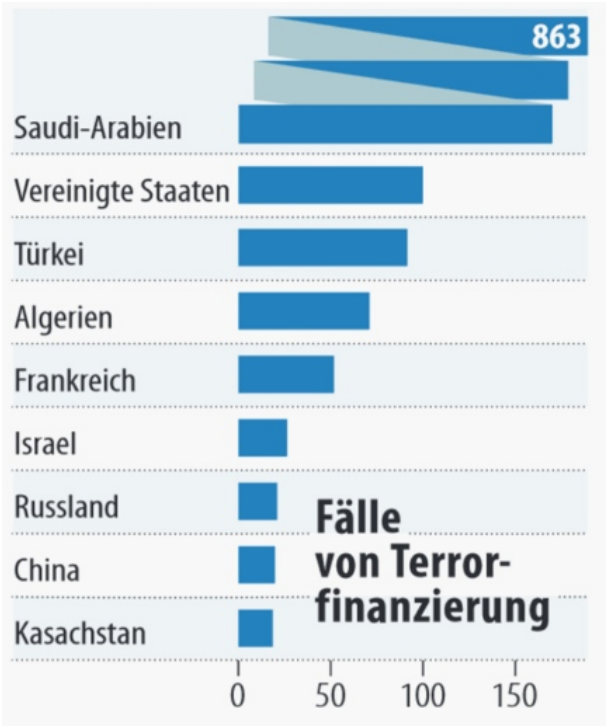


Abbildung 2.17: Staaten, die Terroristen finanzieren

Erkennung einer neuen Liebesbeziehung

Der Beginn einer neuen Liebe oder einer erotischen Affäre ist anhand der Änderungen im Kommunikationsverhalten gut erkennbar. Big-Data-Analysten nennen die typischen Muster *Balzverhalten*. Alle Player auf dem Gebiet der Datenanalyse (kommerzielle Datensammler, Anbieter von Software zur Mitarbeiterüberwachung, Geheimdienste usw.) haben passende Detektoren zur Erkennung von *Balzverhalten* entwickelt.

- Marketingexperten haben herausgefunden, dass man sich in dieser Situation leichter zum Wechsel von Marken bewegen lässt und mehr Geld ausgibt.
- Headhunter wissen, dass man Menschen in dieser Situation leichter zu beruflichen Veränderungen bewegen kann.
- Personalmanager großer Firmen interessieren sich für die Auswirkungen auf die Produktivität bei Affären innerhalb der Firma.
- Geheimdienste interessieren sich für die Erpressbarkeit von Ziel-Personen.

Arbeitslos?

Unser Smartphone liefert die aktuelle Position des Nutzers an viele Trackingdienste. Außerdem verraten Postings bei Twitter oder Facebook unseren Aufenthaltsort.

In der Regel sind wir nachts zuhause und an Werktagen tagsüber an unserem Arbeitsplatz. Was kann man schlussfolgern, wenn sich dieses Verhalten ändert und man auch tagsüber über einen längeren Zeitraum zuhause bleibt, in Kombination mit einem sparsameren Konsumverhalten bei Online- oder Offline-Einkäufen mit Rabattkarten bzw. Kreditkarten? Welchen Einfluss hat das auf unsere Kreditwürdigkeit?

Unzufrieden mit dem Job?

Vorreiter auf diesem Gebiet war Google. Schon 2010 protzte Google damit, im Rahmen der Mitarbeiterüberwachung den Wunsch nach beruflicher Veränderung schneller erkennen zu können, als der betroffene Mitarbeiter sich selbst darüber im Klaren sei. Inzwischen nutzen auch andere Firmen diese Überwachung. Personalchefs können auf einen solchen computergenerierten Verdacht unterschiedlich reagieren. Einarbeitung eines Nachfolgers und Entlassung des verdächtigen Mitarbeiters ist eine Möglichkeit.

L. Reppesgaard versendete im Rahmen eines Selbstversuches mehrere E-Mails mit kritischen Bemerkungen zu seinem Arbeitsverhältnis von seinem GMail-Account. Unmittelbar darauf konnte er Veränderungen in der personalisierten Werbung registrieren, die plötzlich auf Headhunter und kommerzielle Jobbörsen hinwies.

Kein Studienplatz?

In Großbritannien werden Studienbewerber für bestimmte Fachrichtungen geheimdienstlich überprüft. Eine Anzahl von 739 Bewerbern wurde bereits abgelehnt, weil aufgrund dubioser Datensammlungen der Geheimdienste befürchtet wurde, dass die Bewerber zu Terroristen werden und die im Studium erworbenen Kenntnisse zur Herstellung von Massenvernichtungswaffen nutzen könnten. Die geheimdienstlichen Gesinnungsprüfungen sollen zukünftig ausgeweitet werden.[95]

Einzelbeispiele

- Emma L. hatte sich auf dem Dating-Portal OkCupid zu einem Treffen verabredet. Das Date war ein Reinfall (kommt manchmal vor). Wenig später wurde ihr der Dating-Partner von Facebook als Freund empfohlen, in der Section *People You May Know*. Maria L. wurden ihre Tinder-Dates von Facebook als Freunde empfohlen. Es gibt auf Twitter noch viele weitere Beispiele für diese seltsamen Facebook-Empfehlungen.[96]

  Weder OkCupid noch Tinder geben Daten an Facebook weiter. Die Empfehlungen für Freunde werden anhand der Geolocation (*zur gleichen Zeit am gleichen Ort*) und aufgrund ähnlicher Interessen (*Dating-Webseite besucht*) ermittelt. Daraus könnten sich auch unangenehme Folgen ergeben, wie Netzpolitik.org an Beispielen zeigt.

- Target ist einer der größten Discounter in den USA. Eines Tages stürmte ein wütender Vater in eine Filiale und beschwerte sich, dass seine minderjährige Tochter Rabattmarken für Babysachen erhalten habe. Später musste der Vater kleinlaut zugegeben, dass seine Tochter wirklich schwanger sei, er selbst aber nichts davon gewusst habe. Target hatte die Schwangerschaft der minderjährigen Tochter an den kleinen Änderungen im Kaufverhalten erkannt.[97]

- Im Rahmen der Zulässigkeitsprüfung für Piloten wurde Herr J. Schreiber mit den vom Verfassungsschutz gesammelten Fakten konfrontiert:[98]

  1. Er war 1994 auf einer Demonstration kontrolliert worden. Er war nicht angezeigt, angeklagt oder einer Straftat verdächtigt, sondern nur als Teilnehmer registriert worden.

[95] https://www.heise.de/tp/artikel/44/44538/1.html
[96] https://twitter.com/search?q=facebook%20suggest%20tinder
[97] http://www.tagebau.com/?p=197
[98] http://www.pilotundflugzeug.de/artikel/2006-02-10/Spitzelstaat

2. Offensichtlich war daraufhin sein Bekanntenkreis durchleuchtet worden.
3. Als Geschäftsführer einer GmbH für Softwareentwicklung habe er eine vorbestrafte Person beschäftigt. Er sollte erklären, welche Beziehung er zu dieser Person habe.
4. Laut Einschätzung des Verfassungsschutzes neige er zu politischem Extremismus, da er einen Bauwagen besitze. Bei dem sogenannten *Bauwagen* handelte es sich um einen Allrad-LKW, den Herr S. für Reisen nutzte (z. B. in die Sahara).

Für Herrn S. ging die Sache gut aus. In einer Stellungnahme konnte er die in der Akte gesammelten Punkte erklären. In der Regel wird uns die Gelegenheit zu einer Stellungnahme jedoch nicht eingeräumt. Es werden Entscheidungen getroffen und wir haben keine Ahnung, welche Daten dabei eine Rolle spielen.

- Ein junger Mann meldet sich freiwillig zur Bundeswehr. Mit sechs Jahren war er kurzzeitig in therapeutischer Behandlung, mit vierzehn hatte er etwas gekifft. Seine besorgte Mutter war mit ihm zur Drogenberatung gegangen. In den folgenden Jahren gab es keine Drogenprobleme. Von der Bundeswehr erhält er eine Ablehnung, da er ja mit sechs Jahren eine Psychotherapie habe durchführen müssen und Drogenprobleme gehabt hätte.[99].

- Kollateralschäden: Ein großer deutscher Provider lieferte falsche Kommunikationsdaten ans BKA. Der zu Unrecht Beschuldigte erlebte das volle Programm: Hausdurchsuchung, Beschlagnahme der Rechner, Verhöre und sicher nicht sehr lustige Gespräche im Familienkreis. Die persönlichen und wirtschaftlichen Folgen sind schwer zu beziffern.[100]

  Noch krasser ist das Ergebnis der *Operation Ore* in Großbritannien. Einige Tausend Personen wurden wegen Konsums von Kinderpornografie angeklagt. Acht Jahre später stellte sich heraus, dass die meisten Betroffen zu unrecht verurteilt worden waren, weil sie Opfer von Kreditkarten-Betrug geworden waren. Inzwischen hatten 39 Menschen Selbstmord begangen, da ihnen alles genommen worden war.[101].

- „Leimspur des BKA“: Wie schnell man in das Visier der Fahnder des BKA geraten kann, zeigt ein Artikel bei Zeit-Online. Die Webseite des BKA zur Gruppe „mg“ ist ein Honeypot, der dazu diente, weitere Sympathisanten zu identifizieren. Die Bundesanwaltschaft verteidigt die Maßnahme als legale Fahndungsmethode.

  Mit dem im Juni 2009 beschlossenen BSI-Gesetz übernahm die Behörde die Aufzeichnung und unbegrenzte Speicherung personenbezogener Nutzerinformationen wie IP-Adressen, die bei der Online-Kommunikation zwischen Bürgern und Verwaltungseinrichtungen des Bundes anfallen. Ich kann daraus nur den Schluss ziehen, diese und ähnliche Angebote in Zukunft ausschließlich mit Anonymisierungsdiensten zu nutzen.

Nicht immer treten die (repressiven) Folgen staatlicher Sammelwut für die Betroffenen so deutlich hervor. In der Regel werden Entscheidungen über uns getroffen, ohne das wir darüber benachrichtigt werden. Wir bezeichnen die (repressiven) Folgen dann als Schicksal.

Politische Aktivisten

Wer sich politisch engagiert und gerne auf vertuschte Missstände hinweist, hat besonders unter der Sammelwut staatlicher Stellen zu leiden. Einige deutsche Beispiele:

[99] https://blog.kairaven.de/archives/998-Datenstigmaanekdote.html
[100] https://www.lawblog.de/index.php/archives/2008/03/11/provider-liefert-falsche-daten-ans-bka/
[101] https://en.wikipedia.org/wiki/Operation_Ore

1. Erich Schmidt-Eenboom veröffentliche 1994 als Publizist und Friedensforscher ein Buch über den BND. In den folgenden Monaten wurden er und seine Mitarbeiter vom BND ohne rechtliche Grundlage intensiv überwacht, um die Kontaktpersonen zu ermitteln. Ein Interview unter dem Titel *Sie beschatteten mich sogar in der Sauna*[102] gibt es bei SPON.

2. Fahndung zur Abschreckung: In Vorbereitung des G8-Gipfels in Heiligendamm veranstaltete die Polizei am 9. Mai 2007 eine Großrazzia. Dabei wurden bei Globalisierungsgegnern Rechner, Server und Materialien beschlagnahmt. Die Infrastruktur zur Organisation der Proteste wurde nachhaltig geschädigt. Wenige Tage nach der Aktion wurde ein Peilsender des BKA am Auto eines Protestlers gefunden. Um die präventiven Maßnahmen zu rechtfertigen, wurden die Protestler als terroristische Vereinigung eingestuft.

   Das Netzwerk Attac konnte 1,5 Jahre später vor Gericht erreichen, dass diese Einstufung unrechtmäßig war. Das Ziel, die Organisation der Proteste zu behindern, wurde jedoch erreicht.

3. Dr. Rolf Gössner ist Rechtsanwalt, Vizepräsident der Internationalen Liga für Menschenrechte, Mitherausgeber des Grundrechte-Reports, Vizepräsident und Jury-Mitglied bei den Big Brother Awards. Er wurde vom Verfassungsschutz 38 Jahre lang überwacht. Obwohl das Verwaltungsgericht Köln bereits urteilte, dass der Verfassungsschutz für den gesamten Bespitzelungszeitraum Einblick in die Akten gewähren muss, wird dieses Urteil mit Hilfe der Regierung ignoriert. Es werden Sicherheitsinteressen vorgeschoben!

Mit dem Aufbau der „neuen Sicherheitsarchitektur“ bedeutet eine Überwachung nicht nur, dass der direkt Betroffene überwacht wird. Freunde und Bekannte aus dem persönlichen Umfeld werden ebenfalls einbezogen und in der Antiterrordatei gespeichert. Auch ihre Kommunikation kann überwacht werden, es ist sogar möglich, Wanzen in den Wohnungen der Freunde zu installieren.

[102] http://www.spiegel.de/politik/deutschland/0,1518,384374,00.html

Kapitel 3

Digitales Aikido

Die folgende grobe Übersicht soll die Orientierung im Dschungel der nachfolgend beschriebenen Möglichkeiten etwas erleichtern.

- **Einsteiger-Trackingschutz:** Datensammler nutzen verschiedenste Möglichkeiten, Informationen über Menschen, über ihre Interessen und Vorlieben usw. zu aggregieren und diese Daten zur Manipulation des Einkaufsverhaltens oder politischer Ansichten zu nutzen. Um sich dem zu entziehen, kann man das allgegenwärtige Tracking mit verschiedenen Mitteln erschweren.

  – Spurenarm surfen: Datensammler meiden und Alternativen nutzen, Cookies und Javascript kontrollieren, Werbung filtern;
  – E-Mail: Auswahl des Providers, E-Mail-Client sicher konfigurieren, unterschiedliche Alias-E-Mail-Adressen für unterschiedliche Aufgaben verwenden;
  – Messenger: Nachdenken über einen oder mehrere geeignete Dienste für Instant-Messaging, Boykottieren von Datensammlern;
  – Social-Media: Dienste meiden, die in erster Linie Daten sammeln, um ihre Nutzer an die Werbeindustrie zu verkaufen;
  – ...

  Man kann in kleinen Schritten anfangen und darüber nachdenken, welche Spuren man beim Surfen, Einkaufen usw. im Netz hinterlässt, und Alternativen bewusst wählen.

- **Level 2 (Verschlüsselung):** Das Verschlüsseln persönlicher Daten und privater Kommunikation verwehrt es Dritten, Kenntnis über diesen privaten Bereich des Lebens zu erlangen (E-Mails, Daten und Backups, Telefonie und Chats verschlüsseln).

- **Level 3 (Anonymisierung):** Wie ein Geist durch das Internet streifen, nicht greifbar sein wie ein Hauch von Nebel oder als Whistleblower wirklich anonym bleiben ...

  Anonymisierungsdienste wie Tor bilden die technische Basis dafür. Tor Onion Router bietet eine dem realen Leben vergleichbare Anonymität beim Surfen usw. Man kann anonym an Diskussionsforen teilnehmen oder Artikel kommentieren, indem man sich mit Wegwerf-Adressen registriert und Pseudonyme häufig wechselt.

  Neben der technischen Basis kommt es dabei aber vor allem auf das eigene Verhalten an. Man muss den inneren Drang nach Selbstdarstellung überwinden und auf die Reputation oder Anerkennung als Person verzichten. Das ist manchmal nicht leicht und häufig sind es die kleinen Eitelkeiten, die zur Deanonymisierung führen können.

In der Regel wird man sowohl als reale Person im Internet unterwegs sein (bei Einkäufen mit Lieferung, als IT-Nerd, als Wissenschaftler, als Fotograf oder als Blogger usw. – es gibt viele Gründe) und bei anderen Themen versuchen, anonym zu bleiben. Wichtig ist, diese unterschiedlichen Identitäten vollständig zu trennen.

- **Level 4 (Dan, Guru):** Wenn man nicht nur beim passiven Konsumieren anonym bleibt sondern es schafft, Reputation für eine virtuelle Identität aufzubauen (bspw. als Blogger, Autor oder Händler), die nicht mit einer realen Person verknüpft werden kann, dann hat man einen Dan-Level erreicht.

  (Das ist übrigens auch der Traum krimineller Drogen- und Waffenhändler u. Ä. im Internet.)

  Die technische Basis bieten Tor-Onion-Services oder anonyme Peer-2-Peer Netze wie das Invisible-Internet-Projekt (I2P) oder das GNUnet-Projekt. Eine dezentrale und verschlüsselte Infrastruktur verbirgt die Inhalte der Kommunikation und wer welchen Dienst nutzt. Auch Anbieter von Informationen sind in diesen Netzen anonym.

Die einzelnen Level bauen aufeinander auf! Es macht wenig Sinn, die IP-Adresse zu verschleiern, wenn man anhand von Cookies eindeutig identifizierbar ist. Auch die Versendung einer anonymen E-Mail ist in der Regel verschlüsselt sinnvoller.

3.1 Nachdenken

Eine Graduierung in den Kampfsportarten ist keine Garantie, dass man sich im realen Leben erfolgreich gegen einen Angreifer zur Wehr setzen wird. Ähnlich verhält es sich mit dem *Digitalen Aikido*. Es ist weniger wichtig, ob man gelegentlich eine E-Mail verschlüsselt oder einmal pro Woche Anonymisierungsdienste nutzt. Entscheidend ist ein konsequentes, datensparsames Verhalten.

Ein kleines Beispiel soll zum Nachdenken anregen. Es ist keinesfalls umfassend oder vollständig. Ausgangspunkt ist eine reale Person P mit Namen, Geburtsdatum, Wohnanschrift, Fahrerlaubnis, Kontoverbindung usw.

Im Internet verwendet diese Person verschiedene Online-Identitäten:

1. Facebook-Account (es könnte auch Xing oder ein ...VZ sein);
2. Eine E-Mail-Adresse mit dem realen Namen;
3. Eine anonyme/pseudonyme E-Mail-Adresse bei einem ausländischen Provider;
4. Pseudonyme in verschiedenen Foren, die unter Verwendung der anonymen E-Mail-Adresse angelegt wurden;
5. Für Kommentare in Blogs verwendet die Person meist ein einheitliches Pseudonym, um sich Anerkennung und Reputation zu erarbeiten. (Ohne Reputation könnte das soziale Gefüge des Web 2.0 nicht funktionieren.)

Mit diesen Online-Identitäten sind verschiedene Datenpakete verknüpft, die irgendwo gespeichert und vielleicht nicht immer öffentlich zugänglich sind. Um übersichtlich zu bleiben, nur eine minimale Auswahl:

- Das Facebook-Profil enthält umfangreiche Daten: Fotos, Freundeskreis usw.

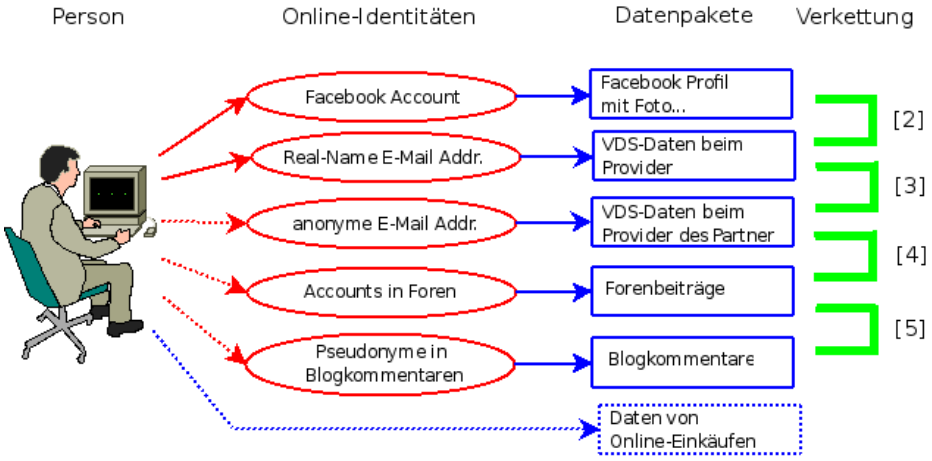


Abbildung 3.1: Datenverkettung

- Bei der Nutzung von vielen Webdiensten fallen kleine Datenkrümel an. Auch E-Mails werden von den Datensammlern ausgewertet. Die IP-Adresse des Absenders im Header der E-Mails kann mit anderen Einträgen von Cookies oder User-Tracking-Systemen zeitlich korreliert werden. So können den Surf-Profilen E-Mail-Adressen und reale Namen zugeordnet werden.
- Von dem anonymen E-Mail-Postfach findet man Daten bei den Empfängern der E-Mails. (Google has most of my emails because it has all of yours.) Auch diese Datenpakete enthalten einen Zeitstempel sowie oft die IP-Adresse des Absenders. Durch zeitliche Korrelation kann das anonyme E-Mail-Postfach mit dem Real-Name-Postfach und dem Surf-Profil verknüpft werden.
- In Foren und Blogs findet man Postings und Kommentare, häufig mit den gleichen Pseudonymen, die auch für die E-Mail-Adressen verwendet werden.
- Online-Einkäufe erfordern die Angaben zur Kontoverbindung und einer Lieferadresse, die der Person zugeordnet werden können.

Verkettung der Informationen und Datenpäckchen

Viele Datenpakete können auf vielfältige Art verknüpft werden. Diese *Datenverkettung* ist eine neue Qualität für Angriffe auf die Privatsphäre, die unterschätzt wird.

1. Online-Communitys wie Facebook bieten viele Möglichkeiten. Neben der Auswertung von Freundschaftsbeziehungen gibt es auch viele Fotos. Dieser Datenpool ist schon sehr umfangreich:
   - Wirtschaftswissenschaftler haben eine Methode vorgestellt, um Meinungsmacher und kreative Köpfe in Online-Communitys zu identifizieren.[1]
   - MIT-Studenten erkennen homosexuelle Neigungen ihrer Kommilitonen anhand der Informationen über Freundschaften in den Facebook-Profilen.[2]

[1] https://www.heise.de/tp/r4/artikel/31/31691/1.html
[2] https://www.heise.de/tp/r4/artikel/31/31181/1.html

- Der Grünen-Vorsitzende Özdemir pflegte eine Freundschaft mit dem Intensivstraftäter Muhlis Ari, das ist in seinem Facebook-Profil erkennbar[3].

2. Dem Facebook-Profil kann man durch Kombination mit anderen Datenkrümeln den realen Namen und die meisten genutzten E-Mail-Adressen zuordnen. Die Firma Rapleaf ist z. B. darauf spezialisiert. Auch pseudonyme Facebook-Accounts können deanonymisiert werden.

3. Durch Analyse der im Rahmen der VDS gespeicherten IP-Adressen können bei zeitlicher Übereinstimmung beide E-Mail-Adressen der gleichen Person zugeordnet werden. Ein einzelner passender Datensatz reicht aus. (Wenn nicht konsequent Anonymisierungsdienste für das anonyme Postfach verwendet werden.)

4. Die Verbindung zwischen anonymer E-Mail-Adresse und Foren-Account ergibt sich durch die Nutzung der E-Mail-Adresse bei Anmeldung.

5. Durch Vergleiche von Aussagen und Wortwahl lassen sich Korrelationen zwischen verschiedenen Nicknames in Foren und Blogs herstellen. Dem Autor sind solche Korrelationen schon mehrfach offensichtlich ins Auge gesprungen und konnten durch Nachfrage verifiziert werden.

6. Durch Datenschutzpannen können Informationen über Online-Einkäufe mit anderen Daten verknüpft werden. Dabei schützt es auch nicht, wenn man sich auf das Gütesiegel des TÜV Süd verlässt und bei einem Händler einkauft, der bisher nicht negativ aufgefallen ist. Eine kleine Zusammenfassung vom 29.10.09 bis 04.11.09:

   - Die Bücher der Anderen (500.000 Rechnungen online einsehbar)
   - Die Libris-Shops (Zugang zu Bestellungen von 1000 Buchshops)
   - Sparkassen-Shops (350.000 Rechnung online einsehbar)
   - 8 Mio. Adressen von Quelle-Kunden sollen verkauft werden

   Eine reichhaltige Quelle für Datensammler, die Profile ihrer Zielpersonen vervollständigen wollen oder nach potentiellen Zielpersonen rastern.

Durch die Verkettung der Datenpäckchen konnten in dem fiktiven Beispiel alle Online-Identitäten deanonymisiert werden. Für den Sammler, der diese Datensammlung in der Hand hält, ergibt sich ein komplexes Persönlichkeitsbild der Person P. Diese Datensammlung könnte das Leben von P in vielerlei Hinsicht beeinflussen, ohne dass dem Betroffenen klar wird, dass hinter scheinbar zufälligen Ereignissen ohne Zusammenhang bewusste Entscheidungen stehen.

- Die Datensammlungen werden mit kommerziellen Zielen ausgewertet, um uns zu manipulieren und Kaufentscheidungen zu beeinflussen.
- Personalabteilungen rastern routinemäßig das Internet nach Informationen über Bewerber. Dabei ist Google nur ein erster Ansatzpunkt. Bessere Ergebnisse liefern Personensuchmaschinen und soziale Netzwerke. Ein kurzer Auszug aus einem realen Bewerbungsgespräch:
  - Personalchef: *Es stört Sie sicher nicht, dass hier geraucht wird. Sie rauchen ja ebenfalls.*
  - Bewerber: *Woher wissen Sie das?*
  - Personalchef: *Die Fotos in ihrem Facebook-Profil ...*

[3] https://www.heise.de/tp/r4/artikel/32/32138/1.html

Qualifizierten Personalchefs ist dabei klar, dass eine kurze Recherche in Sozialen Netzen kein umfassendes Persönlichkeitsbild liefert. Die gefundenen Indizien können aber den Ausschlag für eine Ablehnung geben, wenn man als Frau gebrauchte Unterwäsche anbietet oder der Bewerber eine Nähe zur Gothic-Szene erkennen lässt.

- Von der israelischen Armee ist bekannt, dass sie die Profile in sozialen Netzen überprüfen, wenn Frauen den Wehrdienst aus religiösen Gründen verweigern. Zur Zeit verweigern in Israel 35 % der Frauen den Wehrdienst. Anhand der sozialen Netze wird der Lebenswandel dieser Frauen überprüft. Es werden Urlaubsfotos in freizügiger Bekleidung oder Anhaltspunkte für Essen in einem nicht-koscheren Restaurant gesucht. Dabei wird auch aktiv gehandelt und Fake-Einladungen zu einer Party werden während des Sabbats verschickt.
- Firmen verschaffen sich unrechtmäßig Zugang zu Verbindungs- und Bankdaten, um ihre Mitarbeiter auszuforschen (z. B. Telekom- und Bahn-Skandal).
- Identitätsdiebstahl ist ein stark wachsendes Delikt. Kriminelle durchforsten das Web nach Informationen über reale Personen und nutzen diese Identitäten für Straftaten. Wie sich Datenmissbrauch anfühlt: Man wird plötzlich mit Mahnungen für nicht bezahlte Dienstleitungen überschüttet, die man nie in Anspruch genommen hat.[4]
- Mit dem Projekt INDECT hat die EU ein Forschungsprojekt gestartet und mit 14,8 Mio. Euro ausgestattet, um unsere Daten-Spuren für Geheimdienste zu erschließen.[5]

Ich habe doch nichts zu verbergen ...

... oder habe ich nur zu wenig Fantasie, um mir die Möglichkeiten der Datensammler vorzustellen, mein Leben zu beeinflussen?

3.2 Ein Beispiel

Das *Seminar für angewandte Unsicherheit* (SAU) hat ein sehr schönes Lehrbeispiel im Internet vorbereitet. Jeder kann selbst nach Informationen über diese fiktive Person suchen und das Profil verifizieren. Es geht um folgende Person:

Name:	Fiona Flauderer
geboren:	17.06.1985
E-Mail:	fiona.flauderer@gmail.com
Status:	Studentin
Anschrift:	Dorthenstr. 17, 10995 Berlin

Diese Informationen könnte ein Personalchef einer Bewerbung entnehmen oder sie sind der Krankenkasse bekannt oder sie ist bei einer Demo aufgefallen ... Eine kurze Suche bei Google und verschiedenen Personensuchmaschinen liefert nur sehr wenig, im Moment sind es 3 Treffer. Gleich wieder aufgeben?

Die moderne Studentin ist sozial vernetzt. Naheliegend ist es, die verschiedenen Netzwerke wie StudiVZ usw. nach F. abzusuchen. Bei Facebook wird man erstmals fündig. Es gibt ein Profil zu dieser Person mit Fotos, Interessen und (wichtig!) eine neue E-Mail-Adresse:

[4] http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung
[5] https://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung

goagirl17@ymail.com

Bezieht man diese Adresse in die Suche bei anderen Sozialen Netzwerken mit ein, wird man bei MySpace.com erneut fündig. Hier gibt es ein Profil mit dieser E-Mail-Adresse und man findet den Twitter-Account von F. sowie ein weiteres Pseudonym:

flaudi85

Mit den beiden gefundenen Pseudonymen g.....17 und f.....85 kann man erneut bei Google suchen und die Ergebnisse mit den Informationen aus den Profilen zusammenfassen.

- g.....17 ist offenbar depressiv. Das verordnete Medikament deutet auf Angstzustände hin, wurde von der Patientin aber nicht genommen sondern ins Klo geworfen.
- Sie hat Probleme im Studium und will sich krankschreiben lassen, um nicht an Prüfungen teilnehmen zu müssen.
- Außerdem hat sie ein massives Alkoholproblem und beteiligt sich am *Syncron-Saufen* im Internet. Scheinbar ist sie auch vereinsamt.
- F. ist offenbar lesbisch, sie sucht nach einer Frau bei abgefuckt.de.
- F. ist im linksradikalen Spektrum aktiv. Sie hat an mehreren Demonstrationen teilgenommen und berichtet über Erfahrungen mit Hausdurchsuchungen. Möglicherweise ist das die Ursache für ihre Angstzustände.
- Öffentlich prangert sie in einem Diskussionsforum die Firma ihres Vaters an (wegen Ausspionierens von Mitarbeitern).
- Ihre linksgerichtete Grundhaltung wird durch öffentliche Unterstützung der Kampagne *Laut ficken gegen Rechts* unterstrichen.
- Von regelmäßiger Arbeit hält sie nicht viel.
- Die angegebene Adresse ist falsch. F. wohnt in einer 11-Personen-WG in einem besetzten Haus in Alt-Moabit. Die WG sucht nach einem neuem Mitglied.
- Die Wunschliste bei Amazon und Fotos bei Flickr ...

Würden sie als Personalchef diese fiktive Person einstellen?

Welche Ansatzpunkte ergäben sich für den Verfassungsschutz?

Was könnte zukünftig für die Krankenkasse interessant sein?

Was hätte F. tun können, um die Profilbildung zu vermeiden?

3.3 Schattenseiten der Anonymität

Auf den ersten Blick scheint Anonymität eine Lösung für fast alle beschriebenen Probleme zu sein. Anonymität verhindert das Tracking durch kommerzielle Datensammler, schützt die Privatsphäre vor neugierigen Blicken der Spanner, schränkt die Überwachungsmöglichkeiten der Geheimdienste ein, bietet Whistleblowern Schutz usw.

Neben den unbestreitbaren Vorteilen hat Anonymität aber auch Schattenseiten. Einige kleine Denkanstöße sollen zu einem verantwortungsbewussten Umgang mit Anonymität anregen, bevor der technische Teil beginnt.

Am Beispiel ANONYMOUS sieht man einige Nachteile deutlich. ANONYMOUS ist als Protestgruppe gegen Scientology gestartet und mit dem Einsatz der *low orbit ion canone* (LOIC) gegen Banken zur Unterstützung von Wikileaks bekannt geworden. Später belauschte ANONYMOUS angeblich den E-Mail-Verkehr der lettischen Botschaft und veröffentlicht selektiv belastende E-Mails von Klitschko. Oder war das der russische GRU im Rahmen der Propagandaschlacht um die Krim? Das Label ANONYMOUS kann jeder Hanswurst für beliebige Zwecke missbrauchen und die Bewegung diskreditieren.

Reputation, Vertrauen, Respekt und Verantwortung sind an Persönlichkeit gebunden. Dabei muss Persönlichkeit nicht unbedingt mit einem realen Namen verbunden sein. Reputation und Respekt kann man auch unter einem Pseudonym oder als eine Gruppe erwerben, wenn man die Verantwortung für seine Handlungen übernimmt.

Im Schutz der Anonymität muss man aber keine Verantwortung für sein Handeln übernehmen, da Fehlverhalten oder gesellschaftlich unerwünschte Handlungen nicht sanktioniert werden können. In einem Diskussionsforum kann man sich verbale Entgleisungen erlauben, ohne negative Reputation für seine Person fürchten zu müssen. Man verwendet in Zukunft einfach einen neuen anonymen Account und beginnt von vorn. Das habe ich schon öfters erlebt. Dieser Umgang mit Anonymität ohne Verantwortung stört im einfachen Fall nur. Es kann aber auch schwerere Auswirkungen haben.

Ein anonymer Schwarm vereinzelter Individuen kann sich zu einem Shitstorm zusammenfinden. Der Schwarm kann kurzzeitig viel Lärm ohne gesellschaftlichen Diskurs produzieren und wird dann wieder zerfallen. Er wird kein *Wir!* entwickeln und kann keine gemeinsamen Ziele verfolgen, die über einen kurzzeitigen Hype in den Medien hinaus gehen. Außerdem lassen sich Empörungswellen durch eine kritische Masse anonymer Sockenpuppen leicht manipulieren.

Ein Beispiel für den Konflikt zwischen Anonymität und Vertrauen:

1. Ich kann mir ganz anonym in meiner Einsiedlerzelle mit einem Anonymisierungsdienst bei YouPorn, RedTube, XHamster ...
2. Oder ich kann eine Frau im Arm halten, die sich sehnsuchtsvoll an mich drängt, ihre Haut spüren, das gegenseitige Begehren fühlen und eintauchen in einen Strudel der ...

Bei Variante 1) bleibt meine Anonymität gewahrt, aber sie hinterlässt gähnende Leere und Einsamkeit. Variante 2) funktioniert nur mit gegenseitigem Vertrauen und Respekt. Um die Liebesbriefe in 2) gegen mitlesende sabbernde Schlapphüte zu schützen, ist **jedes** Mittel zulässig, aber Kryptografie, TorBrowser, JonDonym usw. sind nur Werkzeuge und kein Selbstzweck.

Für ein soziales Zusammenleben und gemeinsame Ziele brauchen wir Vertrauen. Vertrauen kann missbraucht werden, man sollte es nicht leichtfertig verschenken. Es ist aber wichtig, bei aller gebotenen Vorsicht auch einen Weg zu finden, um gegenseitiges Vertrauen aufzubauen.

Das Beispiel kann man auf beliebige Gebiete übertragen. Es gilt für politische Aktivisten, die von der Demokratiesimulation genug haben und dem *Stillen Putsch* etwas entgegen setzen wollen. Und es gilt für Mitglieder im Kleintierzüchterverein, die in den Suchergebnissen bei Google nicht ständig Links für Kaninchenfutter finden wollen. Welche Werkzeuge angemessen sind, hängt von den konkreten Bedingungen ab.

3.4 Wirkungsvoller Einsatz von Kryptografie

Nach einer anerkannten Faustregel ist der wirkungsvolle Einsatz von Kryptografie von folgenden allgemeinen Faktoren abhängig:

- Zu 10 % hängt der Schutz von der eingesetzten Technik ab.
- Zu 60 % beeinflusst das Wissen der Anwender über Möglichkeiten und Grenzen den wirkungsvollen Einsatz kryptografischer Verfahren.
- Zu 30 % hängt die Wirksamkeit von der Disziplin der Anwender ab.

Bevor es mit konkreten Anleitungen weiter geht, sollen einige allgemeine Gedanken zum Nachdenken über die Verwendung von Verschlüsselung anregen. Man kann natürlich einfach irgendwie beginnen, irgendwas zu verschlüsseln. Nachhaltigen und vor allem wirksamen Schutz gegen Überwachung und Datensammlung erreicht man damit aber nicht.

1. Kryptografie ist kein Selbstzweck, sondern ein Hilfsmittel zum Schutz unserer Privatsphäre. Erste Voraussetzung für den wirksamen Einsatz von Kryptografie ist, dass eine Privatsphäre existiert, die geschützt werden kann. Dieser Bereich privater Lebensführung entsteht nicht zwangsläufig durch den Einsatz von Kryptografie, sondern muss zuerst **durch Verhalten** geschaffen werden.

   Beispiel: Wenn man einem Bekannten eine verschlüsselte E-Mail mit einem Link zu der Sammlung von Urlaubsfotos bei Facebook schickt, dann gibt es keine Privatsphäre, die durch die Verschlüsselung der E-Mail geschützt werden könnte.

2. Wenn man einen Bereich gefunden oder festgelegt hat, den man gegen Datensammler und Überwachung schützen möchte, dann sollte die technische Umsetzung des Schutzes vollständig und umfassend sein. Es ist nur wenig nachhaltig, wenn man gelegentlich eine verschlüsselte E-Mail schreibt und gleichzeitig zwei unverschlüsselte E-Mails mit dem gleichen Inhalt an andere Empfänger (mit Google Accounts?) schickt.

   - Studien haben nachgewiesen, dass es ausreichend ist, in einer organisierten Gruppe nur 10–20 % der Mitglieder zu überwachen, um über die Struktur der Gruppe und ihre wesentlichen Aktivitäten informiert zu sein.
   - Wenn man Anonymisierungsdienste zur Verwaltung von E-Mail-Konten, für ein anonymes Blog, für digitale Identitäten oder zur Recherche zu sensiblen Themen nutzt, dann muss man sie in diesem Kontext immer nutzen. Anderenfalls könnten die Aktivitäten aus der Vergangenheit nachträglich deanonymisiert werden und für die Zukunft ist die Anonymität in diesem Kontext nicht mehr gegeben.
   - Schützenswerte, private Daten (was das ist, muss man selbst definieren) sollten immer verschlüsselt gespeichert und transportiert werden. Das betrifft nicht nur die Speicherung auf dem eigenen Rechner, sondern auch alle Backups und jede Kopie bei Dritten. Wer private Dateien ohne zusätzliche Verschlüsselung via Skype verschickt, sollte sich darüber klar sein, dass Microsoft immer mitliest.

   Die Umsetzung dieser Anforderung erfordert in erster Linie Disziplin im Umgang mit den technischen Kommunikationsmitteln. *Schnell mal ...* ist immer schlecht. Man kann in kleinen Schritten spielerisch beginnen. Dabei sollte man das Gesamtziel aber nicht aus den Augen verlieren.

3. Die meisten Protokolle zur verschlüsselten Kommunikation verwenden Public-Key-Verfahren (SSL/TLS, OpenPGP, OTR, SSH). Wenn man für hohe Anforderungen wirklich sicher sein will, dass nur der Kommunikationspartner (oder der Server bei SSL) die gesendeten Daten entschlüsseln kann, dann muss man den öffentliche Schlüssel der Gegenseite über einen sicheren, unabhängigen Kanal verifizieren.

   Ein universelles Verfahren für die Verifizierung von kryptografischen Schlüsseln ist der Vergleich des Fingerprint anhand veröffentlichter Werte. Über einen sicheren Kanal (z. B. ein persönliches Treffen) tauscht man die Fingerprints der Public-Keys aus und vergleicht sie später am eigenen Rechner mit den Fingerprints der tatsächlich verwendeten Schlüssel. Man kann die Fingerprints der eigenen Schlüssel auch veröffentlichen, um den Kommunikationspartnern die Verifikation zu ermöglichen.

   Krypto-Messenger wie die Signal-App, [matrix]/Riot oder Threema bieten die Möglichkeit, die Schlüssel des Gegenübers anhand der Fingerprints zu verifizieren, und unterstützen diese Verifikation bei persönlichen Treffen durch QR-Codes, die man gegenseitig scannen kann, ohne lange Zahlenkolonnen vergleichen zu müssen.

Kapitel 4

Spurenarm surfen mit Firefox

Es gibt noch immer einige Zeitgenossen, für die Privatsphäre ein wichtiges Thema ist und die sich nicht ständig über die Schulter schauen lassen wollen beim Lesen von News, beim Kaufen von Theaterkarten oder beim Entspannen auf irgendwelchen You-Dingends-Seiten.

Hier soll das Thema **spurenarmes Surfen** behandelt werden. Zur Abgrenzung und zur Vermeidung von Missverständnissen ist es nötig, die Zielstellung zu klären:

Spurenarmes Surfen ist in erster Linie ein Schutzkonzept gegen das allgegenwärtige Tracking und Beobachten zur Erstellung von umfassenden Persönlichkeitsprofilen, die dann zur gezielten Manipulation der betroffenen Person missbraucht werden können. Anonymität (z. B. für Whistleblower) steht dabei nicht im Fokus.

Schutz gegen Tracking erreicht man durch mehrere Maßnahmen:

- Daten sammelnde Dienste kann man meiden und Trackingelemente wie Werbebanner, antisoziale Like-Buttons, JavaScript-Trackingcode oder HTML-Wanzen werden blockiert.
- Langfristige Markierungen für das Tracking (Cookies, EverCookies) werden gelöscht oder eingesperrt.
- Features, die sich für Browser-Fingerprinting eignen, werden geringfügig mit zufälligen Werten manipuliert, so dass eine Wiedererkennung erschwert wird.
- ...

Das Spitzenprodukt beim Schutz gegen Tracking ist zweifellos der TorBrowser mit jahrelanger Erfahrung auf diesem Gebiet und der davon abgeleitete Mullvad Browser. Man könnte den Mullvad Browser empfehlen (mit ein paar Tipps, siehe Kapitel 5) und das Thema wäre ausreichend behandelt.

Der Mullvad Browser ist restriktiv konfiguriert, was zu einigen Einschränkungen führt. Er kann beispw. nicht für Videokonferenzen oder für WiFi Hotspot Logins genutzt werden. Die Medienwiedergabe ist etwas eingeschränkt und man kann keine Cookies u. ä. oder Login Credentials für ausgewählte Webseiten dauerhaft speichern, was manchmal praktisch wäre.

Deshalb gibt es für Firefox hier im Privacy-Handbuch ein abgestuftes Schutzkonzept inkl. ausführlicher Begründungen, so dass Interessierte selbst entscheiden können, welchen Schutz sie umsetzen möchten. Beim spurenarmen Surfen kommt es nicht unbedingt darauf an, zu 100% geschützt zu sein. Zugunsten des Komfort kann man Kompromisse machen.

Den Abschluss dieses Themas bildet eine kurze Vorstellung des Librewolf (Kapitel 6) als Alternative zum Firefox, der bei Auslieferung etwa auf dem mittleren Level des hier vorgestellten Konzeptes für Firefox mit dem man sich viele Anpasssungen erspart.

Anonymes Surfen hat eine etwas andere Zielstellung. Starke Anonymität soll Risikogruppen Schutz gegen Repressionen bieten. Es gibt sehr unterschiedliche Gründe, warum man Repressionen befürchten könnte. Minderheiten befürchten Repressionen durch die Majorität. Wer Regeln, Gesetze oder andere staatliche Vorgaben nicht respektieren möchte, muss Repressionen durch den Macht- bzw. Staatsapparat befürchten usw.

Durch starke Anonymisierung ist ein Tracking von einzelnen Individuen zur Erstellung von Persönlichkeitsprofilen natürlich auch unmöglich, ein positiver Nebeneffekt.

Im Gegensatz zum spurenamrmen Surfen kann man sich beim anonymen Surfen keine Kompromisse erlauben. Ein kleiner Fehler, der zur Deanonymisierung führen kann, ist nicht tolerierbar. Das Thema *Anonymität im Netz* wird im Kapitel 12 ausführlich behandelt.

Sicheres Surfen stellt den Schutz des eigenen Rechners und der lokalen Daten gegenüber Angriffen aus dem Internet in den Mittelpunkt.

- Wichtigste Punkte sind regelmäßige Updates von Browser und OS.
- Überflüssige Features deaktivieren, um die Angriffsfläche gering zu halten.
- Man kann den Browser gegen Angriffe härten (z. B. mit *apparmor*).
- Virtualisierung der Surfumgebung kann die lokalen Daten gegen erfolgreich kompromittierte Browser schützen.
- ...

Die Übergänge zwischen den Konzepten sind fließend, es gibt keine klaren Grenzen. Neben technischen Mitteln hängt es auch wesentlich vom eigenen Verhalten im Netz ab, ob man das angestrebte Ziel erreicht:

- Wer bei Facebook oder Twitter sein Leben postet, der nimmt damit natürlich die Auswertung der Daten für Marketingzwecke oder politische Kampagnen (z. B. zur Beeinflussung des Wahlverhaltens) in Kauf.
- Wer als Whistleblower nichtanonymisierte Dokumente versendet, die auf einen kleinen Personenkreis zurückgeführt werden können, riskiert seine Anonymität.[1]
- Wer sich aus dubiosen Quellen wahllos irgendwelche Software-Bundles installiert, riskiert die Sicherheit seines Systems.

4.1 Mozilla Firefox installieren

Firefox ist der Webbrowser der Mozilla Foundation. Er ist kostenfrei nutzbar und steht auf der Website des Projekts[2] für Windows, MacOS und Linux zum Download bereit.

Die *Extended Support Releases*[3] (ESR-Versionen) von Firefox werden im Gegensatz zu den vierwöchigen Updates des Firefox für ca. ein Jahr gepflegt. Es werden keine neuen Features eingebaut,

[1] https://heise.de/-3734142
[2] https://www.mozilla.org/en-US/firefox/all/
[3] https://www.mozilla.org/en-US/firefox/organizations/all.html

was sich positiv auf die Stabilität auswirkt. Allerdings fehlen damit aktuelle Verbesserungen und neue Features.

Download-Hinweis: der Download von Firefox von den offiziellen Downloadseiten ist einfach, aber dabei wird jeder Browser mit einer individuellen Kennung markiert. Diese Kennung wird dann bei der Installation und im Rahmen der Telemetrie verwendet, sodass Mozilla die Telemetriedaten eindeutig einem Download zuordnen kann. Außerdem wird die Download-ID und damit die gesamte Telemetrie einer Google-Analytics-Tracking-ID zugeordnet.[4]

Alternativ kann man das FTP-Verzeichnis[5] von Mozilla nutzen. Die dort heruntergeladenen Firefox-Browser für Windows und MacOS sind nicht markiert.

Linux-Distributionen bieten Firefox i. d. R. in den Repositorys zur Installation an (ohne individuelle Download-ID). Man kann ihn mit der bevorzugten Paketverwaltung installieren, wenn er nicht standardmäßig bei der Installation des Betriebssystems installiert wird.

Debian GNU/Linux und **RedHat** enthalten den Firefox ESR. Mit folgenden Kommandos wird der Browser aus den Repositorys installiert:

```
Debian:  > sudo apt install firefox-esr firefox-esr-l10n-de
RedHat:  > sudo yum install firefox
```

Fedora, openSUSE und **Linux Mint** enthalten den aktuellen Firefox in den Repositorys und installieren ihn standardmäßig bei der Installation des Betriebssystems.

Ubuntu und Derivate installieren Firefox als Snap-Package. Die Aktualisierung des Snap-Paketes ist nicht in den normalen Update-Prozess des Systems integriert und muss extra angestoßen werden. Außerdem gibt es Probleme mit *KeepassXC* und der Ressourcenbedarf ist größer.

Statt der Snap-Packages kann man den Firefox (oder Firefox ESR) aus dem PPA-Repository des Mozilla-Teams verwenden, der als normales DEB-Paket installiert wird.

1. Wenn man seine Firefox-Konfiguration behalten will, muss man die Daten aus dem Snap-Verzeichnis in das Verzeichnis $HOME kopieren:

   ```
   > cp -R ~/snap/firefox/.mozilla ~/
   ```

2. Dann ist der unerwünschte Firefox zu entfernen (Snap und transitionales DEB):

   ```
   > sudo snap remove firefox
   > sudo apt purge firefox
   ```

3. Als Nächstes ist das PPA-Repository des Mozilla-Teams zu aktivieren:

   ```
   > sudo add-apt-repository ppa:mozillateam/ppa
   > sudo apt update
   ```

4. Wenn man Firefox ESR bevorzugt, kann man ihn sofort installieren:

   ```
   > sudo apt install firefox-esr
   ```

   (Der Firefox ESR kann die alte Firefox-Konfiguration aber nicht übernehmen!)

[4] https://bug1677497.bmoattachments.org/attachment.cgi?id=9195911
[5] https://ftp.mozilla.org/pub/firefox/releases/

5. Wenn man die Release-Version von Firefox bevorzugt, muss man zuerst festlegen, dass der Firefox aus dem PPA-Repository des Mozilla-Teams gegenüber dem Snap-Paket der Distribution zu bevorzugen ist. Dafür speichert man im Verzeichnis */etc/apt/preferences.d/* die Datei *mozillateamppa* mit folgendem Inhalt:

```
Package: firefox*
Pin: release o=LP-PPA-mozillateam
Pin-Priority: 501
```

6. Dann kann man Firefox installieren:

```
> sudo apt install firefox
```

apparmor ist ein Sicherheitsframework für Linux. Als Mandatory Access Control System kontrolliert es einzelne Anwendungen und kann mit Profilen die Rechte von Anwendungen feingranular einschränken. Sollte eine Anwendung (z. B. Firefox) kompromittiert werden, kann der Angreifer nur wenig Schaden im System anrichten, wenn die Anwendung unter Kontrolle von *apparmor* läuft.

Um eine Anwendung wie Firefox unter die Kontrolle von apparmor zu stellen, braucht man ein passendes Profil, welches festlegt, was die Anwendung im Untergrund alles tun darf.

Für Firefox und Firefox ESR findet man apparmor Profile im Github Repository[6] von *gerrix1701*. Nach dem Download sind die Profile nach */etc/apparmor.d/* zu kopieren wie in der Anleitung auf Github beschrieben. Danach kann man die definierten Restriktionen durchsetzen mit:

```
> sudo aa-enforce usr.bin.firefox
```

Mit *sudo aa-status* kann man prüfen, ob Firefox im enforced mode unter Kontrolle von *apparmor* läuft, nachdem der Browser neu gestartet wurde.

Wenn Firefox mit diesen Profilen unter der Kontrolle von apparmor läuft, kann Firefox Dateien nur noch im Verzeichnis */Downloads* speichern und aus dem Verzeichnis */Public* lesen. Wenn man aus Bequemlichkeit auch auf die Verzeichnisse */Dokumente/...*, */Schreibtisch/...* oder */Bilder/...* lesend und schreiben zugreifen will, damit man sich das Kopieren der Dateien spart, könnte man im apparmor Profil die entsprechenden Freigaben hinzufügen:

```
...
owner @{HOME}/Dokumente/ r,
owner @{HOME}/Dokumente/* rw,
...
```

Damit werden die Sicherheitseinstellungen ein bisschen aufgeweicht, aber die kritischen Verzeichnisse bleiben weiterhin geschützt.

SELinux SELinux ist das bei Fedora und RedHat Linux standardmäßig eingesetzte Sicherheitsframework zur Einschränkung von Berechtigungen. Mit dem Tool *sandbox* kann Mozilla Firefox in ein geschlossenes Kompartment mit sehr restiktiven Rechten eingesperrt werden.

1. Als erstes sind die Sandbox und die dazu gehöhrenden Policies zu installieren:

[6] https://github.com/gerrix1701/apparmor-profiles/tree/main

```
> sudo dnd install policycoreutils-sandbox selinux-policy-sandbox
```

2. Dann ist ein Verzeichnis zu erstellen, das als $HOME-Verzeichnis für die Firefox Sandbox dienen soll, sowie darin ein Download Verzeichnis. Optional könnte man auch ein Upload Verzeichnis erstellen und das bisher genutzte Firefox Profil in die Sandbox zu kopieren:

   ```
   > mkdir ${HOME}/sandbox
   > mkdir ${HOME}/sandbox/Download
   # optional:
   > mkdir ${HOME}/sandbox/Upload
   > cp -r ${HOME}/.mozilla ${HOME}/sandbox/
   ```

3. Mit folgendem Kommando kann man Firefox in einer SELinux Sandbox starten:

   ```
   > sandbox -X -t sandbox_web_t -H ~/sandbox -w 1440x810 firefox
   ```

   Es wird ein eigener X-Server für die Sandbox gestartet mit separater Zwischenablage. Das kopieren von Texten via Clipboard zwischen dem sandgeboxten Firefox und Programmen außerhalb der Sandbox ist nicht möglich.

   Firefox kann die Ports 80 und 443 für den Internetzugriff nutzen (Faschist Firewall).

   Firefox hat nur Zugriff auf das mit der Option -H angegeben Verzeichnis, welches als $HOME Verzeichnis innerhalb der Sandbox verwendet wird.

   Die Fenstergröße der Sandbox, die gleichzeitig die Bildschrimgöße des neu gestarteten X-Servers ist, wird mit der Option -w angegeben. Diese Fenstergröße sollte etwas kleiner als der echte Bildschirm sein, damit man in andere Fenster wechseln kann, aber eine Größe von real existierenden Monitoren haben.

   In Fedora 37/38 gibt es keine Soundausgabe in der Sandbox - ungeeignet für Videos.

4. Um nicht jedesmal das Kommando im Terminal eingeben zu müssen, bieten die Linux Desktops (KDE, GNOME...) Möglichkeiten, einen Programmstarter zu erstellen.

5. Wenn der Start von Firefox in der Sandbox mit einer SELinux Warnmeldung abbricht, muss man wahrscheinlich folgende Rechte erlauben, um das Problem zu fixen:

   ```
   > sudo setsebool -P xserver_clients_write_xshm 1
   ```

Konfiguration von Firefox könnte man anpassen, wenn der Browser unter Kontrolle von apparmor oder in einer SELinux Sandbox läuft. Da es nicht sinnvoll ist, heruntergeladene Dateien direkt in einer anderen Anwendung zu öffnen, die vom Browserprozess gestartet wird (weil es häufig Probleme gibt, da diese Anwendungen andere Rechte benötigt), kann man diese Optionen unter *about:config* mit folgendem Parameter im Downloaddialog ausblenden:

```
browser.download.forbid_open_with = true
```

Der Downloaddialog bietet dann nur die Möglichkeiten zum Speichern oder Abbrechen.

4.2 Datenschutzfreundliche Schnellkonfiguration

Wer sich nicht mit den Details beschäftigen möchte, kann diese Anleitung zur Schnellkonfiguration nutzen, um Firefox datenschutzfreundlich zu konfigurieren.

Surfer haben sehr unterschiedliche Anforderungen bei der Nutzung eines Browsers. Einerseits gibt es Nutzer, die das Internet ohne Einschränkungen konsumieren wollen (neben dem multimedialen

Surferlebnis auch problemlos im Lieblingswebshop einkaufen und mit PayPal bezahlen). Auf der anderen Seite gibt es Enthusiasten, die im Interesse der Sicherheit deutliche Einschränkungen in Kauf nehmen und zufrieden sind, wenn sie HTML-Seiten lesen und kommentieren können. Man kann nicht alle Anforderungen mit einer Konfiguration erfüllen, deshalb drei Vorschläge:

Basisschutz: Schützt gegen Tracking mit Cookies/EverCookies und bekannte Trackingdienste mit großer Reichweite werden blockiert. Außerdem werden überflüssige Funktionen im Firefox deaktiviert und einige Sicherheitsfunktionen aktiviert.

Mit dieser Konfiguration funktionieren 99,9 % der Webseiten. Man kann shoppen, Bankgeschäfte erledigen, an Videokonferenzen teilnehmen oder sich bei sozialen Medien austoben.

- Das Add-on **uBlock Origin** ist ein einfach bedienbarer Tracking- und Werbeblocker, der mit Filterlisten arbeitet. Einen vorbereiteten Konfigurationsvorschlag findet man auf unserer Webseite, den man in den Einstellungen des Add-ons importieren.
- Außerdem sind einige Parameter unter *about:config* zu setzen, die auf unserer Webseite in der minimalen Konfiguration aufgezählt sind.[7]

Erweiterter Trackingschutz: Schützt gegen Tracking mittels Browser-Fingerprinting. iFrames werden standardmäßig blockiert. Es kann einige wenige kleine Einschränkungen und Verlangsamungen bei JavaScript-lastigen Webshops, Bankwebseiten o. Ä. geben. Durch das Blockieren von iFrames können Probleme mit Captchas auftreten.

Mit dieser Konfiguration funktionieren 95 % der Webseiten. Man kann News lesen, diskutieren, Videos konsumieren usw. Bei Bedarf kann man Add-ons auf einzelnen Webseiten deaktivieren.

- Für **uBlock Origin** stellen wir einen erweiterten Konfigurationsvorschlag bereit, der auch iFrames blockiert oder als click2load darstellt, um den Schutz zu verbessern.
- **Skip Redirect** entfernt Umleitungen in der URL. Diese Umleitungen werden genutzt, um die Klicks auf Links zu externen Domains zu tracken.
- **CanvasBlocker** kann Zugriffe auf Canvas-API, SVG-API, Screen usw. geringfügig modifizieren, um ein Fingerprinting des Browsers zu verhindern. Für die Konfiguration stellen wir einen Vorschlag auf unserer Webseite bereit. (Nur für Firefox 115.x ESR!)
- Außerdem sind einige Parameter unter *about:config* zu setzen, die auf unserer Webseite in der moderaten user.js Konfiguration aufgezählt sind.

  In der medium-strengen user.js Konfiguration werden zur Verbesserung der Sicherheit zus. einige Funktionen deaktiviert, um die Angriffsfläche zu verkleinern.

Hohe Sicherheitsanforderungen: es wird zusätzlich die Angriffsfläche verringert, indem Features deaktiviert werden, die potentiell kompromittierbare Daten aus dem Internet an Bibliotheken des Betriebssystems weiterleiten, wo sie möglicherweise das System gefährden. Diese Konfiguration verhunzt viele Webseiten und man braucht Frustrationstoleranz!

- Die Add-ons **uBlock Origin** und **SkipRedirect** kann man wie beim erweiterten Trackingschutz verwenden.
- **NoScript** verwaltet Freigaben für JavaScript, WebGL, iFrames usw. Für die Erstkonfiguration kann man den Vorschlag des PrHdb-Teams verwenden, den man in die NoScript-Einstellungen importieren kann.

[7] https://www.privacy-handbuch.de/handbuch_21u.htm

- **JShelter** ist ein Add-on zum Schutz gegen Browserfingerprinting, dass etwas umfangreicher eingreift als CanvasBlocker. Es werden Timer-APIs gefakt und die Webworker linearisiert, was zu Problemen mit Captchas führt. (Nur für Firefox 115.x ESR!)
- Außerdem sind einige Parameter unter *about:config* zu setzen, die auf unserer Webseite in der medium-strengen oder strengen user.js Konfiguration aufgezählt sind.

Optional: Es gibt noch Add-ons, die für die Privatsphäre nicht relevant, aber dennoch sinnvoll sein und gefahrlos installiert werden können:

Das Add-on **Binnen-I be gone** ersetzt ideologisch motivierte Sprachverhunzungen wie *Politiker*innen* oder *Panzerfahrer_Innen*, die man nicht aussprechen oder in andere Sprachen übersetzen kann, die laut Duden kein korrektes Deutsch sind und vom Rat für Deutsche Rechtschreibung nicht empfohlen werden, durch das grammatikalische Generikum.

(Ein Tipp für alle, die sich politisch korrekt ausdrücken wollen: Der Duden gibt Hinweise zum sprachlich korrektem Gendern und diese Verballhornungen gehören amtlich nicht dazu. Sprache muss man sprechen können. Die Verwendung von Binnen-Is ist kein amtlich korrektes Deutsch und demonstriert ideologische Verblendung.)

Um die Installation von datenschutzfreundlichen **Suchmaschinen** zu vereinfachen, sind einige Such-Plugins vorbereitet. Wenn man die folgende Website aufruft, kann man auf die drei Punkte in der URL-Zeile klicken und in dem ausklappenden Menü die gewünschten Suchmaschinen hinzufügen: https://www.privacy-handbuch.de/handbuch_21browser.htm

Das funktioniert auch auf den Webseiten der Suchmaschinen.

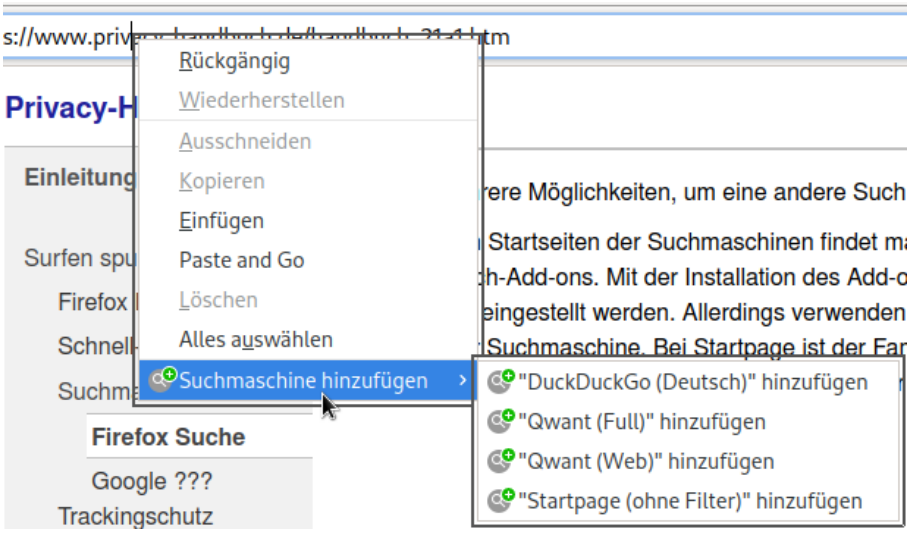


Abbildung 4.1: Suchmaschinen hinzufügen

4.3 Datensparsame Suchmaschinen

Am häufigsten werden Suchmaschinen für die Orientierung im Web genutzt. Neben den bekannten Datensammlern wie Google, Bing oder Yahoo! gibt es jedoch auch Alternativen.

Für alle alternativen Suchmaschinen gilt, dass sie eine andere Sicht auf das Web bieten und die Ergebnisse sich von Google unterscheiden. Man sollte bei der Beurteilung der Ergebnisse

beachten, dass auch Google nicht die reine Wahrheit bieten kann, sondern nur eine bestimmte Sicht auf das Web.

Bisher ist es so, dass man eine Frage oder ein paar kurze Stichworte an eine Suchmaschine schickt und man bekommt als Ergebnis eine Liste von Webseiten, auf denen man (möglicherweise) passende Antworten findet. Die Reihenfolge ist dabei das Geheimnis der Suchmaschinen.

Zukünftig wird es durch die Einführung von Chat-KIs Umwälzungen geben. Suchmaschinen werden ihre Chat-KIs in die Suche integrieren und diese sollen Fragen direkt beantworten, ohne das man als Suchender erst andere Webseiten abklappern muss. Die direkten Antworten von Chat-KIs werden bequem sein. Aber man sollte sich darüber klar sein, dass diese Antworten nicht immer objektiv und neutral sind. Aktuell beeindruckt Microsofts ChatGPT nicht nur durch sprachlich perfekte Ausdrucksweise sondern auch damit, dass sie komplett falsche Dinge mit großer Überzeugungskraft behauptet.

Suchmaschinen mit eigenem Index

Es ist nicht einfach, eine Suchmaschine aufzubauen, die die Privatsphäre respektiert, einen umfangreichen Index zur Verfügung stellt, gute Ergebnisse liefert und finanziell überleben kann.

Qwant (https://www.qwant.com/) Das Projekt wird seit 2011 als europäische Alternative zu Google mit 50 Millionen Euro von der EU gefördert, kann bisher aber alleine keine gleichwertigen Ergebnisse liefern und kooperiert deshalb mit Bing. Auch finanziell konnte Qwant keine Unabhängigkeit aufbauen und musste 2022 einen Kredit über 8 Millionen Euro von Huawei annehmen, um überleben zu können.

Es gibt eine JavaScript-freie Lite-Version (aber die Suchergebnisse sind mit Freigabe von JavaScript irgendwie besser) und die Kindersuchmaschine Qwant Junior.[8]

Qwant hat 2022 ein dreistufiges Filtersystem für Suchergebnisse eingeführt:

1. In der untersten Filterstufe setzt Qwant die EU-Verordnungen zur Zensur um. Das betrifft derzeit russische Nachrichtenmedien wie RT DE, die gemäß Anordnung aus Brüssel aus dem Index entfernt werden müssen. Aber die als Antwort darauf eingerichteten Domains wie https://www.rtde.site sind in den Suchergebnissen enthalten.
2. Die moderate Stufe ist standardmäßig aktiv und entspricht dem betreuten Suchen bei DuckDuckGo. Es werden gesäuberte Suchergebnisse präsentiert, die weniger Fake News oder abweichende Meinungen zu Corona, russischer Propaganda o. Ä. enthalten. Proxy-Domains für russische Medien werden bspw. bei den Ergebnissen nicht mehr angezeigt.
3. In der Filterstufe *strikt* wird ein gewalt- und pornofreies, familienfreundliches Teletubby-Internet präsentiert.

In den Sucheinstellungen kann man die Filterstufe wählen und als Cookie oder URL-Parameter speichern. Die Einstellungen öffnet man mit Klick auf das Zahnradsymbol auf der Webseite. Außerdem kann man auf der Website des Privacy-Handbuchs einfach ein Such-Plug-in in der niedrigsten Filterstufe installieren.

Eric Leandri war einer der Gründer von Qwant und wurde als *Mr. Privacy* gefeiert. Im Jahr 2020 hat er Qwant verlassen, die Seite gewechselt und die Firma Altrnativ gegründet. Diese Firma stellt ihre Kompetenz beim Durchsuchen öffentlicher Daten zahlungskräftigen Kunden

[8] https://www.qwantjunior.com/

zur Ausspähung der Konkurrenz und den französischen Geheimdiensten zur Überwachung des Web zur Verfügung. Frankreich hat eine lange Tradition bei der Überwachung des Internet (French-Echelon usw.) und damit kann man bestimmt gut Geld verdienen. Es gibt aber keine Anzeichen dafür, dass die Firma Altrnativ irgendwie die Arbeit von Qwant beeinflusst.

DuckDuckGo.com (https://duckduckgo.com) DuckDuckGo ist eine datenschutzfreundliche Suchmaschine. Es gibt eine JavaScript-freie Version (HTML), aber die Ergebnisse der JavaScript-Version sind irgendwie besser. Neben der eigentlichen Suche bietet DuckDuckGo viele nette Erweiterungen. Das Suchfeld kann als Taschenrechner oder zum Umrechnen von Einheiten genutzt, Fragen nach dem Wetter werden beantwortet (englisch: *weather:*) usw.

In den DuckDuckGo-Settings kann man die Sucheinstellungen konfigurieren. Die Einstellungen werden in Cookies oder als URL-Parameter gespeichert.[9]

DuckDuckGo manipuliert seit März 2022 die Suchergebnisse. Auf Wunsch der EU-Führung werden staatlich finanzierte Webseiten mit *feindlicher* Propaganda aus dem Index entfernt. Außerdem wird die Relevanz von Webseiten reduziert, die nach irgendwelchen Kriterien der *Desinformation* verdächtigt werden, ohne sie komplett aus dem Index zu werfen. Bevormundung nach undurchsichtigen Kriterien gibt es seit Jahren auch bei Google.

Nicht alle Nutzer von DuckDuckGo waren von dieser Entwicklung begeistert:

> *We want a privacy-centric search engine . . . not your opinion.*
>
> *I don't need mommy anymore. I'm grown up; thread me as such.*
>
> *Your neutrality was your value. Now you became but Google 2, the poorer version of the same wokism.*

Mojeek (https://www.mojeek.com) Mojeek.com ist eine kleine (aber aufstrebende), datenschutzfreundliche Suchmaschine mit eigenem Index, die bei der Suche nach *Lauterbach lügt* ca. 3.000 passende Suchergebnisse liefert (Google.de findet 102.000, allerdings auf den ersten Ergebnisseiten auch viele unpassende).

Mojeek hat das Ziel, neutrale Suchergebnisse ohne moralische Bevormundung zu liefern. Alternative Medien sind deutlich besser platziert als bei Google oder DuckDuckGo, die offizielle, westeuropäische Nachrichtenseiten vergleichsweise deutlich bevorzugen.

mojeek.com alleine ist auf Dauer etwas mager aber es ist in jedem Fall eine Option, die die Ergebnisse von searX(NG) Metasuchmaschinen um interessante Facetten bereichert. Man kann Mojeek in den Einstellungen der bevorzugten searX(NG) Instanz aktivieren.

Proxy-Suchmaschine

Eine Proxy-Suchmaschine leitet die Suchanfrage an einen anderen Suchdienst weiter, um die Privatsphäre der Nutzer etwas zu schützen, und sortiert die Ergebnisse neu.

Startpage (https://startpage.com/) bietet datenschutzfreundlichen Zugriff auf die Google-Suche. Dabei werden eindeutig identifizierende Informationen über den Surfer entfernt. Um Missbrauch zu verhindern und Werbung von Google Adwords einzublenden, werden aber einige Informationen über den Browser an Google weitergegeben, siehe Privacy Policy:

[9] https://duckduckgo.com/settings

> *Unsere Suchergebnisse können ein paar klar gekennzeichnete gesponserte Links enthalten, mit denen wir Geld verdienen und unsere Betriebskosten decken. Diese Links werden von Plattformen wie Google Adwords abgerufen. Um Klickbetrug zu verhindern, werden einige nicht-identifizierende Systeminformationen gemeinsam genutzt.*

Bei Startpage ist standardmäßig ein *Family-Filter* aktiv. Wer etwas Anstößiges sucht, erhält keinen Hinweis auf den Filter sondern nur:

> *Es wurden keine mit Ihrer Suchanfrage übereinstimmenden Dokumente gefunden.*

In den Startpage-Settings kann man den *Family-Filter* deaktivieren und weitere Einstellungen vornehmen. Sie werden in Cookies oder als URL-Parameter gespeichert.[10]

Metasuchmaschinen

Metasuchmaschinen leiten die Suchanfrage an eine oder mehrere Suchmaschinen weiter. Sie sammeln die Ergebnisse ein und sortieren sie neu. Außerdem schützen sie die Privatsphäre der Nutzer, indem sie deren Identität gegenüber den angefragten Suchmaschinen verbergen.

SearXNG (https://searx.space) ist eine Open-Source-Metasuche, die man auch für sich selbst betreiben könnte, wenn man sich einarbeitet. Es gibt viele SearX-Instanzen, die man probieren kann. Die Qualität der Suchergebnisse ist unterschiedlich. Populäre SearX-Instanzen werden von Suchmaschinen öfters blockiert, wenn sie viele Anfragen stellen.

Da SearXNG nicht mit Werbung finanziert wird, werden im Gegensatz zu Startpage oder Metager keine Daten an Dritte weitergegeben.

Die Einstellungen für die Suche (welche Suchmaschinen genutzt werden sollen, welche Sprache bevorzugt werden soll, Autoscrolling usw.) kann man in den Einstellungen auf den Such-Webseiten konfigurieren und als Cookies speichern. Die angegebene Parameter-URL gilt nur für eine einzige Anfrage, bei Änderung der Suchanfrage werden wieder die Default-Einstellungen genutzt. Um die Einstellungen längerfristig zu behalten, muss man die Cookies für die Domain dauerhaft speichern (siehe Abschnitt *Cookies*)

Hinsichtlich Zensur sind die SearXNG Instanzen von den Suchmaschinen abhängig, die die Ergebnisse zuliefern. Durch die Kombination von verschiedenen Suchmaschinen aus unterschiedlichen Regionen der Welt mit unterschiedlichen Zensurschwerpunkten kann man ein relativ unzensiertes Gesamtergebnis erreichen. Neben Qwant und DuckDuckGo als Suchmaschinen mit Zugriff auf einen großen Index könnte man Mojeek, Naver und Seznam aktivieren, um eine breitere Auswahl an Ergebnissen zu bekomen.

Metager.de (https://www.metager.de/) ist ein deutscher Klassiker vom Suma e. V. Mit JavaScript sieht die Seite etwas besser aus, funktioniert aber auch ohne JavaScript. Die Suchmaschine ist auch als Tor-Onion-Service verfügbar.

Metager finanziert sich ebenfalls aus Werbung. Um die Relevanz der Werbeanzeigen etwas zu verbessern, werden Informationen aus der User-Agent-Kennung des Browsers und die ersten beiden Blöcke der IP-Adresse des Surfers zusammen mit der Suchanfrage an die Werbepartner weitergegeben.

Metager braucht einen Proxy, um Ergebnisse aus der Suchliste anonym aufzurufen. Der Link ist unter dem Ergebnis zu finden und das Add-on *Skip Redirect* muss deaktiviert

[10] https://www.startpage.com/do/settings

werden, wenn man den Metager-Proxy verwenden will. Der Proxy entfernt JavaScript und viele Bilder:

Spezielle Anwendungsfälle

- Wikipedia kann man auch ohne Umweg über Google direkt fragen, wenn man Informationen sucht, die in einer Enzyklopädie zu finden sind.
- Statt Google übersetzen zu lassen, kann man DeepL[11] nutzen. Der Translator kennt neben Englisch und Deutsch weitere Sprachen.

Google ???

Anfang Februar 2012 hat Google seine Suchmaschine überarbeitet. Die Webseite macht jetzt intensiven Gebrauch von JavaScript. Eine vollständige Analyse der verwendeten Schnüffeltechniken liegt noch nicht vor. Einige vorläufige Ergebnisse sollen kurz vorgestellt werden:

Einsatz von EverCookies: Der Surfer wird mit EverCookie-Techniken markiert. Die Markierung wird im DOMStorage gespeichert. Der DOMStorage wurde vom W3C spezifiziert, um Web-Applikationen die lokale Speicherung größerer Datenmengen zu ermöglichen und damit neue Features zu erschließen. Google wertet die User-Agent-Kennung und weitere Informationen über den Browser aus, um die Möglichkeit der Nutzung des DOMStorage erst einmal zu prüfen und gegebenenfalls Alternativen wie normale Cookies zu verwenden.

Tracking der Klicks auf Suchergebnisse: Bei Klick auf einen Link in den Suchergebnissen wird die Ziel-URL umgeschrieben. Aus der für den Surfer sichtbaren Zieladresse

```
https://www.privacy-handbuch.de/index.htm
```

wird im Moment des Klick eine Google-URL:

```
https://www.google.de/url?q=https://www.privacy-handbuch.de/...
```

Die zwischengeschaltete Seite enthält eine 302-Weiterleitung auf die ursprüngliche Ziel-URL. Der Surfer wird also fast unbemerkt über einen Google-Server geleitet, wo der Klick registriert wird. Bei deaktiviertem JavaScript ist stets die Google-URL sichtbar, nicht die Zieladresse.

Diese Umschreibung der Links gibt es auch bei Bing, Facebook, YouTube und anderen Datensammlern. Das Firefox-Add-on **Skip Redirect** entfernt diese Umleitungen. Es ist natürlich besser, eine datenschutzfreundliche Suchmaschine zu nutzen statt Google.

[11] https://www.deepl.com/translator

Browser-Fingerprinting: Mittels JavaScript wird die innere Größe des Browserfensters ermittelt. Folgenden Code findet man in den Scripten:

```
I[cb].oc= function() {
var a=0, b=0;
self.innerHeight?(a=self.innerWidth,b=self.innerHeight):....;
return {width:a, height:b}
};
```

Die ermittelten Werte werden als Parameter *biw* und *bih* der Google-URL übergeben. Sie haben aber keinen Einfluss auf die Bildschirmdarstellung. Auch wenn das Browserfenster zu klein ist und die Darstellung nicht passt, bleibt die Größe der HTML-Elemente erhalten.

Die inneren Abmessungen des Browserfensters sind sehr individuelle Parameter, die vom Betriebssystem und den gewählten Desktop-Einstellungen abhängig sind. Sie werden von der Schriftgröße in der Menüleiste, der Fensterdekoration, den aktivierten Toolbars der Desktops bzw. der Browser usw. beeinflusst. Sie sind für die Berechnung eines individuellen Fingerprints des Browsers gut geeignet. Anhand des Browser-Fingerprints können Surfer auch ohne Cookies oder EverCookies wiedererkannt werden. Die Google-Technik kann dabei besser differenzieren als das Projekt Panopticlick der EFF, das bereits 80 % der Surfer eindeutig identifizieren konnte.

Auf der Webseite der Google-Suche kann man dem Tracking kaum entgehen. Wer unbedingt die Ergebnisse von Google braucht, kann die Suchmaschine *Startpage.com* als anonymisierenden Proxy nutzen.

4.3.1 Suchmaschinen in Firefox hinzufügen

Es gibt mehrere Möglichkeiten, um eine andere Suchmaschine als Google zu nutzen:

1. Auf den Startseiten der Suchmaschinen kann man mit einem Klick der rechten Maustaste in der Adressleiste ein Menü öffnen, wo man die Option zur Installation des Such-Add-ons findet. Nach dem Hinzufügen kann man sie in den Einstellungen zur Standardsuche machen. Allerdings verwenden diese Such-Add-ons die Standardeinstellungen der Suchmaschine. Bei Startpage ist der Familienfilter aktiv, bei DuckDuckGo werden die Suchanfragen per GET gesendet und sind in der History lesbar: suboptimal.
2. Mit den Startpage-[12] oder DuckDuckGo[13]-Settings kann man die Suche konfigurieren:
   - Man kann die Filter abschalten, um mal nach schmuddeligen Dingen zu suchen.
   - Man kann die Suchanfragen von HTTP-GET auf HTTP-POST umstellen, damit die Suchbegriffe nicht in der URL auftauchen und nicht in der History angezeigt werden.
   - Man kann das Laden des Favicons deaktivieren, damit man weniger Spuren in den Logs der Webserver hinterlässt.
   - Man kann die Anzahl der angezeigten Suchergebnisse pro Seite anpassen, die Sprache für die Webseite auf Deutsch und das Farbschema einstellen.
   - ...

[12] https://www.startpage.com/do/settings
[13] https://duckduckgo.com/settings

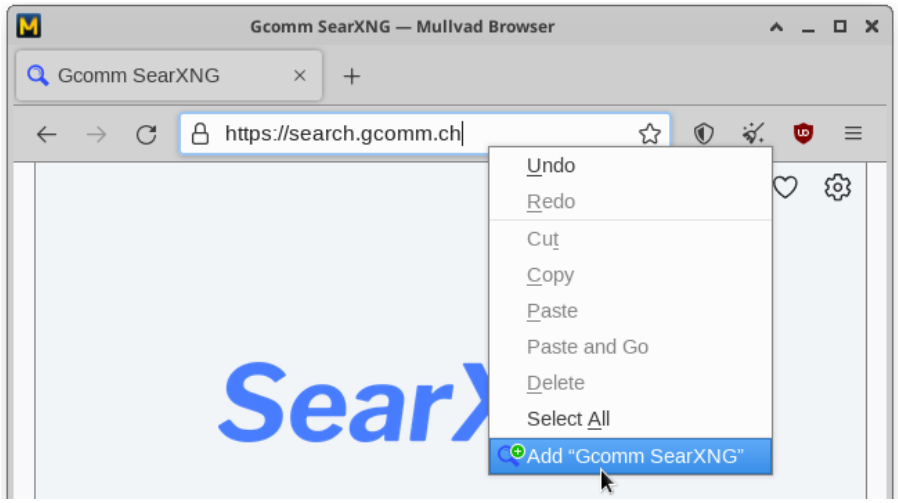
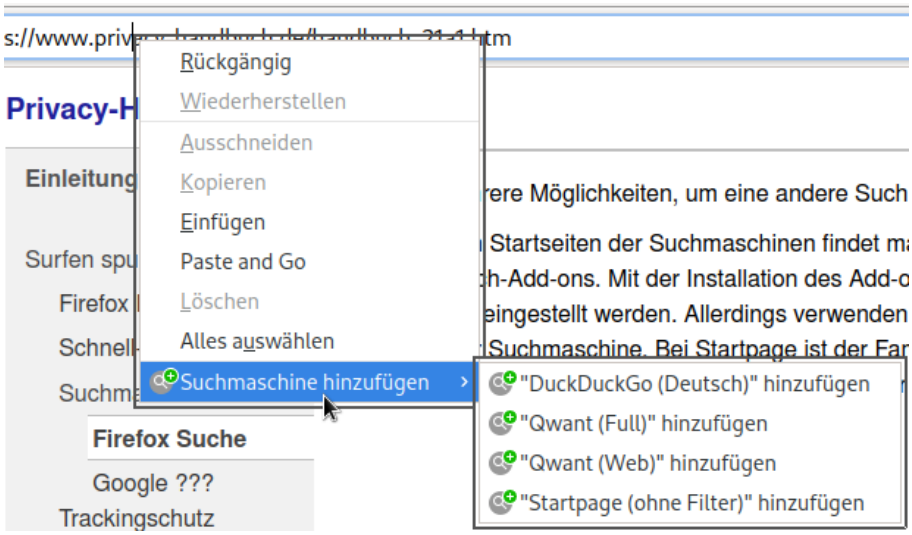


Abbildung 4.2: Suchmaschinen-Plugin auf der Webseite der Suchmaschine hinzufügen

Die Einstellungen für die Suche werden in Cookies gespeichert oder als URL-Parameter angegeben. Da die meisten Leser die Cookies regelmäßig löschen werden, sind die URLs mit den Parametern wahrscheinlich das Mittel der Wahl. Die Adressen kann man als Lesezeichen speichern oder man setzt sie als Firefox-Startseite und New-Tab-Page, um sie schnell aufzurufen.

3. Wenn man auf der Webseite des Privacy-Handbuches zum Thema Suchmaschinen ist, kann man mit eienm Rechtsklick in der URL-Leiste angepasste Such-Plug-ins für Startpage (DE, ohne Filter), DuckDuckGo (DE) oder Qwant (ohne Filter) installieren.



4.3.2 Defaultsuchmaschine konfigurieren

Nach der Installation einiger Such-Plug-ins kann man in den Einstellungen von Firefox die Suchmaschinen anpassen, die standardmäßig installierten Suchmaschinen deaktivieren und **eine datenschutzfreundliche Default-Suche wählen** (Abb. 4.3).

Die Default-Suche wird an mehreren Stellen von Firefox ohne weitere Nachfrage genutzt. Es sollte eine datenschutzfreundliche Suche ausgewählt werden.

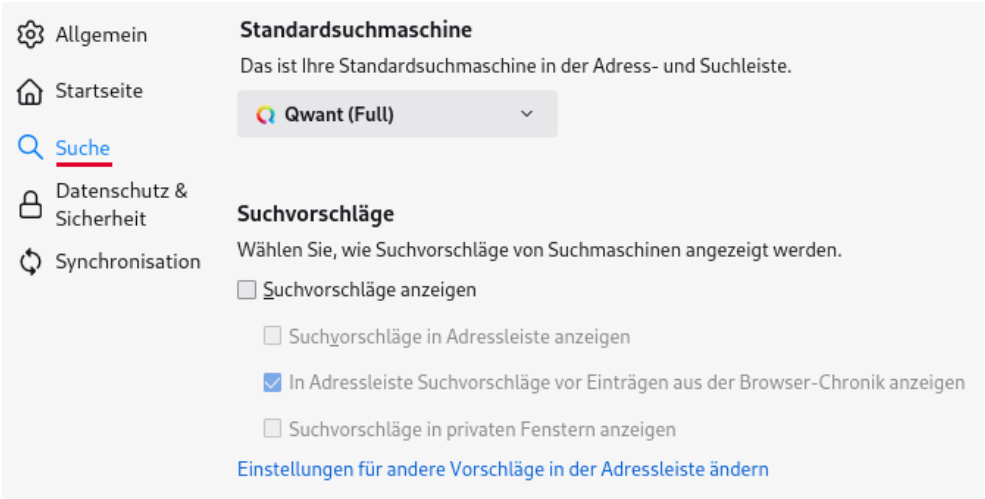


Abbildung 4.3: Default-Suchmaschine auswählen

Die standardmäßig im Firefox installierten Suchmaschinen verraten überflüssige Informationen über die Installation. Wenn man z. B. unter Ubuntu den Firefox aus dem Repository nutzt, wird bei jeder Suchanfrage ein Hinweis auf Ubuntu angehängt:

```
https://www.google.de/search?...&client=ubuntu

http://www.amazon.com/s?...&tag=wwwcanoniccom-20
```

Nimmt man den offiziellen Firefox für Windows von der Mozilla-Downloadseite, dann werden folgende Informationen angehängt:

```
https://www.google.de/search?...&rls=org.mozilla:de:official

http://www.amazon.com/s?...&tag=firefox-de-21
```

Diese Parameter in der Suchanfrage können einen User-Agent-Fake entlarven.

4.3.3 Vorschläge bei Eingabe einer URL reduzieren

Um die Anzeige von Vorschlägen bei der Eingabe einer URL etwas zu reduzieren, kann man die Suchfunktion bei URL-Eingaben abschalten (wenn man suchen will, dann verwendet man das Suchfeld). Wenn die Anzeige von Suchvorschlägen aktiv ist, wird jede Tasteneingabe bei Eingabe einer URL an die gewählte Standardsuchmaschine gesendet. Das möchte man nicht unbedingt, daher ist dieser Parameter relevant für die Privatsphäre:

```
browser.urlbar.suggest.searches = false
```

Firefox zeigt bei Eingabe einer Adresse in der URL-Leiste eine handverlesene und gesponserte Liste von Vorschlägen an. Das deaktiviert man mit folgenden Optionen:

```
browser.urlbar.suggest.topsites    = false
browser.urlbar.groupLabels.enabled = false
```

Wer nicht mit Vorschlägen belästigt werden möchte, kann weitere Werte deaktivieren, bspw. die Vorschläge aus den geöffneten Seiten oder Lesezeichen, da man auf diese Quellen direkt zugreifen kann, wenn man möchte.

```
browser.urlbar.suggest.openpage = false
browser.urlbar.suggest.bookmark = false
browser.urlbar.suggest.history  = false
```

Mit Firefox 110 hat Mozilla begonnen, die *quicksuggestions* als weiteres Empfehlungsfeature in einigen Regionen zu aktivieren. Dabei werden bei Eingabe einer URL nicht-gesponserte und gesponserte Vorschläge angezeigt sowie Vorschläge, die Mozilla aus den Suchanfragen ableitet. Mit folgenden Optionen kann man *quicksuggestions* abschalten:

```
browser.urlbar.quicksuggest.enabled                = false
browser.urlbar.quicksuggest.dataCollection.enabled = false
browser.urlbar.quicksuggest.showedOnboardingDialog = true
browser.urlbar.suggest.quicksuggest.nonsponsored   = false
browser.urlbar.suggest.quicksuggest.sponsored      = false
```

Außerdem könnte man die Anzeige der Suchmaschinen bei URL-Eingabe abschalten:

```
browser.urlbar.engines = false
```

4.4 Cookies und EverCookies

Cookies werden für die Identifizierung des Surfers genutzt. Neben der erwünschten Identifizierung, um personalisierte Inhalte zu nutzen, bspw. einen Web-Mail-Account oder um Einkäufe abzuwickeln, werden sie für das Tracking von Surfern verwendet.

Der Screenshot auf Abb. 4.4 zeigt die Liste der Cookies, die bei einem einmaligen Aufruf der Seite *www.spiegel.de* im Jahr 2011 gesetzt wurden. Es war nicht ungewöhnlich, dass populäre Webseiten mehrere Datensammler einbinden. Eine Studie der Universität Berkeley[14] hat 2011 beim Surfen auf den Alexa-TOP100-Webseiten 5.675 Cookies gefunden (ohne Login oder Bestellung). Von diesen wurden 4.914 Cookies von Dritten gesetzt, also nicht von der aufgerufenen Webseite. Die Daten wurden an mehr als 600 Server übermittelt. Spitzenreiter unter den Datensammlern ist Google: 97 % der populären Webseiten setzen Google-Cookies.

Immer mehr Trackingdienste sind inzwischen dazu übergegangen, die Cookies im First-Party-Context zu setzen, da Cookies von Drittseiten einfach blockierbar sind.

- Eine empirische Studie der Universität Leuven von 2014 zeigte, dass damals bereits 44 Trackingdienste mehr als 40 % des Surfverhaltens auch dann verfolgen konnten, wenn man Cookies für Drittseiten blockierte und nur First-Party-Cookies erlaubte.[15]

  Ein Beispiel ist der Trackingdienst WebTrekk, der sich auf Webseiten wie *heise.de, zeit.de* oder *zalando.de* mit DNS-Aliases wie *prophet.heise.de* als Subdomain der überwachten Webseite First-Party-Status erschleicht, um seine Trackingcookies zu setzen.[16]

[14] http://heise.de/-1288914
[15] https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf
[16] https://anonymous-proxy-servers.net/blog/index.php?/archives/377-Tracking-mit-Cookies.html

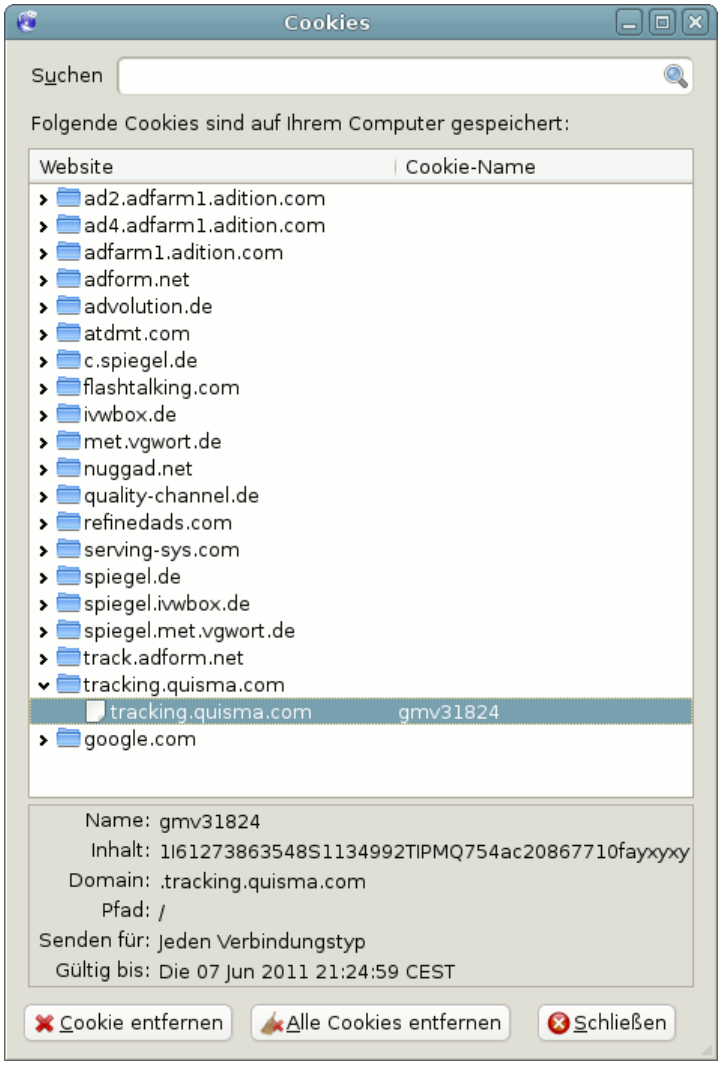


Abbildung 4.4: Liste der Cookies beim Besuch von Spiegel-Online 2011

- Google kombiniert seit 2017 den Dienst Analytics mit dem AdWords-Tracking, um den Trackingschutz von Apples Browser Safari zu umgehen. Für Google Analytics bindet der Webmaster Trackingcode direkt auf der Webseite ein, der damit First-Party-Status erhält und die Cookies für das AdWords-Tracking setzt.[17]
- Microsoft folgte im Januar 2018 und setzte eine Lösung um, die das Cookie mit der Microsoft-Click-ID für das Conversation-Tracking im First-Party-Context setzt. Die Microsoft-Tracking-ID wird als URL-Parameter übertragen und dann von einem JavaScriptchen in ein Cookie geschrieben.[18]
- Facebook folgte den Beispiel von Google und Microsoft im Herbst 2018, nachdem Mozilla angekündigt hatte, nach dem Vorbild von Safari das Tracking via Third-Party-Cookies in Firefox zu erschweren. Wie bei Microsoft wird die Tracking-ID in URL-Parametern übertragen und dann mit Javascript in First-Party-Cookies geschrieben.[19]

Der Screenshot in Abb. 4.5 von 2022 zeigt die Veränderung bei einem einmaligen Aufruf der Seite *www.spiegel.de*. Die meisten Trackingdienste sind mit verschiedenen Tricks dazu übergegangen, Cookies im First-Party-Context zu platzieren. Dabei werden 22 Cookies im First-Party-Context geschrieben. Nur drei Trackingdienste schreiben ihre Cookies noch als Drittseite.

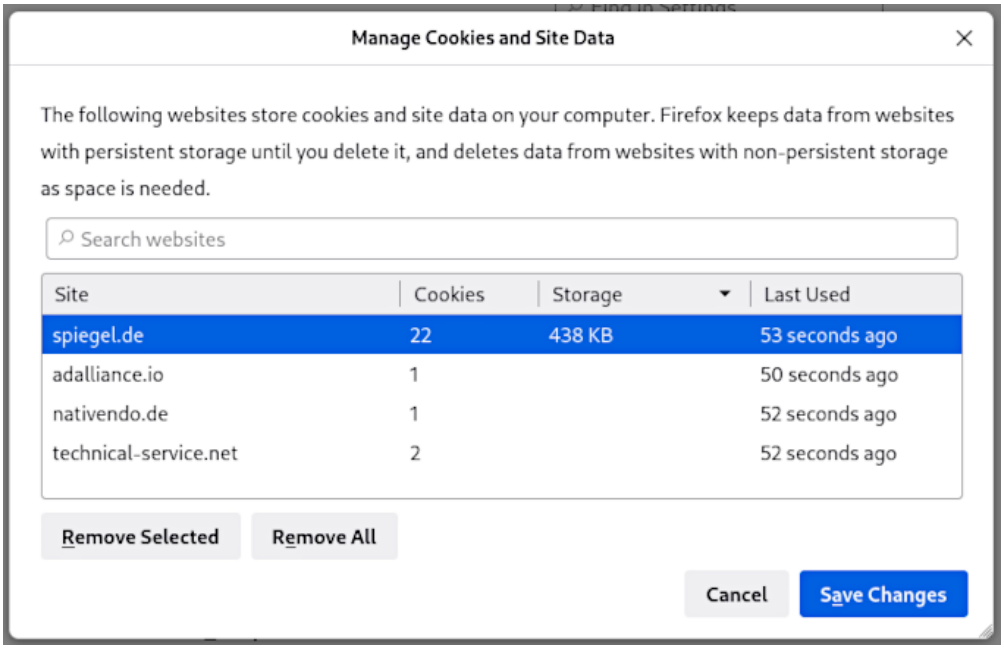


Abbildung 4.5: Liste der Cookies beim Besuch von Spiegel-Online 2022

Google hat im Nov. 2023 angekündigt, die Unterstützung für Drittseitencookies bis Ende 2024 aus dem Browser Chrome zu entfernen. Damit wird sich die Trackingbranche endgültig umstellen müssen und es werden dann auch die letzten Cookies von Drittseiten verschwinden.[20]

[17] https://www.heise.de/-3859526
[18] https://advertise.bingads.microsoft.com/en-us/blog/post/january-2018/conversation-tracking-update-on-bing-ads
[19] https://marketingland.com/facebook-to-release-first-party-pixel-for-ads-web-analytics-from-browsers-like-safari-249478
[20] https://www.bleepingcomputer.com/news/google/google-shares-plans-for-blocking-third-party-cookies-in-chrome/

EverCookies – never forget

Als EverCookies bezeichnet man den Missbrauch unterschiedlicher Webtechniken zur individuellen Markierung von Surfern für Trackingzwecke. Es werden eindeutige Markierungen im HTML5-Storage oder in die IndexedDB geschrieben, ETags für das Cache Management können Tracking-IDs enthalten, TLS-Session und HSTS können für das Tracking missbraucht werden u. a. m.

Trackingcookies konnten lange Zeit anhand dieser Markierungen wiederhergestellt werden, auch wenn alle Cookies gelöscht worden waren. Moderne Browser bieten inzwischen Schutzmöglichkeiten gegen diese Trackingverfahren.

- Nach empirischen Untersuchungen der University of California nutzten 2012 bereits 38 % der TOP100-Websites verschiedene EverCookies zur Markierung der Surfer.
- Laut Web Privacy Census 2015 wurden drei Jahre später EverCookie-Techniken von 76 % der TOP100-Websites zum Tracking eingesetzt.

NSA und Co.

Die Trackingcookies wurden auch von der NSA und GCHQ im Rahmen der globalen Überwachung genutzt. Die Geheimdienste beobachteten den Datenstrom und identifizierten Surfer anhand langlebiger Trackingcookies. Zielpersonen wurden anhand dieser Cookies verfolgt und bei Bedarf mit Foxit Acid angegriffen, wenn die Identifikation über zwei Wochen stabil war. Mit der Verbreitung von HTTPS und des HTTPS-only-Mode wurden NSA und GCHQ diese Möglichkeiten genommen.

1: Schutz gegen Website-übergreifendes Tracking

Gegen Tracking mit Cookies und EverCookies über mehrere Websites bzw. Domains schützen Surf-Container (s. u.). Es wird für jede Domain in der URL-Leiste gemäß Same-Origin-Policy automatisch ein neuer Surf-Container erstellt und alle Daten werden abgeschottet in diesem individuellen Context gespeichert. Für unterschiedliche Websites ergeben sich damit unterschiedliche Tracking-IDs in Cookies und HTML5-Storage sowie unterschiedliche ETags im Cache und den TLS-Sessions usw.

Für Firefox besteht das Schutzkonzept aus den beiden Komponenten *Netzwerk-Partitionierung* und *Total Cookie Protection*, die das veraltete *FirstParty.Isolate* abgelöst haben.

1. Die *Netzwerk-Partitionierung* isoliert alle Cache-Speicher (HTTP, Bilder oder Fonts) sowie SSL-Session-IDs, HSTS, OCSP, DNS usw. in getrennten Containern für jede First-Party-Domain und ist in Firefox standardmäßig aktiviert.
2. *Total Cookie Protection* ist das Konzept zur Isolation von Cookies, Third-Party Cookies, DOMStorage und IndexDB in getrennten Containern für jede Domain. Dieses Feature ist in Firefox ebenfalls standardmäßig aktiviert.

2: Schutz gegen langfristiges Tracking

Langfristiges Tracking mit Cookies und allen möglichen Varianten von EverCookies verhindert man mit dem Löschen aller angesammelten Daten beim Schließen des Browsers:

```
privacy.history.custom                = true
privacy.sanitize.sanitizeOnShutdown   = true
privacy.clearOnShutdown.cache         = true
privacy.clearOnShutdown.cookies       = true
privacy.clearOnShutdown.downloads     = true
privacy.clearOnShutdown.history       = true
privacy.clearOnShutdown.sessions      = true
privacy.clearOnShutdown.offlineApps   = true
```

Wenn man gründlich sein will, könnte man zusätzlich folgende Daten bereinigen:

```
privacy.clearOnShutdown.siteSettings  = true
```

Es besteht manchmal der Wunsch, dass man ein paar Cookies für einzelne Domains behält und beim Beenden nicht alles radikal beseitigt. Die Einstellungen für searX(NG)-Metasuchmaschinen werden z. B. in Cookies gespeichert. Eventuell möchte man dauerhaft auf einigen Webseiten eingeloggt bleiben o. Ä., dann darf man die SiteSettings beim Beenden des Browsers nicht löschen:

```
privacy.clearOnShutdown.siteSettings  = false
```

In den Firefox-Einstellungen kann man im Abschnitt *Datenschutz und Sicherheit* Ausnahmen für Websites definieren, deren Cookies nicht beim Beenden gelöscht werden sollen.

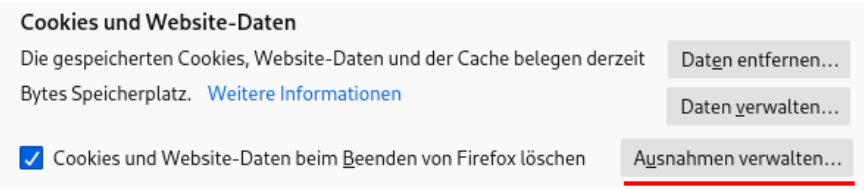


Abbildung 4.6: Webseiten definieren, die dauerhaft Cookies speichern dürfen

3: Schutz gegen Redirect-Tracking

Beim Redirect-Tracking wird der Surfer bei Klick auf einen Link nicht direkt von der Webseite A zur Webseite B geleitet (A → B), sondern von der Webseite A zur Zwischenstation T, die den Besucher mit Tracking-Elementen im First-Party-Context markiert und dann automatisch zur gewünschten Webseite B weiterleitet (A → T → B). Der Redirect wird vom Surfer in der Regel kaum bemerkt.

Das Add-on **Skip Redirect** kann diese Tracking-Umleitungen in URLs entfernen, wenn sie nicht kodiert wurden. (Für Wi-Fi-Hotspot-Logins muss man das Add-on deaktivieren.)

Firefox 79+ kann Redirect-Tracking erkennen und die Tracking-Markierungen entfernen. Das Feature ist seit Firefox 83+ standardmäßig aktiviert. Alle 24 Stunden einmal löscht Firefox alle Cookies und Evercookies von Domains, die in der Blockierliste für den Trackingschutz gelistet sind (aber nur, wenn die Domain in den letzten 72 Stunden nicht als First-Party mit Nutzerinteraktion aufgerufen wurde). Das Feature ist überflüssig, wenn man beim Beenden von Firefox alle Daten löscht, wie oben empfohlen.

Cookie-Management mit zusätzlichen Add-ons

Zusätzliche Add-ons wie CookieAutoDelete oder CookieController tun in der Regel das, was der Name vermuten lässt. Sie löschen oder verwalten Cookies, die nicht mehr gebraucht werden, automatisch oder nach vorgegeben Regeln (und machen um jedes gelöschte Cookie viel Getöse).

Das einfache Löschen von Cookies schützt nur wenig gegen Tracking. Trackingdienste verwenden EverCookies, um gelöschte Trackingcookies wiederherzustellen. Diese Add-ons erfüllen ihre Aufgabe, bieten aber hinsichtlich Trackingschutz kaum Verbesserungen.

4.5 Surf-Container

Surf-Container sind ein Konzept von TorProject.org und Mozilla, um Website-übergreifendes Tracking mit Cookies und EverCookie-Techniken zu verhindern.

- Ein Surf-Container enthält alle Daten, die von Webseiten gespeichert wurden, in einer abgeschotteten Umgebung (Cookies, HTML5-Storage, IndexedDB, Cache, TLS-Sessions, Shared Workers, HTTP Authentication usw.). Diese Daten bilden dann den sogenannten *Context* für das Surfen in diesem abgeschotteten Container.
- Der Zugriff auf Daten in einem anderen *Context* bzw. einem anderen Surf-Container ist nicht möglich. Somit werden in den verschiedenen Contexts unterschiedliche Tracking-Markierungen gesetzt. Man kann sich auch in verschiedenen Surf-Containern (userContext) gleichzeitig mit unterschiedlichen Identitäten bei einer Website anmelden.

Aber: Surf-Container schützen nicht gegen Tracking anhand des Browser-Fingerprint! Da das gleiche Browserprofil mit identischer Konfiguration und identischen Add-ons genutzt wird und außerdem die IP-Adresse identisch ist, können viele Trackingdienste eine Verknüpfung des Surfverhaltens in unterschiedlichen Containern herstellen!

Konzepte für Surf-Container in Firefox

Mozilla hat mehrere Konzepte für Surf-Container in Firefox implementiert:

1. **FirstParty.Isolate** wurde für den TorBrowser unter dem Titel *Cross-Origin Identifier Unlinkability* entwickelt und mit Firefox 58+ von Mozilla übernommen. In aktuellen Firefox-Versionen sollte man es aber nicht mehr verwenden.

   ```
   privacy.firstparty.isolate = false
   ```

2. Basierend auf den Erfahrungen mit *FirstParty.Isolate* hat Mozilla das Konzept überarbeitet und mit Firefox 85 komplett neu implementiert. Dabei wurde der Schutz in zwei getrennte Komponenten aufgeteilt und IPv6-tauglich gemacht:

   - **Netzwerk-Partitionierung** isoliert alle Cache Speicher (HTTP, Bilder, Fonts), SSL-Sessions, HSTS, OCSP, DNS usw. in getrennten Containern für jede First-Party-Domain. Damit wird verhindert, das Trackingdienste diese Techniken, die nicht zur Speicherung von Daten vorgesehen sind, für die Markierung mit EverCookies missbrauchen können.

     Die *Netzwerk-Partitionierung* ist standardmäßig aktiv:

```
privacy.partition.network_state = true
```

- **Total Cookie Protection** ist das Konzept zur Isolation von Cookies, Third-Party Cookies, DOMStorage und IndexDB in getrennten Containern für jede First-Party-Domain. Für unterschiedliche Websites ergeben sich damit unterschiedliche Tracking-IDs in Cookies, HTML5-Storage usw. und ein Tracking über mehrere Webseiten ist mit Cookies nicht möglich.
  Die *Total Cookie Protection* ist in Firefox ebenfalls standardmäßig aktiviert:

```
network.cookie.cookieBehavior = 5
```

HINWEIS: Wenn man *FirstParty.Isolate* aktiviert, dann wird der alte Code verwendet und nicht *Netzwerk-Partitionierung* bzw. *Total Cookie Protection*. Es ist empfehlenswert, *FirstParty.Isolate* zu deaktivieren und stattdessen *Total Cookie Protection* zu nutzen.

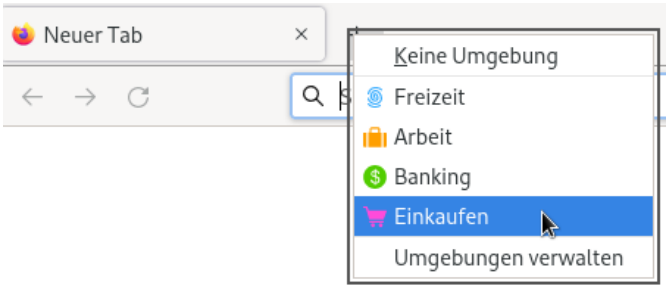
3. **userContext** steht seit Firefox 50+ zur Verfügung. Es werden mehrere Surf-Container bereitgestellt, die man selbst aktiv auswählen muss. Um das Feature zu aktivieren, muss man zuerst unter der Adresse *about:config* folgende Werte setzen:

```
privacy.userContext.enabled     = true
privacy.userContext.ui.enabled  = true
```

Die Freigaben für den Zugriff auf Mikrofon, Kamera, Geolocation oder Webnotification können ebenfalls im userContext gekapselt werden und gelten dann nur, wenn die Webseite in einem spezifischen Context aufgerufen wird. Dafür ist folgende Variable unter der Adresse *about:config*zu aktivieren:

```
permissions.isolateBy.userContext = true
```

Man kann einen neuen Tab in einem bestimmten userContext öffnen, indem man mit der rechten Maustaste auf den Plus-Button für neue Tabs klickt oder die linke Maustaste lange gedrückt hält:



Außerdem kann man über den Menüpunkt *Datei → Neuer Tab in Umgebung...* einen Tab in einem anderen Surf-Container öffnen sowie mit Klick der rechten Maustaste auf einen Link wählen, in welchem Surf-Container man den Link/Tab öffnen möchte.

Anhand einer Farbkennung auf dem Reiter ist erkennbar, zu welcher Umgebung er gehört. Man kann auch selbst weitere Surf-Container definieren. Ob dieses Konzept effektiv eingesetzt wird, hängt in erster Linie von der Disziplin des Anwenders ab.

In unterschiedlichen Containern kann man sich gleichzeitig mit unterschiedlichen Accounts bei einem Webdienst anmelden. Das ist eine der Haupteinsatzmöglichkeiten für dieses Feature.

4.6 Werbung, HTML-Wanzen und Social Media

Die auf vielen Websites eingeblendete **Werbung** wird von wenigen Servern bereitgestellt. Diese nutzen häufig (eigentlich immer) die damit gegebenen Möglichkeiten, das Surfverhalten über viele Websites hinweg zu erfassen. Dabei können direkt oder indirekt sehr private Informationen über den Surfer ermittelt werden.

- Der Blutspendendienst des Bayrischen Roten Kreuzes stellt auf seiner Webseite einen Vorcheck bereit. Durch ein eingebundenes Trackingscript von Facebook wurden die Antworten auf sensible Fragen zu Schwangerschaft, Drogenkonsum, Diabetes oder HIV an Facebook gesendet, wie eine Analyse der Süddeutschen Zeitung ergab.[21]
- Eine Studie von Privacy International hat 136 Webseiten mit Gesundheitsinformationen untersucht. Dabei wurde klar, dass fast alle Webseiten mit Trackern verseucht waren und dass die Werbenetzwerke allein durch das Aufrufen einer Seite mit bestimmten Informationen zu Krankheiten interessante Einsichten darüber gewinnen, ob man sich beispielsweise für Krankheitssymptome oder Heilung von Depressionen interessiert. Diese Informationen können in die Profilbildung einfließen und zu Schlussfolgerungen führen, die uns nicht gefallen werden. Bei zwei Websites wurden auch Antworten auf sensible gesundheitliche Fragen zur Ferndiagnose an die Werbenetzwerke übertragen.[22]

Als **Malvertising** (abgeleitet von *malicious advertising*) bezeichnet man Schadsoftware, die Werbenetzwerke ausgeliefert wird. Kriminelle kaufen zur Zielgruppe passende Werbeplätze bei Werbenetzwerken wie Google Ads und lassen Werbebanner mit bösartigem Javascript ausliefern oder locken die Surfer mit Anzeigen auf Malware Webseiten. Einige Beispiele aus den letzten Jahren

- Im Januar 2013 lieferten die Server des Werbenetzwerks OpenX bösartige Scripte aus, die den Rechner über Sicherheitslücken im Java-Plug-in und im Internet Explorer kompromittierten.[23]
- Zum Jahreswechsel 2014 wurden innerhalb von 4 Tagen 27.000 Surfer durch Werbung von Yahoo mit Malware infiziert.[24]
- Eine mehrwöchige erfolgreiche Malvertising-Kampagne konnte im August 2015 mit Hilfe von Doubleclick einige Millionen Surfer infizieren.[25]
- Im November 2015 wurden die Server des Werbenetzwerkes Pagefair gehackt, um bösartigen JavaScript-Code in der Werbung auszuliefern.[26]
- Im Dezember 2022 warnte das FBI vor Werbung, die in die Ergebnisse von Suchmaschinen eingebettet wird. Kriminelle nutzen diese Werbung, um Surfer auf Phishing-Webseiten zu locken oder auf Webseiten, die Malware verbreiten. Diese Werbeanzeigen sind oft nur durch eine kleine, unauffällig Markierung als Werbung gekennzeichnet und nicht auf den ersten Blick von realen Suchergebnissen zu unterscheiden. Das FBI empfiehlt den Einsatz von Werbeblockern.[27]

[21] https://www.sueddeutsche.de/dgital/blutspende-brk-facebook-patientendaten-1.4576563
[22] https://heise.de/-4513282
[23] http://heise.de/-1787511
[24] http://www.zdnet.de/88180242/werbung-auf-yahoo-com-verteilte-malware-an-nutzer-in-europa/
[25] https://blog.malwarebytes.org/malvertising-2/2015/09/large-malvertising-campaign-goes-almost-undetected/
[26] http://www.golem.de/news/anti-adblocker-dienst-500-websites-ueber-pagefair-gehackt-1511-117262.html
[27] https://www.ic3.gov/Media/Y2022/PSA221221

Als **Advertising Intelligence** (AdInt) bezeichnet man die Kooperation von Werbefirmen mit den Geheimdiensten. Die Werbeindustrie hat ein Trackingsystem aufgebaut, mit dem einzelne Personen auch bei Benutzung von mehreren Geräten detailliert verfolgt werden können (nicht alle Internetnutzer aber viele). Die Geheimdienste nutzen dieses Trackingsystem, indem sie eine Werbefirma aufbauen, die Werbung als Wanzen auspielt und dafür Werbeplätze bei Google oder anderen Plattformen per *Real Time Bidding* kauft, die sehr spezifisch auf die Zielpersonen zugeschnitten sind.

1. Passiv: Die Bewegungsdaten von Personen werden mittels Werbung überwacht und mögliche Kontaktpersonen durch Auswertung der mittels Werbetracking gesammleten Daten identfiziert. Die israelische Firma ISA Security verfolgt auf diese Weise mit dem Werkzeuk Patternz bis zu 5 Milliarden Gerate weltweite und stellt die Daten den Geheimdiensten zur Verfügung.[28]

2. Aktiv: Die Werbung wird als Transportmedium genutzt, um die Geräte einer Person mit Trojanern zu infizieren. Die isrealische Firma Insanet hat 2019 den Trojaner Sherlock vorgestellt, der mittels Werbung auf Smartphones und Windows PCs installiert werden kann. Auch die NSO Group hat einen solchen Trojaner im Portfolio (aber bisher keine Exportgenehmigung).

   Das bei der Verteilung von Trojanern möglicherweise auch unbeabsichtigt Dritte infiziert werden, nimmt man in Kauf. Die Trojaner-Werbung wird einfach verteilt, bis sie trifft.

Bei **HTML-Wanzen** (sogenannten Webbugs) handelt es sich um 1x1-Pixel-große transparente Bildchen, welche in den HTML-Code einer Webseite oder einer E-Mail eingebettet werden. Sie sind für den Nutzer unsichtbar und werden beim Betrachten einer Webseite oder beim Öffnen der E-Mail von einem externen Server geladen und ermöglichen es dem Betreiber des Servers, das Surfverhalten Website-übergreifend zu verfolgen.

Die **Like Buttons** werden von Facebook und anderen sozialen Netzen verwendet, um Daten zu sammeln. Mit dem Aufruf einer Webseite mit Facebook-Like-Button werden Daten an Facebook übertragen und dort ausgewertet, auch wenn der Surfer selbst kein Mitglied bei Facebook ist. Die Verwendung der Like-Buttons ist nach Ansicht von Thilo Weichert (ULD) nicht mit dem deutschen Datenschutzrecht vereinbar. Deutsche Webseitenbetreiber sind aufgefordert, die Facebook-Buttons von ihren Seiten zu entfernen.[29]

Forscher der Universität Cambridge (Großbritannien) konnten im Rahmen einer Untersuchung durch Auswertung der Klicks auf Facebook-Like-Buttons die sexuelle Orientierung und politische Einstellung der Teilnehmer vorhersagen.[30] Man verrät mit einem Klick auf einen Like-Button möglicherweise Informationen, die man nicht im Netz veröffentlichen möchte.

4.6.1 Tracking Protection in Firefox

Firefox enthält einen eingebauten Trackingschutz, den man in den Einstellungen in der Sektion *Datenschutz und Sicherheit* aktiviert. Es wird eine Blockliste von Disconnect genutzt, die von einem Mozilla-Server heruntergeladen wird. Diese Blockliste ist nicht dafür ausgelegt, möglichst viel Werbung auf allen Webseiten zu blockieren. Sie blockiert Trackingdienste und damit als Nebeneffekt Werbebanner, die für Tracking genutzt werden. Folgende Schutzlevel stehen dabei zur Auswahl:

[28] https://www.heise.de/news/Gezielte-Werbung-Israelischer-Verein-wirbt-mit-5-Milliarden-ueberwachten-Geraeten-9609259.htm1
[29] https://www.datenschutzzentrum.de/facebook/
[30] http://heise.de/-1820638

Standard: In Firefox ist der Schutz gegen Tracking (*Schutz gegen Aktivitätenverfolgung*) standardmäßig nur in privaten Fenstern aktiv. Der Schutz gegen Trackingcookies und Krypto-Miner ist immer aktiv.

Streng: Im strengen Modus sollen Scripte zum Tracking in allen Fenstern blockiert werden, außerdem Trackingcookies, Krypto-Miner sowie Scripte zum Fingerprinting des Browsers.

Benutzerdefiniert: Dazu gibt es die benutzerdefinierte Konfiguration, in der man selbst entscheiden kann, welche Schutzmechanismen aktiviert werden sollen. Der *Schutz gegen Aktivitätenverfolgung* kann generell aktiviert werden, nur im Private Browsing Mode oder gar nicht.

Der Trackingschutz ist nur bedingt brauchbar, wie ein oberflächlicher Test zeigt. Für den kleinen Test wurde die strenge Tracking Protection von Firefox 69.0 aktiviert, dann wurden ein paar Webseiten aufgerufen. Dabei wurde vor allem beobachtet, welche Third-Party-Cookies jetzt als Trackingcookies erkannt und blockiert wurden.

- Auf den Webseiten *Heise.de* und *Zeit.de* ist die Werbung verschwunden, aber die Trackingcookies von WebTrekk werden nicht blockiert. Das ist evtl. nicht verwunderlich, da sich WebTrekk mit DNS-Aliases auf beiden Webseiten einen First-Party-Status erschleicht und der in Firefox 69.0 implementierte Schutz gegen Trackingcookies nur Third-Party-Cookies analysiert und in gute und böse Cookies einteilt.

  Trackingscripte von Google und OpenX werden auf Heise.de und Zeit.de blockiert, aber man wird auf beiden Webseiten mit Third-Party Cookies von EASYmedia beobachtet, die nicht von der Tracking Protection blockiert werden. In der Datenschutzpolicy von EASYmedia findet man folgenden Satz zum Austausch von Daten:

  > *- EASYmedia ist mit einer großen Anzahl von Partnern wie z. B. Google, OpenX, SmartAds und vielen anderen verbunden. Um die Bereitstellung unseres Dienstes im Cookie-basierten Advertising-Ökosystem zu ermöglichen, tauscht EASYmedia automatisiert pseudonyme IDs mit solchen Partnern aus [. . .]*
  > *- EASYmedia kann auch Informationen von Dritten erhalten, um gezielte und maßgeschneiderte Werbung auf Webseiten und mobilen Anwendungen zu ermöglichen.*

  (Es gibt Tracking-Familien, die die Daten untereinander austauschen und damit eine große Reichweite bei der Beobachtung des Surfverhaltens erreichen . . . und das Google-Imperium ist die größte Familie.)

- Auf *YouTube.com* wird man trotz strengem Trackingschutz mit einem Cookie von DoubleClick.net markiert, das zur Auswahl von individuell optimierter Werbung verwendet wird, siehe IDE Cookie bei Googles Cookie-Arten:

  > *Wir verwenden Cookies auch für Werbung, die wir an verschiedenen Stellen im Web zeigen. Unser wichtigstes Cookie für Anzeigenvorgaben für Websites, die nicht zu Google gehören, heißt IDE. Es wird in Browsern unter der Domain doubleclick.net gespeichert. [. . .] Andere Google-Produkte wie YouTube nutzen dieses Cookie möglicherweise ebenfalls zur Auswahl relevanter Werbung.*

  (Also wenn das kein bekanntes Trackingcookie ist . . .)

Es ist nicht ungewöhnlich, dass der eingebaute Trackingschutz der Browser großzügige Ausnahmen für Geldgeber vorsieht. Was Google für Firefox ist, ist Microsoft für den DuckDuckGo Private Browser. Die Suchmaschine DuckDuckGo finanziert sich hauptsächlich durch Werbung von Microsoft und der DuckDuckGo Private Browser macht beim Trackingschutz eine freundliche Ausnahme für Microsofts Cookies.[31]

- Auf *Bild.de* werden viele Trackingscripte blockiert, die Webseite ist offensichtlich mit unterschiedlichsten Trackern überflutet. Allerdings ist der Schutz auch hier nicht umfassend. Es wurden keine Trackingcookies von der neuen Firefox Tracking Protection gefunden und blockiert, aber einige der akzeptierten Third-Party-Cookies von WebTrekk, Dynamic Yield, TealiumIQ, Adserve.io usw. könnte man wie bei uBlock Origin eindeutig als Tracking einsortieren.

Dies sind nur Beispiele und keine wissenschaftliche Analyse. Sie zeigen aber, dass der Trackingschutz von Firefox oft nur oberflächlich arbeitet und dass andere Lösungen mit optimierten Filterlisten für deutsche Surfer bessere Ergebnisse erreichen und auch mehr Features bieten.

Bei Aktivierung der Tracking Protection werden aber nicht nur die Filter aktiviert, sondern auch Do-Not-Track (DNT). Mit jedem HTTP-Request wird ein DNT-Header gesendet, der allen Webservern den Wunsch des Nutzers anzeigen soll, dass man nicht beschnüffelt werden möchte. Do-Not-Track ist politisch gescheitert, es wird von Trackingdiensten ignoriert. Die Aktivierung des DNT-Headers schafft aber ein Differenzierungsmerkmal für das Browser-Fingerprinting, wie auch die DNT Working Group des W3C in ihrer Spezifikation anmerkt. Deshalb ist es empfehlenswert, die Firefox Tracking Protection abzuschalten und stattdessen einen anderen AdBlocker zu verwenden:

```
privacy.trackingprotection.enabled = false
```

Das gleiche gilt für den Private Browsing Mode (PBM). Im PBM wird die Tracking Protection standardmäßig aktiviert und es wird damit ein DNT-Header gesendet, womit das Fingerprinting des Browsers erleichtert wird. Mit folgender Option deaktiviert man die Tracking Protection im Private Browsing Mode:

```
privacy.trackingprotection.pbmode.enabled = false
```

4.6.2 uBlock Origin für Firefox

uBlock Origin[32] ist ein effizienter und funktionsreicher Werbeblocker für Firefox.

Nach der Installation findet man oben rechts in der Toolbar des Browsers das uBlock-Symbol. Mit einem Klick auf das Symbol kann man die Filterung für die aktuelle Webseite anpassen oder ganz deaktivieren. Mit einem Klick auf das kleine Symbol für *Einstellungen* rechts unten kann man die Konfiguration anpassen.

Um die Konfiguration zu vereinfachen, stehen auf der Webseite zwei Konfigurationen für uBlock Origin als Vorschlag vom PrHdb-Team zum Download bereit, den man auf dem Reiter *Einstellungen* importieren kann.[33]

Auf dem Reiter *Filterlisten* kann man weitere Filterlisten aktivieren, z. B. EasyList Germany oder die Belästigungen aus (un)sozialen Medien blockieren. Aus Sicherheitsgründen sollte man keine Listen abonnieren, die über eine HTTP-Verbindung aktualisiert werden.

[31] https://www.bleepingcomputer.com/news/security/duckduckgo-browser-allows-microsoft-trackers-due-to-

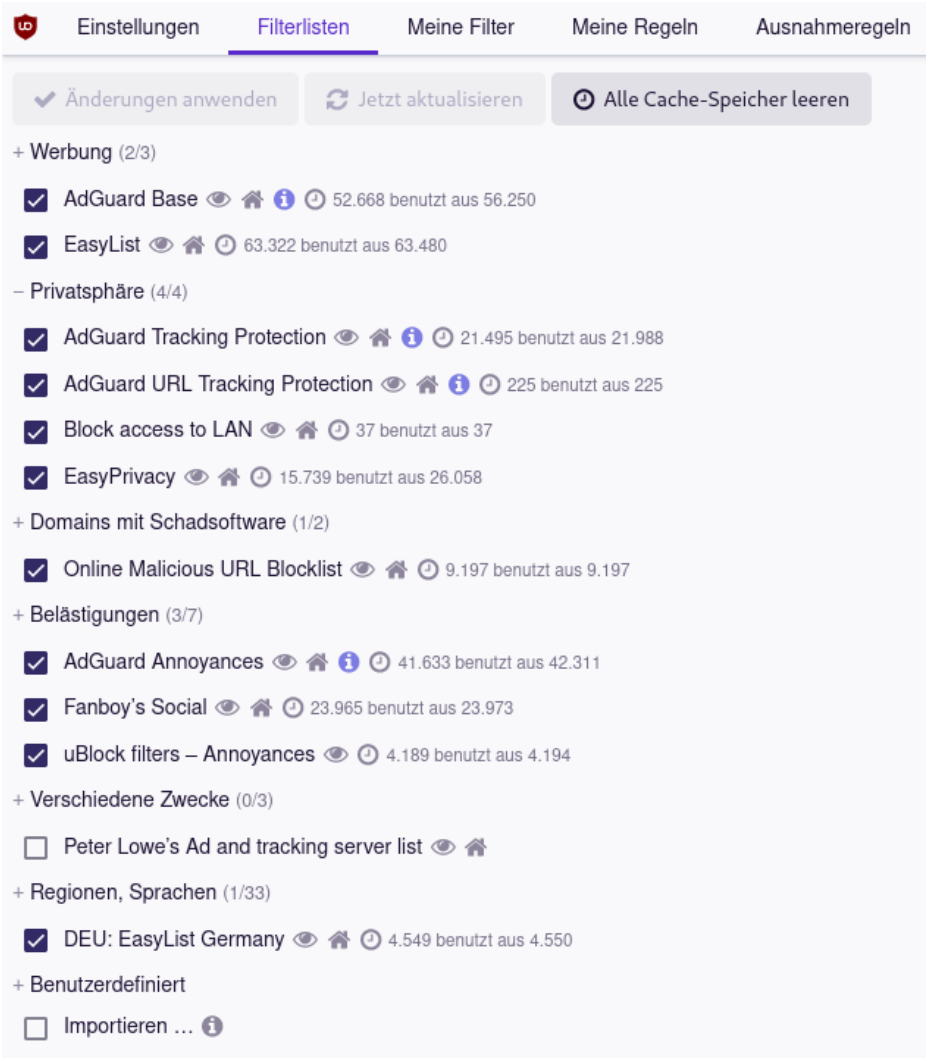


Abbildung 4.7: uBlock Origin: zusätzliche Filterlisten aktivieren

Laden externer Schriftarten mit uBlock blockieren?

Das Blockieren von externen Schriftarten mit uBlock Origin empfehlen wir nicht. Einerseits werden die Zugriffe auf CSS-Server wie *fonts.googleapis.com* damit nicht blockiert, da die Stylesheets trotzdem geholt werden. Außerdem werden damit auch die via Fonts dargestellten Navigationssymbole blockiert, sodass viele Webseiten unbenutzbar werden.

Stattdessen wird der Google-CSS-Font-Server *fonts.googleapis.com* mit einem eigenen uBlock Filter blockiert:

```
||fonts.googleapi.com$important,third-party
```

Um Schutz gegen Tracking via Schriftarten zu gewährleisten, ist folgende Einstellungen unter *about:config* besser geeignet:

search-agreement/

[32] https://addons.mozilla.org/de/firefox/addon/ublock-origin

[33] https://www.privacy-handbuch.de/handbuch_21d2.htm

```
browser.display.use_document_fonts  = 0
layout.css.font-loading-api.enabled = false
gfx.downloadable_fonts.enabled      = false
```

Nervende Cookiebanner entfernen

Viele Webseiten nerven mit der Bitte um Zustimmung, Cookies für das Tracking setzen zu dürfen. uBlock Origin bietet die Möglichkeit, diese nervenden Banner abzuschalten und automatisch ein Tracking-freies Surferlebnis zu fordern. Oft wird dabei von uBlock Origin im Hintergrund automatisch ein Cookie gesetzt, welches der Webseite vorgaukelt, der Nutzer hätte dem Tracking widersprochen.

Um Cookiebanner zu unterdrücken, muss man nur die passenden Filterlisten aktivieren, die man im Abschnitt *Cookie Hinweise* findet. Die *uBlock Cookie Notices* braucht man nur einmal.

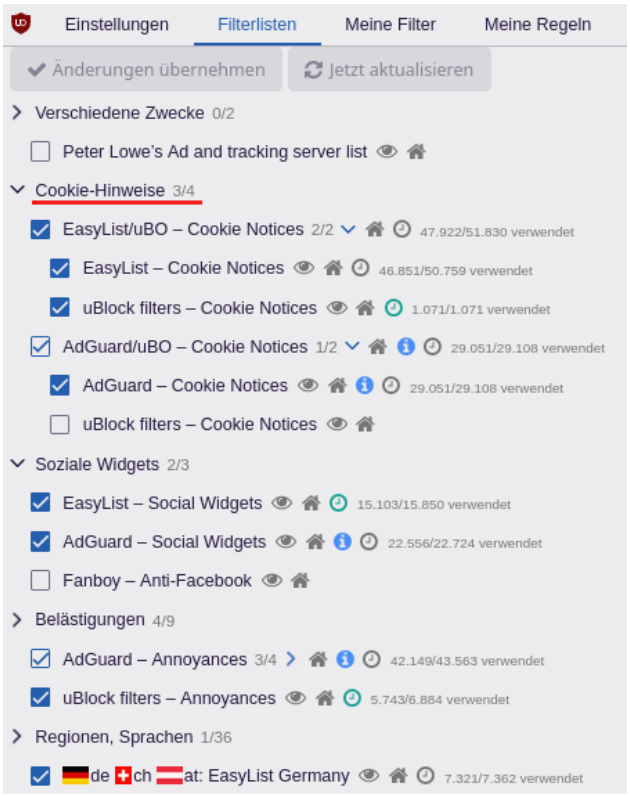


Abbildung 4.8: uBlock Origin: Cookiebanner entfernen

In Firefox 120 wurde eine ähnliche Funktion testweise für deutsche Nutzer implementiert, die aber noch weit davon entfernt ist, vergleichbare Ergebnisse wie die uBlock Filter zu erreichen. Man könnte diese Funktion unter *about:config* mit folgendem Parameter aktivieren:

1. Bei bekannten Cookiebannern das Tracking automatisiert ablehnen:

   ```
   cookiebanners.service.mode = 1
   ```

2. Bei bekannten Cookiebannern das Tracking ablehnen und sonst alles akzeptieren:

   ```
   cookiebanners.service.mode = 2
   ```

Weitere Einstellungen für zusätzliche Aufgaben

uBlock Origin blockiert nicht nur Trackingscripte und Werbebanner, sondern enthält auch die Filter für den Schutz gegen Zugriffe auf lokale URLs und entfernt bekannte Tracking-Parameter aus URLs. Außerdem können iFrames blockiert oder als click2load dargestellt werden.

4.7 iFrames

Einige Trackingdienste verwenden iFrames, um HTML-Wanzen zu laden, wenn JavaScript blockiert ist und keine Trackingscripte ausgeführt werden können. Auf vielen Webseiten findet man den Code von GoogleTagManager (*Google Universal Analytics tracking code*):

```
<noscript>
   <iframe src="//www.googletagmanager.com/ns.html?id=blabala..."
   ↪  height="0" width="0" style="display:none;visibility:hidden"></iframe>
</noscript>
```

Die Tracking-Technik des *DoubleClick Bid Manager* wurde von Invite Media entwickelt und in DoubleClick integriert, nachdem Google die Firma aufgekauft hatte. Auch dieses Tracking nutzt einen unsichtbaren iFrame, um Trackingwanzen mit oder ohne JavaScript zu platzieren:

```
<script type="text/javascript">
...
 <document.write('
    <iframe src="http://nnnn.fls.doubleclick.net/activityi;src=xxxx;...."
    ↪     width="1" height="1" frameborder="0"
    ↪  style="display:none"></iframe>');
</script>
<noscript>
    <iframe src=""http://nnnn.fls.doubleclick.net/activityi;src=xxxxx;"
    ↪  width="1" height="1" frameborder="0" style="display:none">
    </iframe>
</noscript>
```

Integrierte Videos mit JavaScript-Player

Viele Webseiten integrieren Videos von Videoplattformen. Die Integration erfolgt in der Regel als iFrame. Für YouTube-Videos sieht der HTML-Code so aus:

```
<iframe src="https://www.youtube.com/embed/xyz...
```

Mit dem Aufruf der Webseite, welche das eingebettete Video enthält, wird auch der iFrame von YouTube geladen und der Surfer mit einem Cookie von YouTube markiert. Um mit europäischem Datenschutzrecht konform zu sein, bietet YouTube eine Adresse für die Einbettung von Videos in Webseiten an, die auf das Setzen von Tracking-Cookies verzichtet:

```
<iframe src="https://www.youtube-nocookie.com/embed/xyz...
```

Leider wählen nicht alle Webseitenbetreiber die datenschutzfreundlichere YouTube-Variante. Man kann das Add-on *Privacy Enhanced Mode for Embedded YouTube*[34] installieren. Es schreibt die Adressen für embedded YouTube-Videos auf die No-Cookie-Adresse um.

iFrames allgemein blockieren

Mit dem Add-on uBlock Origin kann man alle iFrames von Drittseiten blockieren, indem man auf dem Reiter *Meine Regeln* eine Filterregel einfügt (Abb. 4.9).

```
* * 3p-frame block
```

Die Regel kann auf der rechten Seite zum temporären Ausprobieren editiert werden und wird dann mit dem Button *Dauerhaft speichern* zur linken Seite übernommen.

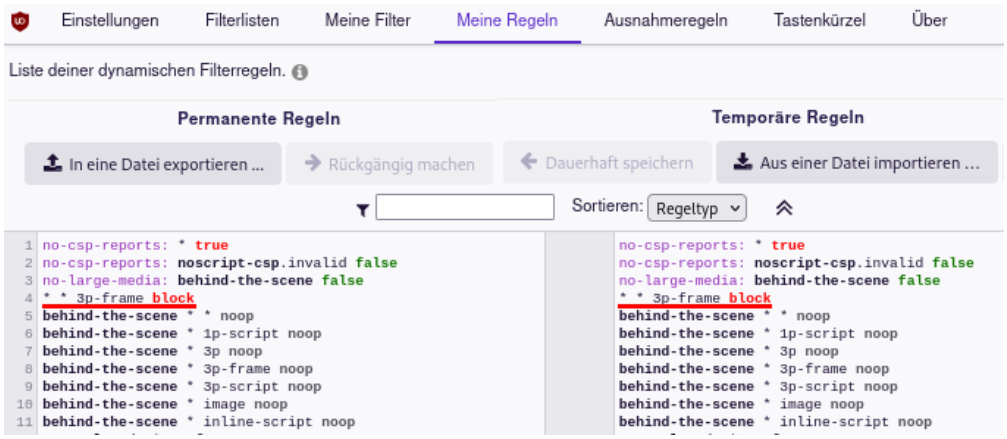


Abbildung 4.9: Blockieren der iFrames von Drittseiten mit uBlock Origin

Einige News-Webseiten wie z. B. *www.Golem.de* oder *www.Zeit.de* sind nicht mehr kostenfrei lesbar, wenn man alle iFrames blockiert, weil sie die Zustimmungsseite für Cookies mit iFrames von einer Subdomain von privacy-mgmt.com (Bauer Media Group) realisieren. Kurioserweise funktioniert es wieder, wenn man *privacy-mgmt.com* unter *Meine Filter* mit einer Regel blockiert.

```
||privacy-mgmt.com$important
```

iFrames auf einzelnen Webseiten freigeben

Manchmal kann es nötig sein, iFrames auf einzelnen Webseiten freizugeben. Das kann man in uBlock Origin mit zwei Klicks erledigen, indem man nach dem Aufruf der Webseite im Menü von uBlock Origin auf das grau markierte Feld in der Zeile *3rd-party frames* klickt (Abb. 4.10). Nach der Freigabe von iFrames ist die Webseite neu zu laden. Die Freigabe kann dauerhaft gespeichert werden oder temporär bis zum Neustart des Browsers gelten.

[34] https://addons.mozilla.org/de/firefox/addon/youtube-nocookie/

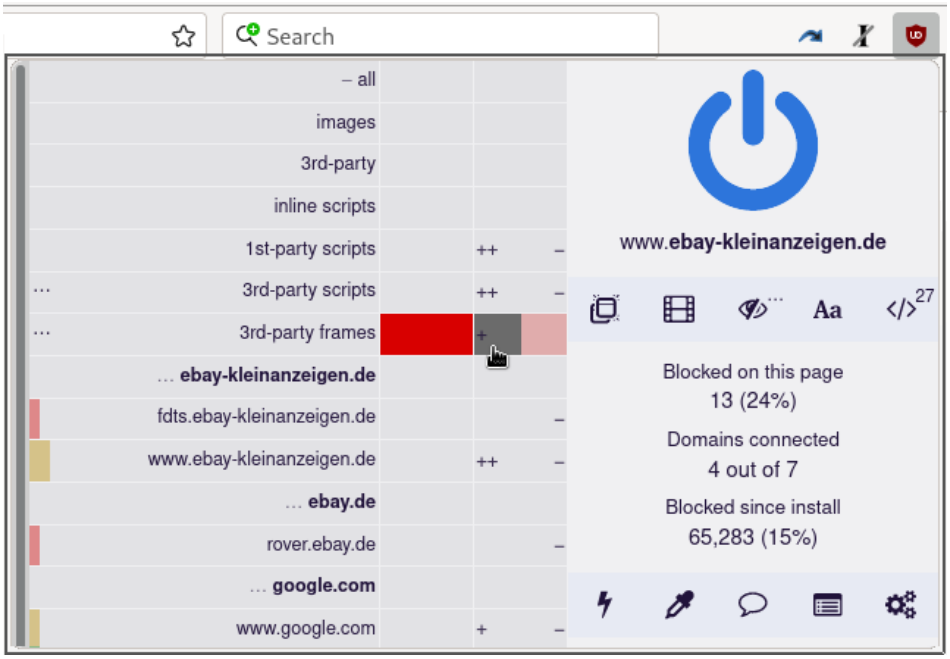


Abbildung 4.10: iFrames auf einzelnen Webseiten in uBlock Origin freigeben

Integrierte Videos mit Click-2-Play laden

Wenn mit der o. g. Regel alle iFrames blockiert werden, verschwinden auch eingebettete Videos von den Webseiten. Um die Videos mit Click-2-Load zu laden, kann man folgende Regeln unter *Meine Filter* einfügen:

```
||youtube-nocookie.com/embed/$3p,frame,redirect=click2load.html
||youtube.com/embed/$3p,frame,redirect=click2load.html
||scribd.com/embeds/$3p,frame,redirect=click2load.html
||player.vimeo.com/video/$3p,frame,redirect=click2load.html
||dailymotion.com/embed/$3p,frame,redirect=click2load.html
||player.glomex.com/integration/$3p,frame,redirect=click2load.html
||players.brightcove.net/$3p,frame,redirect=click2load.html
||cdn.podigee.com/podcast-player/$3p,frame,redirect=click2load.html
||odysee.com/$3p,frame,redirect=click2load.html
||rumble.com/embed/$3p,frame,redirect=click2load.html
||lbry.tv/$3p,frame,redirect=click2load.html
||widget.spreaker.com/$3p,frame,redirect=click2load.html
||media.theplattform.net/videos/embed/$3p,frame,redirect=click2load.html
||vk.com/video_ext.php$3p,frame,redirect=click2load.html
||podbean.com/$3p,frame,redirect=click2load.html
```

Diese Filterliste kann man als *benutzerdefinierte Liste* von folgender Adresse importieren:
https://www.privacy-handbuch.de/download/prhdb-video-embed-click-2-play-list.txt

Die Video-iFrames von diesen Domains werden beim Laden der Seite so dargestellt und können mit einem Klick geladen und gestartet werden:

Googles reCAPTCHA und hCaptcha von Cloudflare

Einige Webseiten verwenden Googles reCAPTCHA oder hCaptcha als Schutz gegen Robots. Die Captchas werden als iFrame geladen und man kann die gewünschte Webseite nicht laden oder sich nicht anmelden, wenn iFrames blockiert werden. Für dieses Problem gibt es zwei Lösungen:

1. iFrames für Captchas können generell freigegeben werden. Dafür trägt man auf dem Reiter *Meine Regeln* folgende Ausnahmen ein, die das Laden von Captchas erlauben:

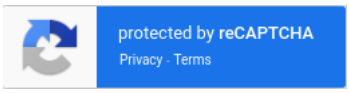
   ```
   * https://www.google.com/recaptcha/ script noop
   * https://www.google.com/recaptcha/api2/ sub_frame noop
   * https://www.gstatic.com/recaptcha/api2/ script noop
   * https://hcaptcha.com * noop
   * https://recaptcha.net script noop
   * https://recaptcha.net sub_frame noop
   ```

   Diese Variante ist in der uBlock-Konfiguration des PrHdB-Teams aktiviert, weil sie problemlos funktioniert. Sie hat den Nachteil, dass die Captchas immer (also auch wenn man sie nicht lösen müsste) geladen und zum Tracking verwendet werden.

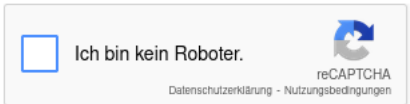
2. Alternativ können die Captchas blockiert, aber mit Click-2-Load-Filterregeln sichtbar gemacht werden. Dafür fügt man auf dem Reiter *Meine Filter* folgende Zeilen ein:

   ```
   ||www.google.com/recaptcha/api*/anchor?$3p,frame,important,redirect=cl
   ↪ ick2load.html
   ||www.recaptcha.net/recaptcha/api*/anchor?$3p,frame,important,redirect
   ↪ =click2load.html
   ||newassets.hcaptcha.com/captcha/$3p,frame,important,redirect=click2lo
   ↪ ad.html
   ```

   Mit einem Klick muss man es aktivieren und sieht, welche Variante genutzt wird. Das kleine reCAPTCHA sieht so aus und mit dem Klick ist schon alles erledigt:

   Wenn man bei dem Captcha ein Häkchen setzen muss, um zu beweisen, dass man kein Robot ist, muss man iFrames in uBlock Origin für diese Webseite freigeben, damit es funktioniert (s. o. Abb. 4.10) und die Webseite neu laden.

   Dann kann dann mit einem Klick bestätigen, dass man kein Robot ist. In der Regel muss man noch ein kleines Bilderrätsel lösen, da Google keine Trackingdaten für die Verifikation nutzen kann.

4.8 Browser-Fingerprinting

Tracking mit Cookies wird immer schwieriger, weil die Browserhersteller Schutzmechanismen implemntieren und standardmäßig aktivieren. Die Branche geht dazu über, andere Techniken wie Browser-Fingerprinting zu nutzen, um Surfer über viele Webseiten zu verfolgen.

Ein Vortrag[35] auf dem Chaos Communication Congress 2020 demonstrierte mit FPMON, dass 20% der TOP 10k Webseiten Javascript Fingerprinting einsetzen. Eine andere Studie[36] (PDF) aus dem gleichen Jahr identifizierte Javascript Fingerprinting Scripte auf 25% der TOP 10k Webseiten und auf 30% der TOP 1.000 Webseiten.

4.8.1 Browser-Fingerprinting mit JavaScript

Mit JavaScript ist es möglich, viele Details des Browsers auszulesen und einen individuellen Fingerprint zu berechnen, der auch ohne Cookies das Tracking ermöglicht.

FingerprintJS Inc. bietet eine kommerzielle Bibliothek an, die laut Eigenwerbung 99,5 % der Surfer anhand des JAvascript Browser-Fingerprint wiedererkennen kann (auch wenn man VPNs oder den Privat Browsing Mode verwendet) und die auf 12 % der Top-500-Webseiten im Einsatz sein soll. Die Demo-Webseite[37] der Firma zeigt, dass die Wiedererkennung mit der hier vorgeschlagenen Konfiguration nicht funktioniert.

Beim Browser-Fingerprinting mit JavaScript werden u. a. folgende Daten ausgewertet:

Bildschirm: Informationen über die Größe des Monitors und des Browserfensters werden am häufigsten für das Hardware-Fingerprinting genutzt. Es liegen keine wissenschaftlichen Analysen zur Verbreitung dieser Trackingmethode vor, aber grob geschätzt werden diese Informationen von 30–50 % der Webseiten ausgewertet. Insbesondere auf größeren Portalen wie heise.de, spiegel.de, zeit.de oder google.com findet man fast immer Trackingscripte, die Bildschirmgröße und Größe des Browserfensters für das Fingerprinting des Browsers nutzen.

Canvas-Fingerprinting wurde 2012 in dem Paper *Perfect Pixel*[38] beschrieben und 2016 auf 14.371 Webseiten als Trackingverfahren nachgewiesen. Der Canvastest auf Browserleaks.com[39] demonstriert das Verfahren. Als einfache Demo kann der Test Schlussfolgerungen über den verwendeten Browser und das Betriebssystem ableiten.

Your Fingerprint :

Signature	1CC7FA60
Found in DB	✓ True
General Conclusion	**It is very likely that you are using [Firefox] on [Ubuntu]**

Canvas Font Fingerprinting wurde 2016 in dem OpenWPM-Paper beschrieben. Dabei wird das *CanvasRenderingContext2D* Objekt mit der Methode *measureText* genutzt. Der Text wird nicht in das Canvas-Element geschrieben, sondern es wird nur die Größe ermittelt, die

[35] https://media.ccc.de/v/rc3-113142-the_elephant_in_the_background/
[36] https://arxiv.org/pdf/2008.04480.pdf
[37] https://fingerprint.com/
[38] https://www.privacy-handbuch.de/download/canvas.pdf
[39] https://www.browserleaks.com/canvas

ein Text mit unterschiedlichen Schriftarten benötigen würde, wenn er geschrieben werden würde. Browserleaks.com demonstriert das Verfahren.[40]

Auch dieses Trackingverfahren wird in-the-wild für das Fingerprinting eingesetzt.

Das Add-on *CanvasBlocker* verhindert einen wiedererkennbaren Fingerprint durch Modifikation der via Canvas-API oder DOM-Rect-API ausgelesenen Werte.

WebGL und **SVG-Bilder** werden ähnlich wie HTML5-Canvas-Elemente angezeigt. Der Webserver schickt kein fertiges Bild, sondern Befehle, um die Grafik lokal im Browser zu generieren. Das Ergebnis kann ausgelesen werden und ist ähnlich wie bei Canvas-Elementen von Grafikhardware und -software abhängig. Mit dem Add-on CanvasBlocker können die Ergebnisse leicht modifiziert werden, um Fingerprinting zu verhindern.

AudioContext: Mit der Audio-API kann JavaScript unhörbare Soundschnipsel im Audiobuffer generieren, manipulieren und die Ergebnisse wieder auslesen. Dabei unterscheiden sich die Ergebnisse in Abhängigkeit von der Audiohardware und -software. Die Daten können für das Fingerprinting genutzt werden.[41]

Das Faken der Audio-API mit den Add-ons JS Restrictor oder CanvasBlocker ist unauffälliger und schwerer erkennbar als das Blockieren der API, was wieder ein seltenes Merkmal für den Browser-Fingerprint generieren würde.

Timing-APIs können von Webanwendungen zur Analyse des Ladens von Ressourcen oder des Nutzerverhaltens missbraucht werden (*Timing Attacks on Web Privacy*).[42]

Die Leistungscharakteristiken moderner Grafikkarten sind sehr individuell, sodass sie sich für das Fingerprinting der Hardware eignen. Man kann z. B. komplexe GPU-Operationen ausführen und die Zeit messen, wie beim *DrawnApart*-Angriff.[43]

Dieses Fingerprinting erfordert hoch-genaue Timer in JavaScript und man verhindert es, indem die Timing-APIs mit dem Add-on *JShelter* ungenauer gemacht werden.

Gamepad-API kann Informationen über ein angeschlossenes Gamepad liefern. Da 99 % der Nutzer kein Gamepad verwenden, liefert sie in der Regel keine Informationen. Aber wenn ein Gamepad angeschlossen wurde, ist es ein sehr eindeutiges Merkmal.

Media Device Enumeration liefert Daten über Kamera und Mikrofon, die man für das Hardware-Fingerprinting verwenden kann. Der Surfer muss dabei nicht um Zustimmung für den Zugriff auf Kamera oder Mikrofon gebeten werden.

Firefox verwendet als Device-IDs einen gesalzenen Hash. Der Salt für die Berechnung des Hashes wird beim ersten Start festgelegt und immer erneuert, wenn Cookies und Cache Daten gelöscht werden. Außerdem ist der Salt in Surfcontainern unterschiedlich.

Die meisten oben genannten JavaScript-APIs könnte man deaktivieren, um ein Auslesen von Daten zu verhindern (was auch oft empfohlen wird). Da ein Trackingscript die Deaktivierung der APIs erkennt, schafft man damit wieder neue Merkmale für das Fingerprinting.

Besser ist es, die Ausgaben der Javascript APIs geringfügig zu manipulieren. Die Parameter für die Manipulation können von der Domain abhängen, die im Browser aufgerufen wird, so dass die Fakes innerhalb einer Domain konstant bleiben und sich nur beim Wechsel der Domain ändern. Außerdem sollte nach einem Neustart des Browsers neue Parameter für die

[40] https://www.browserleaks.com/rects
[41] https://audiofingerprint.openwpm.com/
[42] http://sip.cs.princeton.edu/pub/webtiming.pdf
[43] https://arxiv.org/pdf/2201.09956.pdf

Manipulationen berechnet werden. Damit wird eine langfristige Wiedererkennung des Surfers anhand des Fingerprint und eine Wiedererkennung auf mehrere Webseiten erschwert.

Firefox Fingerprinting Protection (Firefox 120+)

Firefox 120+ hat einen eingebauten Schutz gegen Fingerprinting, der den Canvas und Fontmetrics Fingerprint randomisiert, das exakte Auslesen der installierten Schriftarten verhindert usw.

Eine zusätzliche Installation von Add-ons ist nicht nötig, wenn man die Fingerprinting Protection (FPP) man unter about:config mit folgender Einstellung aktiviert:

```
privacy.fingerprintingProtection = true
```

Hinweis: Im Privat Browsing Mode funktioniert die Fingerprinting Protection noch nicht wie erwartet. Der Schutz ist aktiv aber ein Neustart des Browsers führt nicht zu einer Neuinitialisierung der Parameter für die Randomisierung, wenn man Firefox immer im Privat Browsing Mode startet (getestet mit Firefox 124). Der Fingerprint Fake bleibt trotz Neustart stabil.

Die Fingerprinting Protection (FPP) basiert auf den Erfahrungen von TorProject.org bei der Entwicklung von resistFingerprinting (RFP) für den TorBrowser. FPP vermeidet einige Probleme wie den *UserAgentMissmatch* unter Linux und MacOS sowie den *TimeZoneMissmatch*.

(Bei der Nutzung von Anonymisierungsdiensten ist es nötig, die Zeitzone auf UTC zu setzen, um keine Informationen über den realen Aufenthaltsort zu leaken. Ohne Anonymisierungsdienst ist das eher kontraproduktiv.)

Da RFP das dominierende Feature ist, muss es deaktiviert bleiben, wenn man FPP nutzen will:

```
privacy.resistFingerprinting = false
```

Schutz gegen JavaScript-Fingerprinting mit Add-ons (Firefox 115.x ESR)

Es gibt mehrere Add-ons, die JavaScript-APIs faken können. Zwei Vorschläge:

CanvasBlocker schützt gegen Browsersingerprinting und manipuliert Zugriffe auf Canvas-API, SVG-API und Audio-API. Nach der Installation kann man unseren Konfigurationsvorschlag *CanvasBlocker-settings.json* herunterladen und importieren (Abb. 4.11).[44]

Der Konfigurationsvorschlag basiert auf dem Preset *Stealth Settings*. Die Parameter für die Generierung der Fakes werden aber beim Beenden des Browsers gelöscht, so dass der Fingerprint während einer Surfsession für jede Domain individuell konstant bleibt. Nach einem Neustart werden aber neue Parameter und damit ein neuer Fingerprint generiert.

JShelter wird von einem Team aktiv weiterentwickelt, dass sich intensiv mit Browserfingerprinting beschäftig. Das Add-on bietet drei Schutzfunktionen:

1. *JavaScript Shield* übernimmt den Schutz gegen Fingerprinting und sollte gemäß den Empfehlungen der Entwickler im *Recommended Level* genutzt werden.
2. *Der Network Boundary* Shield schützt gegen unbefugten Zugriff auf lokale Adressen.

[44] https://www.privacy-handbuch.de/handbuch_21c5.htm

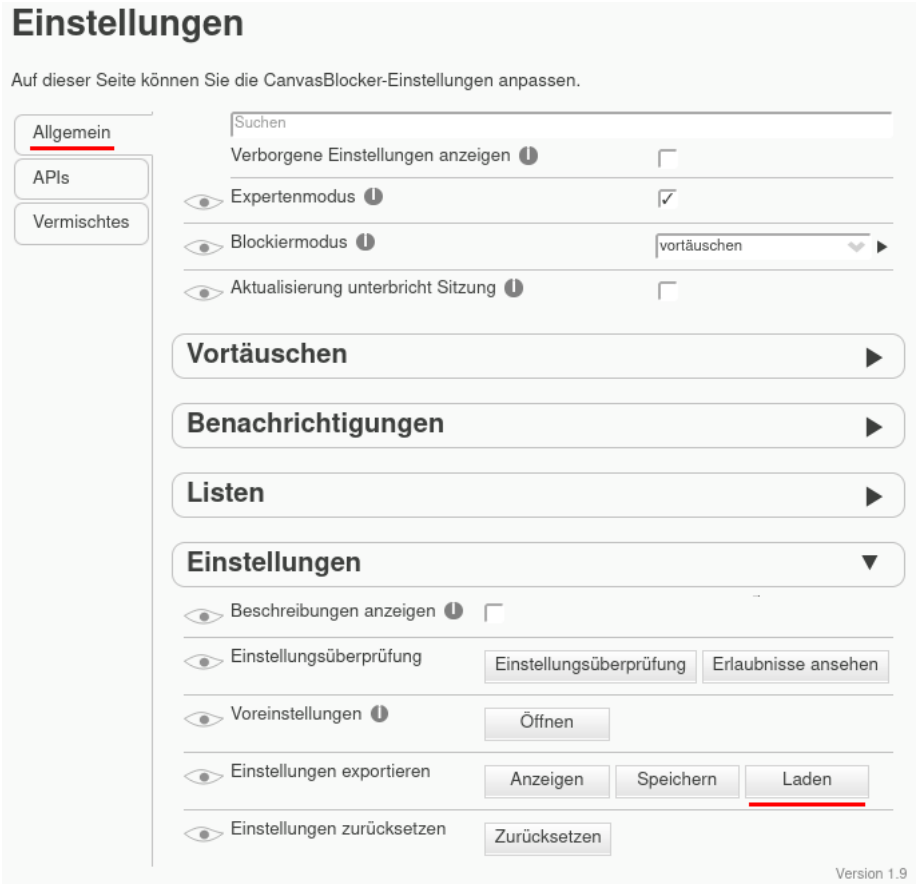


Abbildung 4.11: CanvasBlocker: Konfiguration importieren

3. *Fingerprint Detector* unterbricht die Verbindung zu einer Webseite, wenn vermutet wird, dass die Webseite ein Fingerprinting des Browsers versucht. Diese Funktion macht Webseiten oft unbenutzbar. Daher ist es besser für das Surferlebnis, sie zu deaktivieren.

Für Webseiten zum Onlinebanking (mit Flickercode), JavaScript-lastige Webfrontends der E-Mail-Provider oder für Videokonferenzen kann man im Add-on JShelter den JavaScript Shield deaktivieren und sie funktionieren dann i. d. R. wieder problemlos. Die Auswahl für eine Webseite wird gespeichert und ist beim nächsten Aufruf der Webseite wieder aktiv.

Firefox build-in Schutz resistFingerprinting

Mit *resistFingerprinting* enthält Firefox einen Schutz gegen Fingerprinting, der von TorProject.org entwickelt wurde und Teil des Anonymitätskonzeptes vom TorBrowser ist.

- Es wird das Auslesen der Bildschirmgröße verhindert.
- Das Auslesen von HTML5 Canvas Elementen wird gefakt.
- Angaben zu Ihrer Webcam und Mikrofon werden verschleiert.
- Das Fingerprinting von WebGL Eigenschaften wird verhindert.

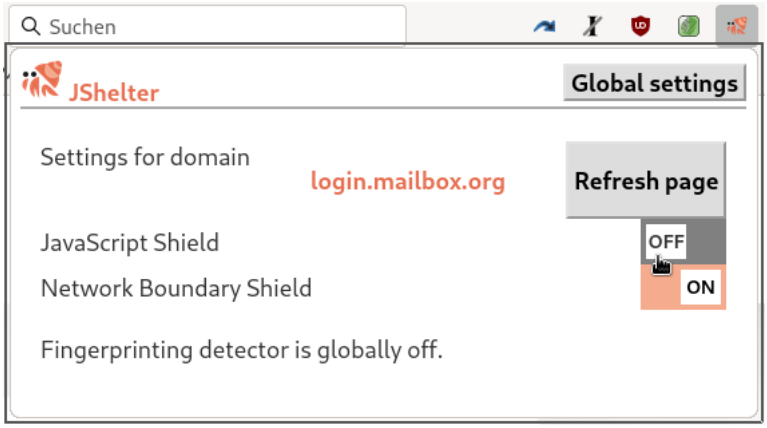


Abbildung 4.12: JShelter für eine bestimmte Webseite deaktivieren

- Die Genauigkeit der Timer wird reduziert.
- Die für eine Webseite auslesbaren Fonts werden reduziert und randomisiert.
- Die bevorzugte Sprache kann auf en-US umgestellt werden (optional).
- Die Zeitzone wird auf UTC gesetzt (was zukünftig abschaltbar sein soll). Die auf Webseiten angezeigten Zeitangaben sind deshalb um 1h oder 2h zeitversetzt.
- Die User-Agent-Kennung wird auf einen Firefox für Windows gesetzt. (Unter Linux oder MacOS ist via Javascript auslesbar, welches OS man nutzt, was kontraproduktiv ist.)

Den Schutz gegen Fingerprinting aktiviert man unter *about:config* mit folgender Einstellung (aufgrund des unplausiblen User-Agent-Fakes aber nur für Windows Nutzer empfehlenswert):

```
privacy.resistFingerprinting = true
```

Nachdem man *resistFingerprinting* aktiviert hat, ist der Browser neu zu starten. Firefox startet dann nicht mehr im Vollbildmodus sondern mit einer Fenstergröße.

Außerdem wird man nach der erstmaligen(!) Aktivierung von *resistFingerprinting* gefragt, ob man sich als englischer Firefox tarnen will oder trotzdem deutsche Webseiten bevorzugt. Im internationalen Maßstab ist es zweifellos besser, sich als englischer Firefox zu tarnen. Bei der überwiegenden (oder ausschließlichen) Nutzung von deutschen Webseiten mit einem deutschen Internetanschluss könnte man aber auch argumentieren, dass in dieser lokalen Gruppe die Browser mit deutscher Lokalisierung überwiegen und man nicht unbedingt auf das Komfortfeature der automatischen Weiterleitung auf die deutsche Version der einer Webseite verzichten muss.

Ob *resistFingerprinting* den Fingerabdruck der Browsers wie gewünscht verschleiern kann, hängt auch von weiteren Einstellungen ab. Wenn man den Zugriffe auf alle APIs blockiert, die randomisiert werden könnten (WebGL, HTML5 Canvas, Media Devices usw.), dann bleibt evtl. nur ein stabiles, eindeutiges Ergebnis übrig, dass langfristig wiedererkannt wird. Es gibt in-the-wild keine Anonymitätsgruppen, die eine nennenswerte Größe zum Abtauchen haben. Der Schutz entsteht durch den ständigen Wechsel der Verkleidung, durch die randomisierten Fakes der WebGL API. . . usw.

Testergebnisse

Alle oben genannten Methoden zum Schutz gegen Fingerprinting führen aufgrund der zufälligen Fakes zu einem einzigartigen Fingerprint, der sich aber für jede Domain und nach Neustart des Browsers ändern sollte, um eine Verknüpfung des Surfverhaltens über mehrere Webseiten und langfristige Wiedererkennung zu verhindern.

Wenn also eine Testseite sagt, dass der Browser einen eindeutigen Fingerprint hat, dann ist das völlig ok und entspricht der Intention. Ein brauchbare Testseite sollte auch den berechneten Gesamtfingerprint oder Teilergebnisse anzeigen (z. B. der Canvas- oder Fontfingerprint bei browserleaks.com), so dass man prüfen kann, ob das Ergebnis stabil ist oder sich nach Neustart ändert. Die Demoseite Fingerprint.com sollte nach einem Neustart das in Abb. 4.13 gezeigte Ergebnis zeigen.

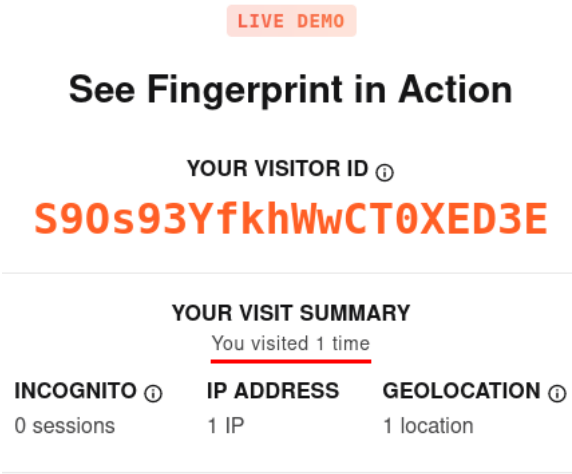


Abbildung 4.13: Testergebnis bei funktionierenden Schutz gegen Fingerprinting

4.8.2 Browser-Fingerprinting via CSS

CSS Fingerprinting verwendet trickreiche CSS Hacks statt Javascript, um Informationen über den Computer zu sammeln und daraus einen möglichst eindeutigen Fingerprint zu berechnen, der eine Wiedererkennung des Browsers ermöglichen soll. Man kann die installierten Schriftarten ermitteln, mit Mediaqueries die Bildschirmgröße schätzen (was ein alter Hut ist) u.v.a.m.

- In dem Paper *Web Browser Fingerprinting Using Only Cascading Style Sheets* (2015) wurde ein Konzept vorgeschlagen, um Surfer anhand des CSS Fingerprint ds Browsers zu verfolgen. Allerdings wurde nicht die gleiche Qualität wie beim Javascript Fingerprinting erreicht.[45]
- No-JS Fingerprint[46] demonstriert, dass man einen Fingerprint mit CSS statt Javascript berechnen kann. Allerdings wird nicht demonstriert, dass dieser Fingerprint individuell genug ist, um einzelne Surfer zu verfolgen. Ein TorBrowser unter Debian GNU/Linux und ein Mullvad Browser unter Fedora Linux hatten bei einem Test den gleichen CSS Fingerprint, so dass dieser Test in erster Linie eine Technologiedemo ist.

[45] https://ieeexplore.ieee.org/document/7424801
[46] https://noscriptfingerprint.com/

- In dem Paper *Implicit Stylistic Fingerprints for Bypassing Browsers' Anti-Fingerprinting Defenses* (Mai 2023) wird von Forschern von IBM Research ein verbessertes CSS Fingerprinting vorgestellt, dass standardmäßig eine vergleichbare Qualität wie Javascript Fingerprinting erreicht soll und deutlich besser als Javascript Fingerprinting abschneidet, wenn die Surfer Schutzmaßnahmen wie resistFingerprinting aktivieren oder Add-ons wie CanvasBlocker verwenden.[47]

Schutz gegen Fingerprinting via CSS

Eine Verteidigung durch Faken der via CSS Tricks gesammelten Daten, wie es beim Schutz gegen Javascript Fingerprinting gemacht wird, ist derzeit nicht möglich.

Folgende Verteidigungsmöglichkeiten stehen derzeit zur Vefügung:

- Die Filterlisten von uBlock Origin blockieren viele (die meisten?) Trackingsdienste mit nennenswerter Reichweite, egal welche Trackingmethoden eingesetzt werden.
- In dem Blockeintrag zum dem Paper von 2023 weisen die Autoren darauf hin, dass man CSS Fingerprinting durch das Blockieren von iFrames aushebeln kann, weil der Trackingdienst einen kleinen (unsichtbaren?) Bereich braucht, in welchem er seine CSS Tricks entfalten kann.
  - Das Add-on uBlock Origin kann iFrames von Drittseiten blockieren (siehe 4.7).
  - Wer noch konsequenter auch 1-Party iFrames blockieren möchte, könnte NoScript nutzen und Frames auch für *Trusted Sites* blockieren.

  Das führt dann allerdings auch dazu, dass man keine eingebetteten Medien mehr sieht, die man evtl. abspielen möchte. Um eingebette Medien auf einer Webseite abspielen zu können, muss man für die jeweilige Webseite individuelle Einstellungen definieren. Eine umfangreichere Einführung zu NoScript ist in 4.15 zu finden.

4.8.3 Hardware-Fingerprinting

Über verschiedene API-Schnittstellen können Trackingscripte Informationen über die Hardware des Rechners sammeln. Dies ist z. B. über die Messung der Performance aufwendiger Grafik-Rendering-Operationen oder beim Abspielen von Videos möglich.

Grafikhardware: Die Hardwarebeschleunigung des Rendering kann man deaktivieren, um ein Fingerprinting der Grafikhardware zu verhindern. Die Einbußen sind kaum erkennbar.

```
gfx.direct2d.disabled                    = true
media.hardware-video-decoding.enabled    = false
```

[47] https://research.ibm.com/publications/fashion-faux-pas-bypassing-browsers-anti-fingerprinting-defenses-through-stylistic-fingerprints

Vibrator-API: Über diese API kann eine Vibration des Gerätes ausgelöst werden. Die Funktion liefert keine Informationen zur realen Ausführung. Das Ergebnis ist FALSE, wenn die Parameter nicht korrekt waren, und TRUE in allen anderen Fällen. Wenn eine ausgelöste Vibration länger als die maximal zulässige Dauer ist, wird sie ohne Rückmeldung gekürzt.

Die Vibrator-API kann in Kombinationen mit anderen Mechanismen die Privatsphäre gefährden, wie das W3C in den *Security and Privacy Considerations* schreibt:

> *Vibration API provides an indirect privacy risk, in conjunction with other mechanisms. This can create possibly unexpected privacy risks, including cross-device tracking and communication. Additionally, a device that is vibrating might be visible to external observers and enable physical identification, and possibly tracking of the user.*

Die komplette Deaktivierung der Vibrator-API könnte als Fingerprinting-Merkmal ausgewertet werden, da die API im Navigator-Objekt nicht mehr sichtbar wäre. Unauffälliger ist es, die maximale Vibrationsdauer auf 0 zu setzen.

```
dom.vibrator.max_vibrate_ms = 0
```

Sensoren: Die Sensor-API von Firefox liefert folgende Daten aus der Umgebung:

1. Ambient Light Sensor: kann die die Helligkeit der Umgebung abfragen.
2. Proximity Sensor: kann Objekte in der Nähe erfassen.
3. Device Orientation Sensor: liefert Informationen darüber, wie ein Phone gehalten wird.
4. Device Motion Sensor: liefert Informationen über die Bewegung des Gerätes.

Die ersten beiden APIs sind datenschutzrelevant und können zum Sammeln von Daten missbraucht werden, wie der Sicherheitsexperte L. Oljenik für den Proximity und den Ambient Light Sensor demonstrierte. Beide sind in Firefox standardmäßig deaktiviert.

Sensoren für die Lage eines Gerätes und Gyroskope zur Beobachtung von Bewegungen sind in Smartphones vorhanden, aber in der Regel nicht in PCs oder Laptops. Daher liefern die beiden letztgenannten APIs auf diesen Geräten keine Daten und können daher aktiviert bleiben. Webseiten könnten eine Deaktivierung erkennen und als Merkmal für das Fingerprinting verwenden, wie Browserleaks demonstriert.[48]

Aus den gleichen Gründen wird die Deaktivierung der gesamten Sensor-API nicht empfohlen. Für Smartphones ist das Risiko anders zu bewerten.

4.9 URL-Parameter

URL-Parameter werden häufig mit folgenden Intentionen für das Tracking verwendet:

1. Beim Tracking des Erfolgs von Werbekampagnen liefern URL-Parameter detailliertere Informationen als der Referer. In den Anleitungen von Google Analytics und Yandex Analytics wird das Verfahren detailliert beschrieben. Diese URL-Parameter der Großen sind gut bekannt und können gefiltert werden.

[48] https://browserleaks.com/features

Die Technik dazu wurde von der Urchin Software Corporation entwickelt, die 2005 von Google übernommen und in das eigene Portfolio integriert wurde. Deshalb beginnen die Trackingparameter bei Google noch heute mit *utm_* (Urchin Tracking Module).

2. Mit dem URL-Kampagnen-Mapper von WebTrekk kann jede Webseite individuelle Trackingparameter nutzen, die nur schwer gesammelt und blockiert werden können.

3. Außerdem können Tracking-IDs in Parametern kodiert werden, die die Container von Firefox austricksen und webseitenübergreifendes Tracking ermöglichen.

   Facebook hängt bspw. an Klicks auf Links zu den Drittseiten den Parameter *fbclid* mit einer eindeutigen ID an, um auf der Zielseite den Surfer mit Hilfe von HTML-Wanzen wiederzuerkennen und damit webseitenübergreifend (und App-übergreifend) ohne Cookies/EverCookies zu tracken.

Ein Beispiel von der Webseite heise.de (Mobil) zeigt beide Anwendungen für das Tracking mit URL-Parametern durch WebTrekk mit dem Referer (wt_ref) und einer numerischen ID (wt_t):

```
https://m.heise.de/foto/?wt_ref=https%3A%2F%2Fwww.heise.de&wt_t=1618985578
```

Die URL-Parameter ermöglichen auch ein Tracking über mehrere Apps. Viele Online-Medien in Deutschland betreiben bspw. einen Kanal auf Twitter oder Telegram und posten Links zu aktuellen Artikeln, die mit Trackingparametern verseucht sind.

Da das webseitenübergreifende Tracking mit Cookies immer schwieriger wird, gewinnen URL-Parameter mit Tracking-IDs an Popularität. Das sieht man u. a. am Wachstum der *AdGuard URL Tracking Protection List*. Im Juli 2021 hatte das AdGuard-Team 225 Trackingparameter in URLs identifiziert. Im März 2023 war die Liste auf 951 gewachsen.

Trackingparameter aus URLs entfernen (Firefox)

Firefox kann Trackingparameter beim Wechsel der Top-Level-Domain aus den URLs entfernen. Bei Links innerhalb der gleichen Top-Level-Domain werden die Parameter nicht entfernt, um Probleme zu vermeiden. Damit wird webseitenübergreifendes Tracking verhindert.

Die Funktion ist aktiv, wenn man in Firefox 102+ den strengen Trackingschutz in den Einstellungen oder unter *about:config* folgende Option aktiviert:

```
privacy.query_stripping.enabled = true
```

Standardmäßig wird eine interne Liste von Parametern genutzt, die bspw. die Trackingparameter von Facebook aus den URLs entfernt, aber nicht die UTM-Parameter von Google. Man kann die Liste der URL-Parametern konfigurieren, die entfernt werden sollen. Die folgende Liste mit eindeutigen Tracking-IDs wird vom Librewolf verwendet und wurde mit den UTM-Parametern ergänzt:

```
privacy.query_stripping.strip_list = __hsfp __hssc __hstc __s _hsenc
↪ _openstat dclid fbclid gbraid gclid hsCtaTracking igshid mc_eid
↪ ml_subscriber ml_subscriber_hash msclkid oly_anon_id oly_enc_id
↪ rb_clickid s_cid twclid vero_conv vero_id wbraid wickedid yclid ysclid
↪ utm_campaign utm_channel utm_cid utm_content utm_id utm_medium utm_name
↪ utm_place utm_pubreferrer utm_reader utm_referrer utm_serial utm_social
↪ utm_social-type utm_source utm_swu utm_term utm_keyword utm_userid
↪ utm_viz_id utm_product utm_campaignid utm_ad utm_brand utm_emcid
↪ utm_emmid utm_umguk
```

Firefox 120+ kann die Trackingparameter aus den URLs nicht nur beim Aufrufen sondern auch beim Kopieren von Links entfernen. Dafür gibt es einen extra Eintrag im Kontextmenü (Rechtsklick auf den Link) und es wird ebenfalls diese Liste verwendet.

Trackingparameter mit uBlock Origin aus URLs löschen

Auch mit dem Add-on **uBlock Origin** kann man Parameter aus URLs entfernen. Dafür muss man eine Liste von Filterregeln erstellen, bspw. für das Facebook-Tracking:

```
$removeparam=fb_action_ids
$removeparam=fb_action_types
$removeparam=fb_comment_id
$removeparam=fbclid
```

. . . oder Trackingparameter auf einer bestimmten Webseite (bspw. eBay):

```
||www.ebay.$removeparam=_trkparms
||www.ebay.$removeparam=_trksid
||www.ebay.$removeparam=mkrid
||www.ebay.$removeparam=campid
```

uBlock Origin enthält die Liste *URL Tracking Protection* vom AdGuard Team[49], die statt der mageren 20-30 URL Parameter in Firefox mehr als 1.200 Einträge enthält und die man unter *Filterlisten* im Abschnitt *Privatspäre* aktivieren kann: (Abb. 4.14):

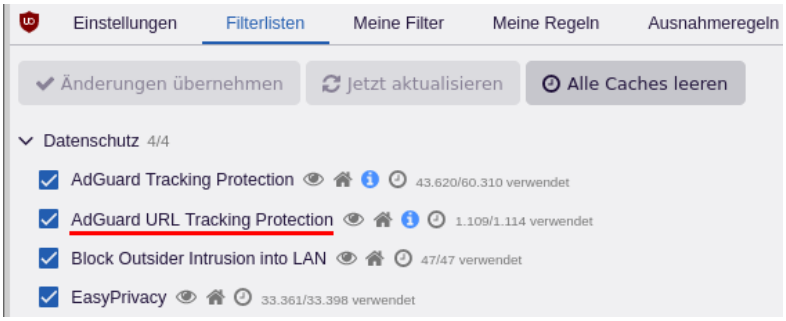


Abbildung 4.14: uBlock Origin: Filterliste für Trackingparameter in URLs aktivieren

4.10 Zugriff auf lokale URLs blockieren

Neugierige oder bösartige Webseiten könnten z. B. mit JavaScript über Adressen wie *http://localhost. . .* oder *http://192.168.1.1. . .* auf lokale Dienste auf dem eigenen Rechner, auf den Router, Netzwerkdrucker oder auf andere Dienste im lokalen Netzwerk (LAN) zugreifen:

[49] https://raw.githubusercontent.com/AdguardTeam/FiltersRegistry/master/filters/filter_17_TrackParam/filter.txt

- Bösartiger Javascript Code könnte lokale Dienste auf dem eigenen Rechner (wie z.B. CUPS) oder andere Rechner, Drucker usw. im LAN angreifen. Ein Klassiker ist der *Cross-Site-Printing Angriff*[50], bei dem aus dem Browser heraus ein Drucker im LAN attackiert wird. Wenn dieser Drucker oder Druckserver verwundbar ist (siehe: BSI Warnung von 2021 zu HP Netzwerkdrucker[51] oder Microsofts PrintNightmare[52]), kann der Angreifer nach erfolgreicher Kompromittierung des Druckers das gesamte lokale Netzwerk übernehmen.
- Auch Internetrouter können aus dem Browser heraus angegriffen werden. Mai 2015 wurde ein Exploit-Kit entdeckt, der als Javascript auf Webseiten platziert wird und bei Aufruf der Webseite automatisiert gängige Router angreift, um die DNS-Einstellungen zu ändern und damit den Internetzugriff beliebig zu manipulieren.[53]
- Die Firma ThreadMetrix hat 2015 für die Webseiten von Banken einen Sicherheitsmechanismus entwickelt, der unter anderem via JavaScript bestimmte Ports auf dem lokalen Rechner scannt, die für einige Viren, Fernwartungssoftware und Remote-Desktops wie VNC typisch sind. Seit Mai 2020 ist ein ähnliches Feature auch bei eBay aktiv, wenn eBay vermutet, dass der Anwender Windows nutzt. Dabei handelt es sich um ein Sicherheitsfeature und keinen Angriff oder Tracking, aber trotzdem ...

JShelter: Network Boundary Shield (bevorzugt)

Das Network Boundary Shield (HTTP Shield) des Add-ons JShelter ist nach der Installation standardmäßig aktiv. Es blockiert alle Zugriffe von Webseiten aus dem Internet auf lokale Adressen und nutzt dabei die DNS-API von Firefox. Damit ist sichergestellt, dass ein Angreifer den Schutz nicht mit DNS-Namen wie die typischen Namen von Routern oder dem DNS-Suffix des lokalen Netzes der Firma umgehen kann.

Wenn eine Webseite aus nachvollziehbaren Gründen(!) eine Freigabe braucht, kann man mit zwei Klicks eine Ausnahme definieren und den HTTP Shield für die aktuelle Seite deaktivieren.

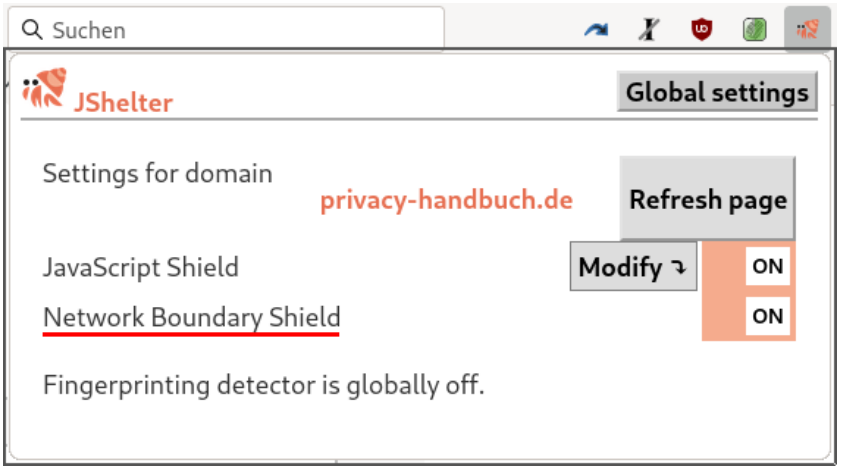


Abbildung 4.15: Network Boundary Shield für eine Webseite deaktivieren

Hinweis: Dass eine Webseite irgendwie nicht wie erwartet funktioniert, ist KEIN plausibler Grund für die Deaktivierung. Das zeigt nur, dass ein Angreifer aktiv versucht, etwas zu tun, was

[50] https://book.hacktricks.xyz/network-services-pentesting/pentesting-printers/cross-site-printing
[51] https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-548868-10M2.html
[52] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
[53] https://heise.de/-2665387

verboten wurde. Gerade in dieser Situation wäre die Schutzfunktion wichtig. Man sollte sich nicht austricksen lassen und eine Schutzfunktion ohne plausiblen Grund deaktivieren, nur weil man neugierig ist und sehen will, wie die Webseite korrekt dargestellt aussehen würde.

uBlock Origin mit Filterliste

Nachdem eBay im Mai 2020 begonnen hatte, die lokalen Ports zu scannen, hat das uBlock-Team die Liste *Block Intrusion into LAN* erstellt, die im Abschnitt *Privatsphäre* zu finden ist (Abb. 4.16). Diese Filterliste kann man als Alternative nutzen, wenn man das Add-on JS-Restrictor nicht verwenden möchte, oder sie zusätzlich zum Network Boundary Shield von JShelter verwenden.

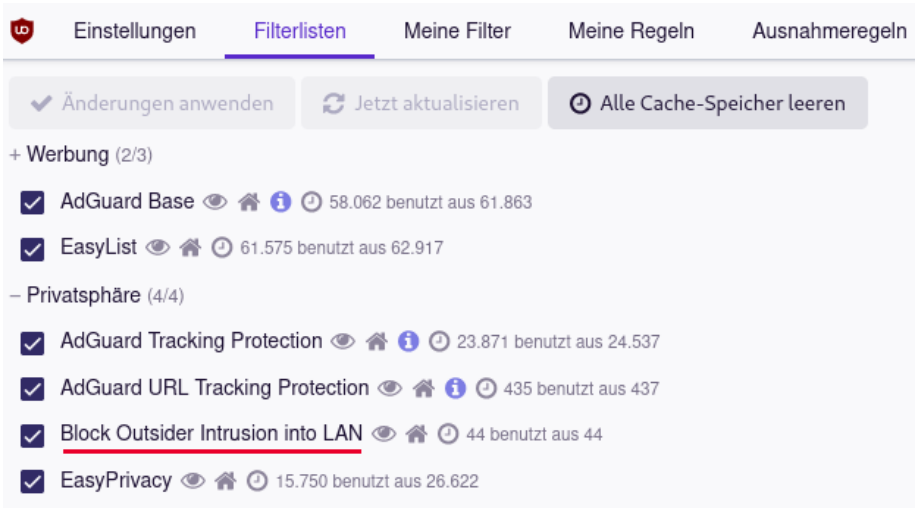


Abbildung 4.16: uBlock Origin: Filterliste *Block Intrusion into LAN* aktivieren

Hinweis: falls die Liste nicht sichtbar ist, muss man auf den Button *Aktualisieren* klicken.

Da uBlock Origin auf Basis der DNS-Namen blockiert und im Unterschied zu JS-Restrictor für diese Aufgabe nicht die DNS-API von Firefox verwendet, müssen zusätzlich die DNS-Namen der lokalen Netzwerke blockiert werden. Sonst könnte ein Angreifer den Schutz mit DNS-Namen umgehen.

uBlock Origin enthält bereits eine Liste typischer DNS Namen, die für die üblichen Router verwendet werden. Als Privatanwender ist man also in der Regel geschützt.

Wenn man untypische Einstellungen für die DNS-Suffix im eigenen LAN gewählt hat, im lokalen Netz einer Firma arbeitet oder via VPN mit einem Firmennetz verbunden ist, muss man für diese lokalen Netzwerke zusätzliche Regeln definieren, um den Zugriff für Webseiten zu sperren. Dafür fügt man auf dem Reiter *Meine Filter* eine Regel nach folgendem Muster ein:

```
||<DNS-Suffix>^$3p,domain=~localhost|~127.0.0.1|~[::1]|~0.0.0.0|~[::]|~local
```

4.11 Referer

Mit jedem Klick auf einen Link sendet der Browser einen Referer im HTML-Header an die aufgerufene Webseite und teilt mit, von welcher Webseite der Surfer gekommen ist.

Bei der Einblendung von Bildern, Videos oder Werbung durch Dritte liefert der Referer die Information, welche Seite man gerade betrachtet. Es ist ein gut geeignetes Merkmal für das Tracking mit Werbung, HTML-Wanzen oder Like-Buttons – die Schleimspur im Web.

Die Studie *Privacy leakage vs. Protection measures*[54] zeigt, dass außerdem viele Webseiten private Informationen via Referer an Trackingdienste übertragen. Das folgende Beispiel zeigt den Aufruf eines Werbebanners nach dem Login auf der Webseite http://sports.com:

```
GET http://ad.doubleclick.net/adj/....
Referer: http://submit.sports.com/...?email=name@email.com
Cookie: id=123456789.....
```

Mit einer eindeutigen User-ID (im Beispiel ein Tracking-Cookie) kann das Surfverhalten über viele Webseiten verfolgt werden. Durch zusätzliche Informationen (im Beispiel eine E-Mail-Adresse) werden die gesammelten Datensätze personalisiert. Im Rahmen der Studie wurden 120 populäre Webseiten untersucht. 56 % der Webseiten sendeten nach dem Login private Informationen wie E-Mail-Adresse, Name oder Wohnort an Trackingdienste.

Firefox bietet sehr graduell abgestufte Möglichkeit, das Senden des Referers zu modfizieren. Folgende Einstellungen kann man unter *about:config* aktivieren, um die Privatsphäre zu verbessern und das Tracking zu erschweren ohne das Surferlebnis zu beeinträchtigen:

- Das Senden des Referers an externe Drittseiten ist (meistens) überflüssig, also:

  ```
  network.http.referer.XOriginPolicy = 1
  ```

- Um auch die kleinsten Restprobleme zu vermeiden, die bei Nutzung von Google Diensten o.ä. entstehen könnten, verwenden TorBrowser, MullvadBrowser und andere Projekte folgenden Einstellungen, die den Referer an Drittseiten auf den Servernamen kürzen:

  ```
  network.http.referer.XOriginPolicy         = 0
  network.http.referer.XOriginTrimmingPolicy = 2
  ```

  Das Beispiel von oben für den Aufruf von Daten von Drittseiten würde dann so aussehen:

  ```
  GET http://ad.doubleclick.net/adj/....
  Referer: http://submit.sports.com/
  Cookie: id=123456789.....
  ```

  Das führt dann aber dazu, dass bei Klick auf einen Link zu einer anderen Webseite im Log der Zielwebseite erkennbar ist, von welcher Domain man gekommen ist. Suboptimal, die Schleimspur des Referers sollte unterbrochen werden, wenn man die Domain wechselt.

Folgenden Einstellungen sind nicht empfehlenswert, weil sie nur wenig Verbesserung für die Privatsphäre bieten aber sich negativ auf das Surferlebnis auswirken können:

[54] http://w2spconf.com/2011/papers/privacyVsProtection.pdf

- Wenn man Subdomains als Drittseiten behandelt und keinen Referer sendet, könnte das auch gegen Trackingdienste schützen, die sich mit DNS-Aliases als Subdomains auf populären Webseiten einschleichen (z.B. WebTrekk bei Heise.de und Zeit.de).

  ```
  network.http.referer.XOriginPolicy = 2
  ```

  Allerdings werden diese Trackingdienste durch uBlock Origin blockiert, da die DNS-Aliases aufgelöst und blockiert werden. Diese Einstellung führt auf einigen Webseiten zu Problemen mit dem Login und teilweise auch zu Problemen beim Laden von Content von Subdomains.

- Einige Webseiten zum Thema Privacy empfehlen, das Senden des Referers mit folgender Option komplett zu deaktivieren:

  ```
  network.http.sendRefererHeader = 0
  ```

  Innerhalb einer Domain kann der Webmaster einen Surfer aber immer verfolgen. Diese Einstellung führt zu Problemen beim Login und auch beim Versand von Kommentaren in Diskussionsforen und Blogs, die den Referer als Feature zur Erkennung von Spam-Bots auswerten.

4.12 Installierte Schriftarten verstecken

Informationen über installierte Schriftarten können mit JavaScript, Flash oder Java ausgelesen und zur Berechnung eines individuellen Fingerprint des Browsers genutzt werden. Viele Trackingdienste nutzen inzwischen diese Technik. Die Studie *Dusting the web for fingerprinters*[55] der KU Leuven (2013) kommt zu dem Schluss, dass mindestens 0,5–1,0 % der Webseiten die installierten Schriftarten für Trackingzwecke auslesen.

Der Download von (exotischen) Schriftarten wird auch von Google zum Tracking genutzt. Viele Webdesigner nutzen Schriften vom Google Font Service, statt fünf Minuten Arbeit zu investieren und die Schriftarten auf dem eigenen Webserver bereitzustellen.

Für den Webdesigner ist die Einbindung der Google-Fonts sehr einfach:

1. Der Webdesigner muss nur ein kleines CSS-Stylesheet importieren. Um die Schriftart OpenSans zu nutzen, reicht folgende Zeile:

   ```
   <link href='https://fonts.googleapis.com/css?family=Open+Sans'
   ↪  rel='stylesheet' type='text/css'>
   ```

2. Beim Aufruf der Webseite lädt der Browser das Stylesheet von dem Google-Server *fonts.googleapis.com*. Das Stylesheet enthält die Links zum Download der Fonts.

3. Der Browser holt sich dann die Dateien mit Schriftarten vom Server *fonts.gstatic.com* und zeigt die Webseite an. Die Font-Dateien werden für 24 Stunden im Cache gespeichert.

Für das Laden von Schriftarten vom Google Font Service gelten die Datenschutzbestimmung von Google[56]. Viele Webseiten weisen in den Privacy-Statements nicht darauf hin, dass beim Aufruf der Webseite Daten bei Google gespeichert und verarbeitet werden.

[55] https://www.cosic.esat.kuleuven.be/publications/article-2334.pdf
[56] https://www.google.com/intl/de/policies/privacy/

Das Laden von Schriftarten aus dem Internet ist außerdem ein Sicherheitsrisiko, weil damit Angriffe direkt auf das Betriebssystem möglich werden. Programmierfehler in den Font-Rendering-Bibliotheken, die Remote Code Execution auf Systemlevel durch das Laden von bösartigen Schriften erlaubten, gab es für Windows (ms11-087, ms15-078), Linux (CVE-2010-3855) oder OpenBSD (CVE-2013-6462). Das Google Security Team hat zwischen 2015 und 2017 mit der Code Fuzzing Software *BrokenType* weitere 40 Bugs im Windows-Kernel und Font-Rendering gefunden, die ein Angreifer nutzen konnte, um mit bösartigen Fonts den Rechner anzugreifen und Code mit Systemrechten auszuführen.[57]

Potente (staatliche) Hacker kombinieren Bugs im Font-Rendering gern mit 0-Days-Bugs im Browser, um nach der Kompromittierung des Browsers den Rechner zu übernehmen:

- Der Bug *ms15-078* wurde von der Firma Hacking Team zur Installation eines Überwachungstrojaners genutzt.
- Im Januar 2021 wurde ein komplexer Angriff auf Windows-Rechner und Android-Smartphones publiziert, bei dem bösartige Schriften auf Webseiten eingebunden und durch Kombination von vier 0-Day-Exploits im Browser Chrome und im Font-Rendering die Computer und Smartphones der Targets übernommen wurden. Die Bugs sind seit April 2020 gefixt und damit verbannt.

  Bruce Schneier vermutet einen staatlichen Angreifer wie die NSA dahinter. Allerdings ist das Spekulation und es gibt keine echten Beweise, die auf die NSA zeigen.

Blockieren externer Schriftarten mit Add-ons?

Einige Firefox-Add-ons wie uBlock Origin oder uMatrix können mit einer Option den Download von zusätzlichen Schriftarten blockieren. Dabei gibt es folgende Nachteile:

1. Es wird beim Google Font Service nur der zweite Schritt blockiert. Das Stylesheet wird trotzdem von Google geladen. Wenn man keine Fonts von Google verwenden möchte, dann sollte man *fonts.googleapis.com* mit einer Filterregel blockieren.
2. Die Add-ons können nicht zwischen Fonts für eine hübsche Schrift (entbehrlich) und notwendigen Fonts für die Darstellung von Icons für die Navigation unterscheiden. Viele Webseiten werden dadurch unbrauchbar.
3. Das Blockieren des Downloads externer Schriftarten schützt nicht gegen das Auslesen lokal installierter Fonts für das Fingerprinting des Browsers.

Deshalb ist die Nutzung des Features *externe Schriftarten blockieren* in uBlock Origin oder uMatrix suboptimal und wird hier nicht empfohlen.

Sichtbarkeit der lokal installierten Schriftarten reduzieren

Man könnte die für Webseiten sichtbaren, lokal installierten Fonts einschränken. Damit können die Informationen reduziert werden, die Trackingscripte via Font FIngerprinting sammeln können. Folgende Werte sind möglich:

[57] https://www.heise.de/-4155012

```
layout.css.font-visibility = 1 - nur Schriftarten des Basissystems sichtbar
layout.css.font-visibility = 2 - zus. Schriftarten von Sprachpacketen verwendbar
layout.css.font-visibility = 3 - zus. auch die vom Nutzer installierten Fonts
```

Bei Firefox 115.x ESR heißt der Parameter *layout.css.font-visibility.standard*.

Webseiten das Verwenden individueller Schriftarten verbieten

Um das Laden externer Schriftarten zu blockieren, deaktiviert man in den Einstellungen die Optionen *Webseiten das Verwenden von eigenen Schriften erlauben* und die CSS Font Loading API. Damit sehen einige Webseiten nicht mehr ganz so hübsch aus, die Einschränkungen sind aber gering:

```
browser.display.use_document_fonts   = 0
layout.css.font-loading-api.enabled  = false
```

Das Underline Handling sollte man deaktivieren, da es zum Fingerprinting der installierten Schriftarten und zur Erkennung des Betriebssystems verwendet werden kann:

```
font.blacklist.underline_offset = "" (leerer String)
```

Immer mehr Websites verwenden Webicon-Fonts für die Darstellung von Symbolen. Häufig sieht man statt der Symbole seltsame Zeichen, weil der passende Font mit den Symbolen nicht aus dem Internet geladen wird. Das Web wird damit unbenutzbar.

Um diese Probleme zu vermeiden, ist die Freigabe von downloadbaren Schriften für die Darstellung von Symbolen empfehlenswert für weniger strenge Sicherheitsanforderungen. Damit werden Icons wieder korrekt dargestellt:

```
gfx.downloadable_fonts.enabled  = true
```

Für hohe Sicherheitsanforderungen kann man das Rendering von OpenType-SVG-Fonts und die Graphite Engine deaktivieren, um die Angriffsfläche zu reduzieren. Die Graphite Engine wird nur für die verbesserte Darstellung komplexer asiatischer Schriften benötigt:

```
gfx.font_rendering.opentype_svg.enabled  = false
gfx.font_rendering.graphite.enabled      = false
```

Um die Lesbarkeit von Webseiten zu verbessern, sollte man gut lesbare Standardschriften verwenden. Unter Windows eignet sich *Arial*, unter Linux *Liberation Sans*. Man findet die Option in den Firefox-Einstellungen auf dem Reiter *Inhalt*. Klicken Sie auf den Button *Erweitert*, um im folgenden Dialog die Standardschriftarten zu wählen.

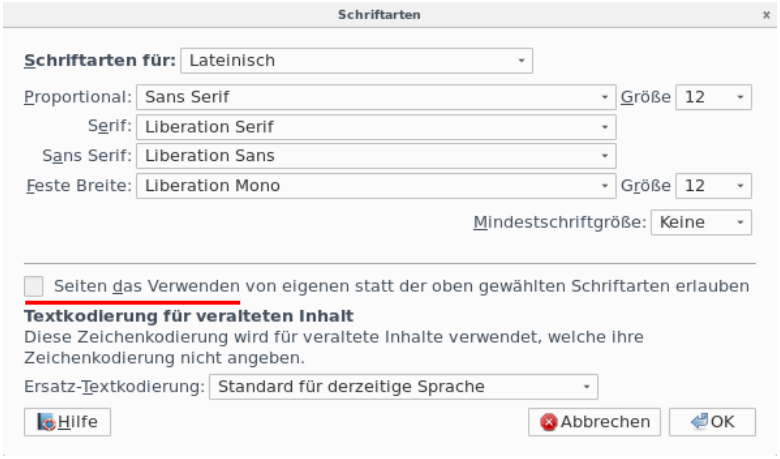


Abbildung 4.17: Schriftarten auswählen

4.13 Browsercache und Surf-Chronik

Browser speichern Informationen über besuchte Webseiten in einer Surf-History. Ein Experiment des Isec Forschungslabors für IT-Sicherheit zeigt, dass die Surf-History zur Deanonymisierung genutzt werden kann. Anhand der Browser-History wurde ermittelt, welche Gruppen der Surfer bisher bei Xing besucht hat. Da es kaum zwei Nutzer gibt, die zu den gleichen Gruppen gehören, konnte mit diesen Daten eine Deanonymisierung erfolgen. Die Realnamen und die E-Mail-Adressen der Surfer konnten ermittelt werden.[58]

Eine Studie der University of California von 2010 zeigte, dass ca. 1 % der Websites versuchten, die Chronik über zuvor besuchte Websites anhand der unterschiedlichen Formatierung der Links von besuchten und nicht besuchten Webseiten auszulesen. Trackingdienste wie Tealium oder Beancounter versuchten ebenfalls, die Formatierung von Links auszuwerten. (Gegen diese Angriffe sind aktuelle Firefox-Versionen immunisiert.)

Außerdem speichert der Browser die besuchten Webseiten, Bilder und Medien im Cache. Mit jeder aufgerufenen Webseite wird vom Server ein ETag gesendet, welches der Browser zusammen mit den Daten der Webseite (HTML, Bilder, JS) im Cache speichert. Wird die Webseite erneut aufgerufen, sendet der Browser zuerst das ETag an den Webserver, um zu erfragen, ob sich die Webseite geändert hat. Wenn der Server antwortet, dass für dieses ETag keine Änderungen vorliegen, dann verwendet der Browser die Daten aus dem Cache. Ein ETag kann eine eindeutige ID enthalten, die als EverCookie zum Tracking verwendet werden kann. KISSmetrics verwendet diese Trackingtechnik seit 2011.[59]

Schutz gegen Tracking über mehrere Webseiten

Gegen Tracking über mehrere Domains schützen Surf-Container. Die Netzwerk-Partitionierung zum Schutz gegen Tracking mit EverCookies wie ETags ist seit Firefox 85 standardmäßig aktiviert.

[58] https://www.heise.de/newsticker/meldung/Plaudertasche-Web-Browser-erleichtert-Deanonymisierung-919076.html
[59] https://heise.de/-1288914

Schutz gegen langfristiges Tracking

Gegen längerfristige Wiedererkennung auf häufiger besuchten Webseiten schützt das Deaktivieren der Surf-History und das Löschen des Cache usw. beim Beenden des Browsers.

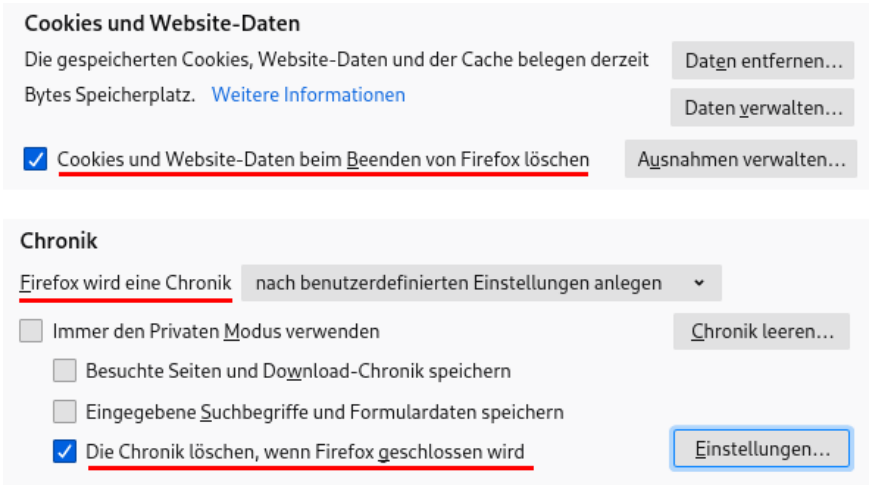


Abbildung 4.18: Deaktivieren der Surf-History und Löschen des Cache

Die Einstellungen zum Löschen des Cache und der Chronik beim Schließen des Browsers findet man in den *Einstellungen* in der Sektion *Datenschutz und Sicherheit* (Abb. 4.18).

Wenn man auf den Button *Einstellungen* hinter *Die Chronik löschen, wenn Firefox geschlossen wird* klickt, kann man festlegen, welche Daten beim Schließen des Browsers gelöscht werden.

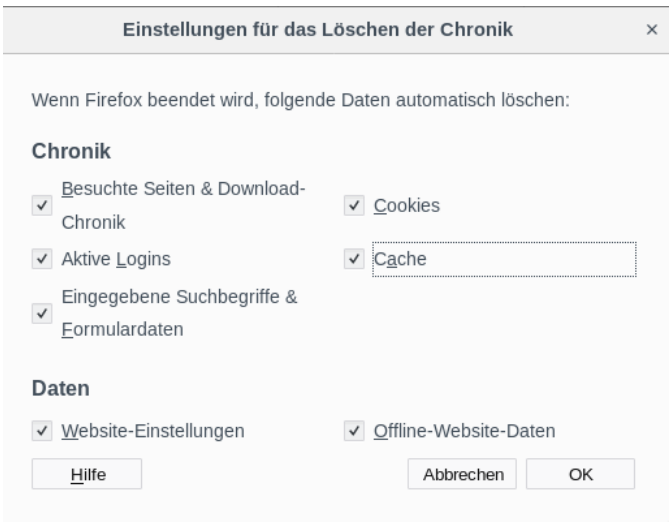


Abbildung 4.19: Konfiguration der zu löschenden Daten beim Beenden

Alternativ kann man unter *about:config* folgende Werte setzen:

```
places.history.enabled                = false
privacy.history.custom                = true
privacy.sanitize.sanitizeOnShutdown   = true
privacy.clearOnShutdown.cache         = true
```

```
privacy.clearOnShutdown.history       = true
privacy.clearOnShutdown.offlineApps   = true
privacy.clearOnShutdown.sessions      = true
```

Während des Surfens kann man die Chronik mit der Tastenkombination STRG-SHIFT-ENTF löschen oder über *Extra* → *Neueste Chronik löschen* (Abb. 4.20).

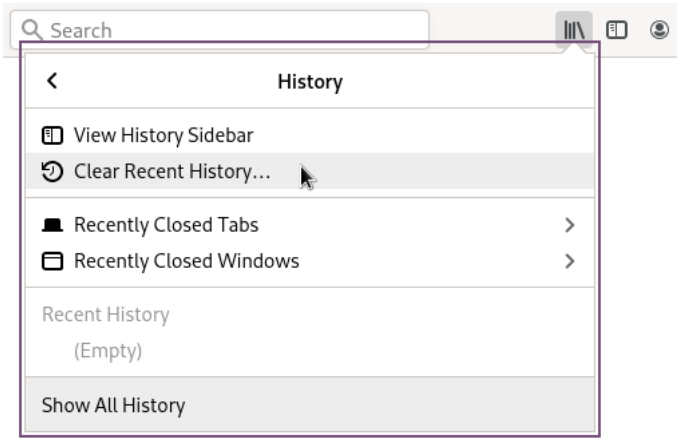


Abbildung 4.20: Chronik während des Surfens löschen

Disk-Cache deaktivieren

Firefox verwendet einen Cache im Hauptspeicher und einen Disk-Cache auf der Festplatte. Der Cache im Hauptspeicher ist mit 64 MB groß genug für eine Surf-Session. Den Disk-Cache kann man deaktivieren und damit auch überflüssige Spuren auf dem Rechner vermeiden, die forensisch sichtbar gemacht werden könnten. Unter *about:config* sind dafür folgende Variablen zu setzen:

```
browser.cache.disk.enable         false
browser.cache.disk_cache_ssl      false
browser.cache.offline.enable      false
```

4.14 Risiko Plugins

Für die Darstellung von Inhalten, die nicht im HTML-Standard definiert sind, kann Firefox Plug-ins nutzen. Sie werden in der Add-on-Verwaltung in der Sektion *Plugins* aktiviert. Um zu verhindern, das bei der Installation von irgendwelchen Softwarepaketen ungewollt Browser-Plug-ins automatisch aktiviert werden, kann man folgende Variable unter *about:config* setzen:

```
plugin.default.state = 0
```

Um unter Windows das automatische Scannen der Registry nach neuen Plug-ins zu deaktivieren, ist unter *about:config* folgende Variable zu setzen:

```
plugin.scan.plid.all = false
```

4.14.1 Media-Plug-ins für Video und Audio

Die Einstellungen zum Deaktivieren des automatischen Abspielens von Audio und Video hat Mozilla immer wieder geändert. Mit folgenden Einstellungen unter *about:config* deaktiviert man das automatische Abspielen von Videos und Audio:

```
media.autoplay.default         = 5
media.autoplay.blocking_policy = 2
```

Das Deaktivieren des automatischen Abspielens von Videos ist auch ein Sicherheitsfeature, das den Start eines bösartigen Videos im Hintergrund verhindert und die Angriffsfläche für Drive-by-Download Angriffe verringert.

Für einige Video- und Audioformate verwendet Firefox externe Plug-ins zum Abspielen. Standardmäßig werden von Firefox zwei Media-Plug-ins verwaltet:

Videocodec OpenH264 von Cisco wird für WebRTC benötigt und die Wiedergabe einige Medien in Mediatheken. Wenn man WebRTC abschaltet und, kann man aus Sicherheitserwägungen auch den Videocodec und das Update deaktivieren:

```
media.gmp-gmpopenh264.autoupdate       = false
media.gmp-gmpopenh264.enabled          = false
media.gmp-gmpopenh264.provider.enabled = true
```

Außerdem kann man das Plug-in OpenH264 in der Add-on-Verwaltung ausblenden:

```
media.gmp-gmpopenh264.visible = false
```

Bei einige Linux Distributionen wie Fedora ist OpenH264 im Firefox standardmäßig deaktiviert. Der Codec wird dann bevorzugt über die Paketverwaltung installiert:

```
> sudo dnf install mozilla-openh264
```

Widevine Content Decryption Module von Google zur Wiedergabe von DRM-geschützten Videos ist unter Windows standardmäßig aktiviert, bei den meisten Linux-Distributionen aber standardmäßig deaktiviert. Man braucht es nicht notwendigerweise. Mit folgendem Wert unter *about:config* kann man es komplett deinstallieren:

```
media.eme.enabled = false
```

Wenn man es wirklich nicht verwenden und auch nicht von irgendwelchen Webseiten immer wieder mit Hinweisen *Bitte den DRM Kopierschutz freischalten!* genervt werden will, kann man Warnungen und Aktivierung mit folgender Einstellung verstecken:

```
browser.eme.ui.enabled = false
```

4.14.2 Anzeige von PDF-Dokumenten

Adobes Acrobat-Plug-in für die Anzeige von PDF-Dokumenten im Browser war über viele Jahre ein erhebliches Sicherheitsrisiko. 2008 gelang es dem *Ghostnet*, mit bösartigen PDF-Dokumenten die Computernetze westlicher Regierungen, der US-Regierung und des Dalai Lama zu infizieren. Dem Trojaner *MiniDuke* gelang es 2012, mit bösartigen PDFs in die Computer von Regierungsorganisationen in Deutschland, Israel, Russland, Belgien, Irland, Großbritannien, Portugal, Rumänien, Tschechien und der Ukraine einzudringen, und der Wurm *Win32/Auraax* wurde ebenfalls mit bösartigen PDF-Dokumenten verteilt.

Aktuelle Firefox-Versionen verwenden die JavaScript-Bibliothek **PDF.js** für die Anzeige von PDF-Dokumenten. Auch diese Bibliothek hatte schon kritische Sicherheitslücken, die von Angreifern aktiv ausgenutzt wurden (z. B. CVE-2015-0802, CVE-2015-0816 oder CVE-2015-4495). Wenn man die Ausführung von Scripting-Code in PDF-Dokumenten verbietet, kann man die Angriffsfläche deutlich verringern:

```
pdfjs.enableScripting = false
```

Für hohe Sicherheitsanforderungen kann man die Anzeige von PDF-Dokumenten im Browser deaktivieren und einen externen PDF-Viewer zum Lesen der Dokumente verwenden:

```
pdfjs.disabled = true
```

Statt funktionsüberladener Monster-Applikationen kann man einfache PDF-Reader nutzen, die sich auf die wesentliche Funktion des Anzeigens von PDF-Dokumenten beschränken. Die FSFE stellt auf PDFreaders.org[60] Open-Source-Alternativen vor.

- Für Windows werden *Sumatra PDF* oder *MuPDF* empfohlen.
- Für Linux gibt es *Okular* (KDE) und *Evince* (GNOME, XFCE, Unity).

Die Linux-Distribution **QubesOS** bietet für potentielle *Landesverräter* und andere Risikogruppen, die als Target für den Einsatz der neuen Bundestrojaner infrage kommen, einige besondere Sicherheitsfeatures. Dazu gehört die Anzeige von PDFs in einer Wegwerf-VM oder die Umwandlung von PDF-Dokumenten aus unbekannten Quellen in Trusted PDFs, die man risikolos weitergeben kann. Die Funktionen kann man nach dem Download mit einem Rechtsklick auf ein PDF-Dokument im Dateimanager aufrufen.

Für die Umwandlung in Trusted PDFs wird *qubes-app-linux-pdf-converter*[61] gestartet, das Rendering des (möglicherweise bösartigen) PDF-Dokuments erfolgt in einer Wegwerf-VM, die danach gelöscht wird. Die gerenderten Bitmaps werden zu einem neuen, ganz harmlosen PDF zusammengesetzt. Wie bei QubesOS üblich, dauert der Vorgang insbesondere bei großen PDF-Dokumenten einige Zeit. (Eile ist ein Feind der Sicherheit!)

[60] https://pdfreaders.org/index.de.html
[61] https://github.com/QubesOS/qubes-app-linux-pdf-converter

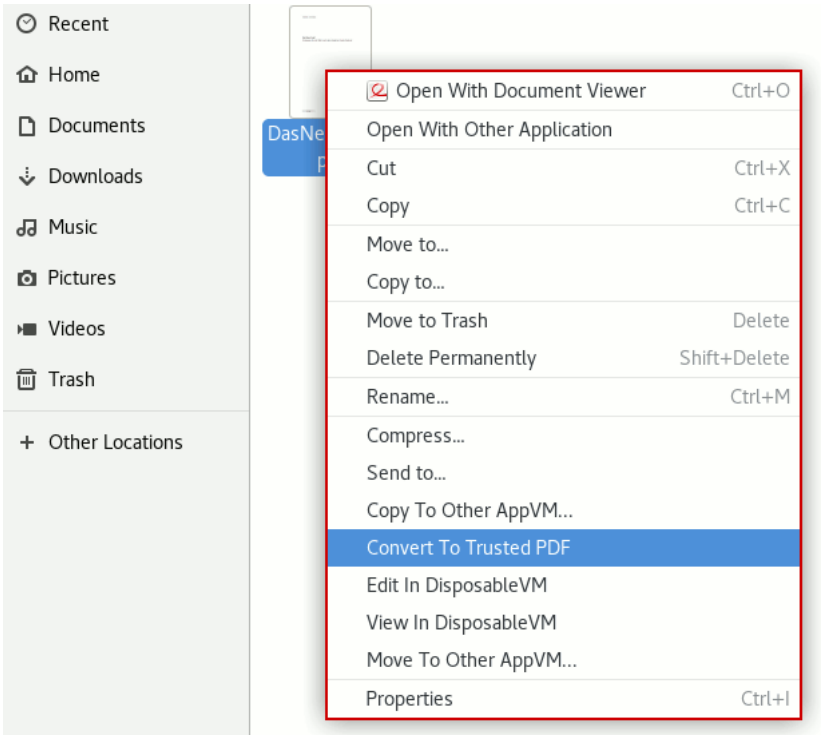


Abbildung 4.21: Konvertierung von PDFs im Dateimanager in QubesOS

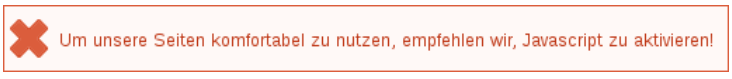
4.15 JavaScript (Sicherheit)

JavaScript ist eine der Kerntechniken des Internet. Der große Funktionsumfang wird aber auch für das Tracking missbraucht und enthält einige Sicherheitsrisiken. Bösartiger JavaScript-Code kann aktiv Sicherheitslücken im Browser ausnutzen und den Rechner kompromittieren.

- Im Januar 2013 lieferten die Server des Werbenetzwerkes OpenX bösartige Scripte aus, die den Rechner über Sicherheitslücken im Internet Explorer kompromittierten.
- Die bisher bekannten Exploits von NSA/FBI gegen den TorBrowser nutzten JavaScript.
- Bösartiger JavaScript-Code kann sich auch gegen Dritte richten, ohne dass der Nutzer es bemerkt. Chinas *Great Cannon* injiziert JavaScript-Code beim Aufruf chinesischer Webseiten, um die PCs der Nutzer als Botnet für DDoS-Attacken zu nutzen.[62]

Prinzip Whitelisting mit NoScript

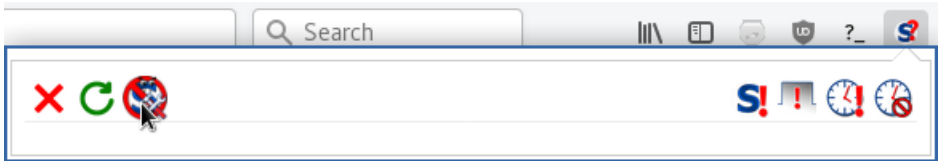
Für hohe Sicherheitsanforderungen kann man ein Whitelisting umsetzen, welches JavaScript für vertrauenswürdige Websites zur Erreichung der vollen Funktionalität erlaubt, im allgemeinen jedoch deaktiviert. Gute Webdesigner weisen den Nutzer darauf hin, dass ohne JavaScript eine Einschränkung der Funktionalität zu erwarten ist.



[62] https://citizenlab.org/2015/04/chinas-great-cannon/

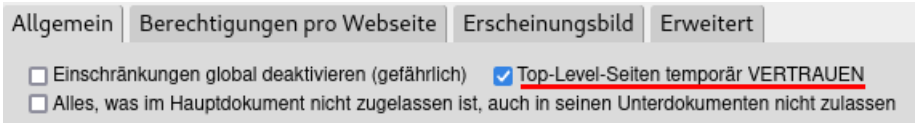
Mit dem Add-on NoScript kann man nicht nur Einstellungen für JavaScript verwalten, sondern auch für iFrames, Fonts, WebGL u. a. Bei der Verwendung von NoScript kann es zu frustrierenden Einschränkungen des Surferlebnisses kommen. Daher ist dieses Add-on dann empfehlenswert, wenn man besondere Anforderungen an die Sicherheit hat.

Nach der Installation kann man die Einstellungen von NoScript anpassen. Dafür klickt man auf das NoScript-Symbol in der Toolbar und dann auf das NoScript-Symbol im Menü.



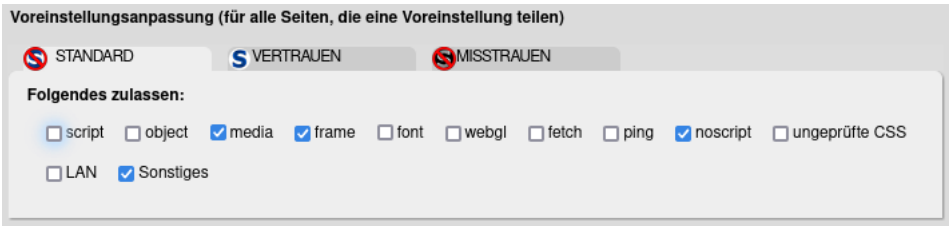
Für eine Erstkonfiguration steht ein Vorschlag vom PrHdb-Team zum Download zur Verfügung, den man in den Einstellungen von NoScript importieren kann.

Da das moderne Web ohne JavaScript kaum benutzbar ist, kann man in den globalen Einstellungen die aktuelle Top-Level-Seite immer temporär als vertrauenswürdig definieren. (Diese temporären Freigaben werden allerdings nicht mit dem Verlassen der Webseite gelöscht, sondern bleiben bis zum Löschen aller temporären Freigaben oder bis zum Neustart des Browsers bestehen.)



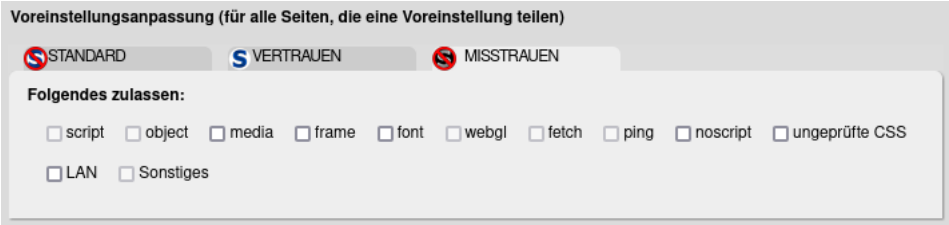
Auf dem Reiter *Allgemein* findet man auch die Einstellungen für drei Kategorien:

1. Standardmäßig muss man nur Bilder und Mediendateien zulassen. iFrames werden mit uBlock Origin blockiert, da sollte sich NoScript nicht einmischen. Zugriff auf lokale Adressen im LAN könnte man auch immer zulassen, wenn das Add-on JShelter mit Network Boundary Shield verwendet wird.



2. Vertrauenswürdige Webseiten dürfen zusätzlich JavaScript ausführen und Schriftarten nachladen, was aber mit der moderaten user.js auf Symbole beschränkt wird.

3. Als *Untrusted* definierte Webseiten dürfen gar nichts.



Auf dem Reiter *Per-site Permissions* kann man die Freigaben für einzelne Webseiten verwalten. NoScript bringt eine Menge Freigaben standardmäßig mit, die man ausmisten kann. Ein grünes Schloss bedeutet in den *Per-site Permissions*, dass die Freigabe nur für HTTPS gilt (sicherer). Wenn die Freigabe auch für unverschlüsseltes HTTP gilt, dann wird ein rotes Schloss angezeigt. Mit einem Klick auf das Schloss kann man die Berechtigung umschalten.

Scripte von Drittseiten

Es kann vorkommen, dass man für zusätzliche Domains Freigaben konfigurieren muss, damit eine Webseite korrekt funktioniert. Insbesondere bei Videoportalen tritt es häufig auf, dass Drittseiten zusätzliche Freigaben verlangen. Wenn man auf das NoScript-Symbol klickt, sieht man, welche Freigaben nötig sein könnten.

Bei der Entscheidung, welche Domains wirklich nötig sind und welche nur Trackingscripte laden, muss man raten. Scripte von *googletagmanager, ioam* oder *trafficjunkie* werden üblicherweise nur zum Spionieren verwendet und sind für die Funktionalität nicht notwendig.

Wenn man die Option *INDIVIDUELL* wählt, sieht man rot hinterlegt die angeforderten Freigaben und kann gleichzeitig festlegen, dass sie nur auf diesen Webseiten gelten sollen. Abb. 4.22 zeigt ein Beispiel für die Freigaben, die für das Videoportal Netflix.com nötig sind und nur für diese Webseite gelten sollen.

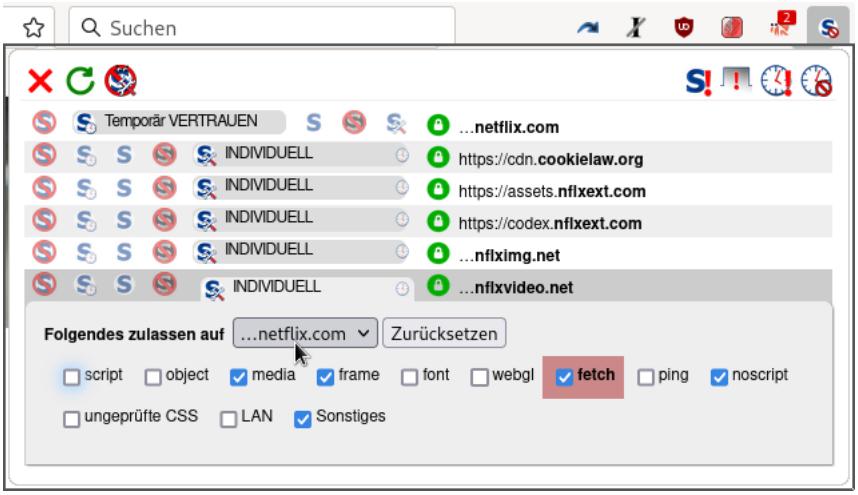


Abbildung 4.22: Individuelle Freigaben in NoScript für Netflix.com konfigurieren

Ein paar kleine Hinweise zu Scripten von Drittanbietern (natürlich unvollständig):

Captchas: Einige Webseiten verwenden Captchas von Drittanbietern als Spamschutz. Die Captchas funktionieren nur, wenn JavaScript für den Captcha-Provider freigegeben wird. Wenn das Captcha auf einer Webseite nicht funktioniert, kann man in der Liste nachschauen, ob evtl. ein Captcha-Provider dabei ist, und diese temporär freigeben.

- Für das häufig verwendete Google Captcha muss man JavaScript temporär für *google.com* und *gstatic.com* freigeben.

Videos: In der Regel muss JavaScript für einige Drittseiten freigegeben werden. Dabei handelt es sich in der Regel um Content Delivery Networks (CDN) des Dienstes, die man häufig an der Zeichenfolge *. . . cdn . . .* im Dateinamen erkennen kann.

- Um YouTube-Videos sehen zu können, muss man JavaScript für *youtube.com, youtube-nocookie.com, ytimg.com* und *googlevideo.com* freigeben. Da viele Webseiten YouTube-Videos einbinden, kann man diese Freigaben dauerhaft speichern.
- Um Vimeo-Videos abzuspielen, muss man JavaScript für *vimeo.com* und *vimeocdn.com* freigeben.
- Für Youporn-Videos muss man JavaScript für *youporn.com* und zusätzlich für *ypncdn.com* sowie *phncdn.com* (temporär) freigeben. *trafficjunkie.com* ist der Trackingdienst, der auf (fast) allen großen Pornoseiten verwendet wird.
- . . .

JIT-Compiler

Just-In-Time-Compiler sollen die Ausführung von JavaScript beschleunigen. Der JavaScript-Code wird dabei nicht Anweisung für Anweisung interpretiert, sondern vor der Ausführung durch einen Compiler gejagt, der verschiedene Optimierungen vornimmt. Diese zusätzliche Komplexität schafft auch zusätzliche Fehlerquellen. Es gab bereits mehrere sicherheitskritische Bugs in den JIT-Compilern von von Firefox, beispielsweise Bug #1607443.[63]

iSEC Partners empfiehlt deshalb in einem Sicherheitsaudit für den Tor-Browser, die JIT-Compiler für hohe Sicherheitsanforderungen (strenge Einstellungen) zu deaktivieren:

```
javascript.options.ion           = false
javascript.options.baselinejit   = false
javascript.options.native_regexp = false
```

Diese Einstellungen können die Performance einiger Webseiten deutlich verringern.

4.16 HTTPS-Verschlüsselung erzwingen und härten

Viele Websites bieten inzwischen HTTPS-Verschlüsselung an. Diese sichere Datenübertragung wird häufig nicht genutzt, obwohl es möglich wäre. Mit wenig Aufwand lässt sich die Nutzung von HTTPS für Websites erzwingen, die diese Option anbieten.

Oft gibt man aus Faulheit in der URL-Leiste des Browsers nur *www.privacy-handbuch.de* ein oder noch einfacher *privacy-handbuch.de*. Daraufhin sendet der Browser einen einfachen HTTP-Request an den Webserver. Gut konfigurierte Webserver antworten mit einem 301-Status und schicken den Surfer auf die HTTPS-verschlüsselte Webseite, aber das ist nicht immer der Fall. Außerdem ist der unverschlüsselte Response manipulierbar.

[63] https://www.heise.de/security/meldung/Jetzt-patchen-Angreifer-attackieren-Firefox-4630850.html

- Mit dem **HTTPS-First-Mode** kann man das Standardverhalten ändern. Wenn man diesen Mode aktiviert, wird Firefox bei Eingabe einer verkürzten URL ohne https:// am Anfang zuerst die HTTPS-Seite probieren und bei einem Fehler automatisch auf die HTTP-Version wechseln. Das ist ein bisschen sicherer.

  Den HTTPS-First-Mode aktiviert man unter *about:config* mit folgender Einstellung:

  ```
  dom.security.https_first = true
  ```

- Der **Nur-HTTPS-Modus** (https-only-mode) ist konsequenter. Wenn er aktiviert ist, wird Firefox immer HTTPS verwenden und einen Fehler anzeigen, wenn das nicht möglich ist. Auf der Seite mit der Warnung man kann mit einem Klick die unverschlüsselte HTTP-Seite aufrufen, wenn man es unbedingt will (Abb. 4.24).

  Den HTTPS-Only-Mode kann man in den grafischen Einstellungen in der Sektion *Datenschutz und Sicherheit* aktivieren (Abb. 4.23).

  Alternativ kann man unter *about:config* folgenden Wert setzen:

  ```
  dom.security.https_only_mode = true
  ```

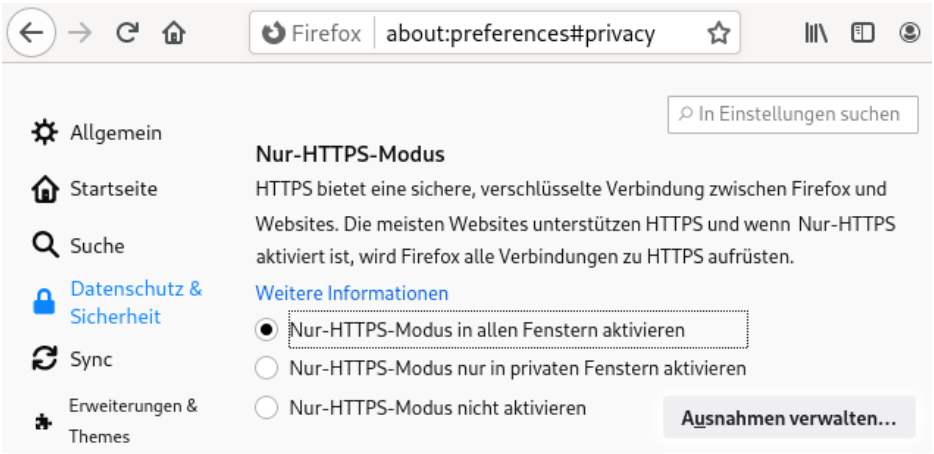


Abbildung 4.23: Nur-HTTPS-Mode in Firefox aktivieren

Damit die Ausnahmen beim Beenden des Browsers nicht gelöscht werden, ist sicherzustellen, dass folgender Wert unter *about:config* gesetzt ist:

```
privacy.clearOnShutdown.siteSettings = false
```

Außerdem kann man Ausnahmen für Webseiten definieren, für die kein HTTPS erzwungen werden soll. Die Konfiguration des Routers ist somit problemlos möglich.

- Für lokale Verbindungen zum eigenen Rechner wird kein HTTPS erzwungen. Man kann z. B. den Druckserver CUPS (Linux) wie gewohnt im Browser administrieren.

  Wenn man auch für http://localhost oder http://127.0.0.1 ein Upgrade auf HTTPS erzwingen möchte, könnte man folgenden Wert setzen (aber warum?):

  ```
  dom.security.https_only_mode.upgrade_local = true
  ```

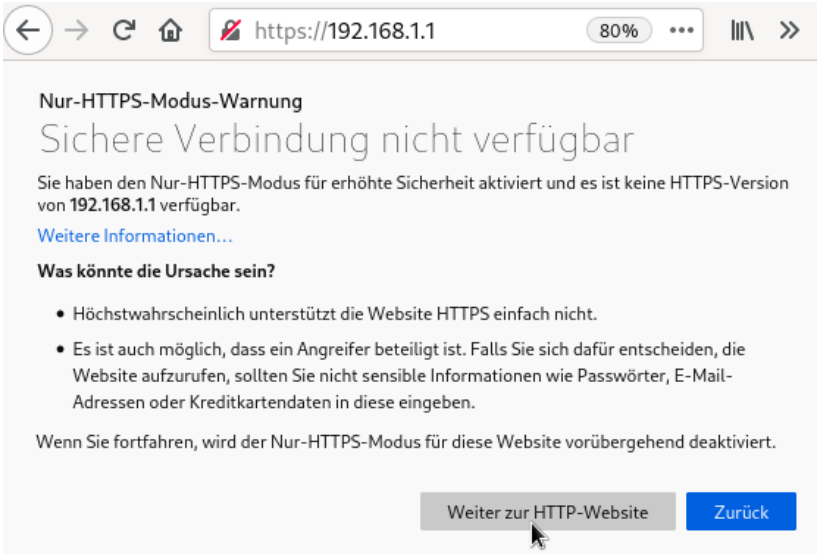


Abbildung 4.24: Warnung bei Aufruf einer unverschlüsselten HTTP-Seite

- *Mixed Content* nennt man die Elemente in HTTPS-Webseiten, welche über einen unverschlüsselten HTTP-Link geladen werden. Mit folgender Option erzwingt das Upgrade auf HTTPS auch für alle Inhalte der Webseite wie Bilder, Fonts, usw.:

  ```
  security.mixed_content.upgrade_display_content = true
  ```

  Das Laden von aktiven Inhalten wie JavaScript via unverschlüsseltem HTTP ist beim Aufruf von Webseiten via HTTPS standardmäßig verboten.

- *Insecure Renegotiation* wird seit 2009 als schwerwiegender Bug des SSL-Protokolls eingestuft. Tools zum Ausnutzen der Insecure Renegotiation gibt es auch als OpenSource (z. B. dsniff). Deshalb sollte man es verbieten:

  ```
  security.ssl.require_safe_negotiation             = true
  security.ssl.treat_unsafe_negotiation_as_broken   = true
  ```

- *Certifikate Pinning* schützt gegen Man-in-the-Middle-Angriffe. Mit folgender Option wird für populäre Webseiten wie Google, YouTube, Twitter, TorProject, Dropbox u. a. eine TLS-verschlüsselte Verbindung nur dann akzeptiert, wenn das Zertifikat des Servers von einer CA signiert wurde, die im Code von Firefox festgeschrieben ist:

  ```
  security.cert_pinning.enforcement_level = 2
  ```

  Wenn einige Webseiten mit dieser Einstellung nicht aufrufbar sind, dann sitzt ein Man-in-the-Middle in der TLS-Verschlüsselung (das kann z. B. ein Virenscanner sein).

- *Enterprise Root Certificates* werden bei Firefox die Root-Zertifikate des Betriebssystems genannt. Es gibt unter Umständen Gründe, warum Firefox diese Root-Zertifikate zusätzlich zur Validierung von HTTPS-Verbindungen nutzen sollte. In Firmen ist es bspw. oft üblich, eigene Root-Zertifikate für interne Webseiten und HTTPS-Proxy-Server zu verteilen. Wenn

Virenscanner als MitM den HTTPS-Traffic scannen wollen, nutzen sie ebenfalls oft diesen Weg.

Es gibt einige Gründe, die dagegen sprechen, diese Zertifikate zu nutzen und nur dem Zertifikatsspeicher von Firefox zu vertrauen. Man steuert das Verhalten mit:

```
security.enterprise_roots.enabled = false (Default)
```

Wenn bei einer HTTPS-Verbindung der Zertifikatsfehler *CertError: Man-in-the-Middle* auftritt, aktiviert Firefox automatisch die *Enterprise Root Certificates* und versucht erneut, das fehlerhafte Zertifikat zu validieren. Diese automatische Aktivierung verhindert man mit folgender Einstellung unter *about:config*:

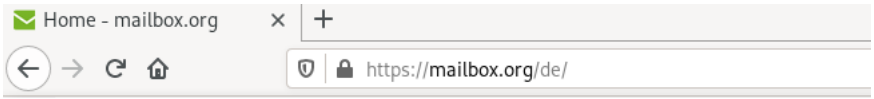
```
security.certerrors.mitm.auto_enable_enterprise_roots = false
```

Bei Bedarf kann man die Verwendung von Enterprise Root Certificates, die im Betriebssystem installiert wurden, selbst aktivieren (z. B. in Firmenumgebungen).

- Weitere Add-ons wie **HTTPSEverywhere** oder **HTTPZ** sind damit überflüssig.

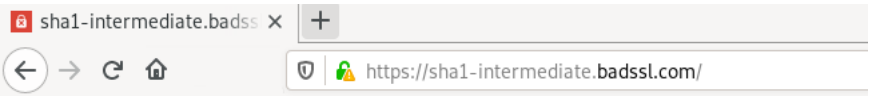
4.16.1 Anzeige der HTTPS-Verschlüsselung

Standardmäßig zeigt Firefox 70+ einen HTTPS-verschlüsselten Transport der Daten mit einem kleinen, unscheinbar grauen Icon neben der Adresse an:



Neben einfachen SSL-Zertifikaten gibt es *Extended Validation Certificates*, bei denen die Certification Authority (CA) die Identität des Inhabers aufwendiger prüft, bevor ein Zertifikat ausgestellt wird. Diese Zertifikate verlieren an Bedeutung und werden immer seltener verwendet. Man kann sich in Firefox diese erweiterte Validierung anzeigen lassen, indem man auf das Verschlüsselungssymbol klickt:

Auf der Webseite https://badssl.com kann man sich anschauen, wie Firefox bei Problemen in der HTTPS-Verschlüsselung reagiert. Wenn man eine unsichere Verschlüsselung akzeptiert hat, zeigt Firefox ein kleines, gelbes Warndreieck neben dem Schloss-Symbol. Diese Warnung sollte man nicht ignorieren:



Außerdem kann man sich anzeigen lassen, wenn die Verbindung zum Webserver nicht verschlüsselt ist. Für ein Warn-Icon aktiviert man unter *about:config* folgende Optionen:

```
security.insecure_connection_icon.enabled          = true
security.insecure_connection_icon.pbmode.enabled   = true
```

Die Anzeige eines Warn-Textes neben der URL aktiviert man mit:

```
security.insecure_connection_text.enabled          = true
security.insecure_connection_text.pbmode.enabled   = true
```

Beide Optionen können auch kombiniert werden, das sieht dann so aus:

4.16.2 Vertrauenswürdigkeit von HTTPS

IT-Sicherheitsforscher der EFF kamen bereits 2009 in einer wissenschaftlichen Arbeit zu dem Schluss, dass Geheimdienste mit gültigen SSL-Zertifikaten schwer erkennbare Man-in-the-Middle-Angriffe durchführen können. Diese Angriffe können routiniert ausgeführt werden.[64]

> *Certificate-based attacks are a concern all over the world, including in the U.S., since governments everywhere are eagerly adopting spying technology to eavesdrop on the public. Vendors of this technology seem to suggest the attacks can be done routinely.*

Anbieter von fertigen Appliances für diesen auch als *Lawful SSL Interception* bezeichneten Angriff findet man beim Stöbern in den SpyFiles von Wikileaks. Auf der Messe für Überwachungstechnik ISS World im März 2015 wurden im *Track 4: Encrypted Traffic Monitoring and IT Intrusion* die neuesten Techniken zu SSL-Interception- und TLS-Downgrade-Angriffen präsentiert. Anhänger der Open-Source-Bewegung können mit *mitm-proxy*[65] oder *dsniff*[66] Man-in-the-Middle-Angriffe mit gefälschten Zertifikaten durchführen. Man braucht nur passende Zertifikate.

Für staatliche Schnüffler gibt es mehrere Möglichkeiten, um diese Technik mit gültigen SSL-Zertifikaten für schwer erkennbare Man-in-the-Middle-Angriffen zu kombinieren:

1. Für einen großflächigen Angriff gegen iranische Internet-Nutzer wurden im August 2011 mehrere CAs gehackt, um gültige SSL-Zertifikate zu erstellen (DigiNotar, Comodo, InstantSSL und zwei Sub-Registrare von Comodo). Bei DigiNotar wurden 531 Zertifikate kompromittiert. Neben den Webseiten von Google, Yahoo, Mozilla, Skype, TorProject.org u. a. waren auch die Webdienste von MI6, CIA und Mossad betroffen.

[64] https://eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl
[65] http://crypto.stanford.edu/ssl-mitm/
[66] http://www.monkey.org/~dugsong/dsniff/

2. Certification Authorities könnten unter Druck gesetzt werden, um staatlichen Stellen SubCA-Zertifikate auszustellen, mit denen die Zertifikate für Man-in-the-Middle-Angriffe signiert werden könnten. Ein Kommentar zum TürkTRUST-Desaster:

   > *I think you will see more and more events like this, where a CA under pressure from a government will behave in strange ways. (A. Shamir)*

   Im Juni 2014 signierte die staatliche indische Certification Authority (NIC) gefälschte SSL-Zertifikate für Google-Dienste und Yahoo!. 45 gefakte Zertifikate wurden nachgewiesen. Ob es sich um eine staatliche Überwachung, einen Hackerangriff oder einen Konfigurationsfehler(?) handelte, ist unklar.[67]

3. Die Anbieter von Webdiensten können zur Herausgabe von Zertifikaten und Keys gezwungen werden, wie am Beispiel des E-Mail-Providers Lavabit bekannt wurde. Die betroffenen Provider sind zum Stillschweigen verpflichtet. Der Angreifer kann mit diesen Zertifikaten einen Angriff auf die SSL-Verschlüsselung durchführen, der nicht mehr erkennbar ist.

4. Verisign ist nicht nur die größte Certification Authority. Die Abteilung NetDiscovery von Verisign ist ein Global Player in der Überwachungstechnik und unterstützt die Behörden und westliche Geheimdienste seit 2002 bei der SSL-Interception.

5. Mit der **eIDAS-Verordnung** will die EU den Rahmen *standardisierten Vertrauensdiensten* schaffen. Dazu zählen neben elektronische Signatur (QES) auch qualifizierte TLS-Zertifikate (QWACs). Ursprünglich war der Plan, dass Browserhersteller gezwungen werden, diese europäischen Certification Authorithies (CAs) ungeprüft zu übernehmen, da die Regulatorien der EU dafür sorgen würden, dass staatliche eIDAS CAs vertrauenswürdig sind.

   Befürchtungen, dass diese Root-Zertifikate für die Überwachung genutzt werden könnten und die Sicherheit von TLS gefährden, sind völlig unbegründet, schreibt die Bundesdruckerei (ohne weitere Begründung). Sicherheitsexperten sehen das anders und warnen vor den staatlich kontrollierten Certification Authorities, die eine Überwachung im Internet erleichtern würden.[68]

   Im eIDAS Dashbord der EU findet man die Listen[69] der *qualifizierten Vertrauensdiensten* aller EU-Länder und in der deutschen Liste finde man die Utimaco GmbH als vertrauenswürder Vertrauensdienst. Die Utimaco GmbH ist ein Hersteller von Überwachungstechnik und bietet auch Technik für TLS Interception. Wäre doch praktisch, wenn...

Kriminelle Subjekte haben ebenfalls nachgewiesen, dass sie für Man-in-the-Middle-Angriffe auf die SSL-Verschlüsselung gültige Zertifikate verwenden können:

- Beim Angriff auf das Forum Bitcointalk (2013) konnten Angreifer die Kontrolle über die Domain erlangen und sich dann Domain-validierte echte Zertifikate ausstellen.[70]
- Bei einem weiteren Angriff auf Bitcoinbörsen (2022) konnten Angreifer die BGP-Routen umlenken. Damit wurde die automatische Verifizierung der Domain-Validierung bei den CAs getäuscht.

[67] https://www.heise.de/-2255992
[68] https://eidas-open-letter.org
[69] https://eidas.ec.europa.eu/efda/tl-browser/
[70] https://www.heise.de/-2058883

- Wenn Administratoren schlampig arbeiten und die E-Mail-Adressen ssladministrator@domain.tld, webmaster@domain.tld, postmaster@domain.tld oder ssladmin@domain.tld nicht schützen, kann ein Angreifer sich E-Mail-verifizierte SSL-Zertifikate ausstellen lassen, wie bereits demonstriert wurde. Eine unverschlüsselte E-Mail mit einem Verification Link an eine dieser E-Mail-Adressen ist oft die einzige Prüfung auf Rechtmäßigkeit durch die CAs.

4.16.3 SSL-Zertifikate via OCSP validieren

Das Online Certificate Status Protocol (OCSP) sollte eine Überprüfung der SSL-Zertifikate ermöglichen. Bevor der Browser eine SSL-Verbindung akzeptiert, fragt er bei der Certification Authority nach, ob das verwendete Zertifikat für diesen Server noch gültig ist. Um SSL-Zertifikate via OCSP zu verifizieren, wurden zwei Verfahren definiert:

OCSP-Server sind eine veraltete Technik und leicht auszutricksen, wie Moxie Marlinspike in dem Paper *Defeating OCSP With The Character 3* (2009) gezeigt hat. Gängige Tools für Man-in-the-Middle-Angriffe wie *sslsniff*[71] können das automatisiert ausführen. Die Validierung via OCSP-Server bringt kaum Sicherheitsgewinn.[72]

Einige CAs nutzen die OCSP-Anfragen zum Tracking des Surfers mit Cookies, wie der folgende Mitschnitt eines OCSP-Request zeigt:

```
POST http://ocsp2.globalsign.com/gsorganizationvalg2 HTTP/1.1
Host: ocsp2.globalsign.com
User-Agent: Mozilla/5.0 (...) Gecko/20130626 Firefox/17.0
↪  Iceweasel/17.0.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
Content-Length: 117
Content-Type: application/ocsp-request
Cookie: __cfduid=57a288498324f76b1d1373918358
```

Auch wenn aktuelle Firefox-Versionen keine Cookies von OCSP.Get-Antworten mehr akzeptieren, erhält die Certification Authority (CA) laufend Informationen, von welcher IP-Adresse die SSL-geschützten Webseiten bzw. Mailserver o. Ä. kontaktiert wurden. Da die OCSP-Anfragen und -Antworten unverschlüsselt übertragen werden, kann auch ein *Lauscher am Draht* diese Informationen abgreifen. Aus Datenschutzgründen kann man die Validierung via OCSP-Server deaktivieren

```
security.OCSP.enabled = 0
```

Wenn man die Validierung von SSL-Zertifikaten via OCSP-Server als Sicherheitsfeature nutzen möchte (damit beispielsweise Extended-Validation-Informationen der Zertifikate angezeigt werden), dann muss man auch darauf bestehen, dass das Ergebnis geliefert und ausgewertet wird. Anderenfalls ist es als Sicherheitsfeature unbrauchbar. Diese verschärfte OCSP-Validierung aktiviert man unter *about:config* mit:

[71] https://moxie.org/software/sslsniff/
[72] https://www.thoughtcrime.org/papers/ocsp-attack.pdf

```
security.OCSP.enabled = 1
security.OCSP.require = true
```

Da es keine klare Empfehlung für eine Abschaltung oder verschärfte Durchsetzung von OCSP gibt, enthält unsere user.js-Konfiguration in der Zusammenfassung keine Vorgaben. Der Anwender möge selbst entscheiden. Die Standardeinstellung von Firefox mit aktiviertem OCSP aber ohne eine Auswertung zu erzwingen, vereint die Nachteile beider Varianten.

OCSP.Stapling ist ein modernes Verfahren, dass die o. g. Probleme vermeidet. Der Browser ruft ein Token vom Webserver ab, das die Gültigkeit des Zertifikates für einen kurzen Zeitraum bestätigt und von der CA signiert wurde.

Moderne Webserver und alle aktuellen Browser unterstützen es inzwischen. Bei dem bekannten Test für Webserver *Qualsys SSL Labs* wird ab Januar 2017 die Bestnote A+ nur vergeben, wenn der Webserver OCSP.Stapling anbietet. Die BSI-Richtlinie TR-03116-4 (Kryptografische Vorgaben für TLS, S/MIME, OpenPGP und SAML) fordert ebenfalls Support für OCSP.Stapling.

Firefox ist sinnvoll vorkonfiguriert. Es wird standardmäßig OCSP.Stapling genutzt, wie man unter *about:config* überprüfen kann:

```
security.ssl.enable_ocsp_stapling      = true
security.ssl.enable_ocsp_must_staple  = true
```

4.16.4 Tracking via TLS-Session

Beim Aufbau einer verschlüsselten HTTPS-Verbindung zwischen Browser und Webserver wird eine sogenannte TLS-Session initialisiert. Diese Session kann für 48 Stunden genutzt werden. Das beschleunigt das Laden der Webseite bei erneutem Zugriff, da die Details der Verschlüsselung nicht jedes mal neu zwischen Browser und Webserver ausgehandelt werden müssen. Da die TLS-Session eindeutig ist, kann sie für das Tracking genutzt werden (RFC 5077).[73]

Die TLS-Session-ID kann von nahezu allen Webservern für das Tracking der Zugriffe genutzt werden. IBM WebSphere, Apache und andere bieten eine API für den Zugriff auf die SSL-Session-ID. Einige Webshops sind für das Tracking via SSL-Session-ID vorbereitet (z. B. die *xtcModified eCommerce Shopsoftware*[74]). Dieses Trackingverfahren ist so gut wie nicht nachweisbar, da es vollständig durch den Webserver realisiert wird und keine Spuren im Browser hinterlässt.

Aktuelle Firefox Browser können sich dagegen schützen.

- Die in Firefox standardmäßig aktivierte *Netzwerk-Partitionierung* isoliert die TLS-Sessions in Containern und verhindert das Website-übergreifende Tracking beim Surfen.
- Löschen von Cache und Sessions beim Schließen des Browsers verhindert das Tracking über einen längeren Zeitraum.

4.16.5 Tracking via HTTP Strict Transport Security

HTTP Strict Transport Security (HSTS) wurde als Schutz gegen den *ssl-stripe*-Angriff eingeführt, den Moxie Marlinspike auf der Black Hack 2009 vorstellte. Der Angriff wurde beispielsweise 2012 von mehreren Tor-Bad-Exit-Nodes aktiv genutzt.

[73] https://tools.ietf.org/html/rfc5077
[74] http://www.modified-shop.org/wiki/SESSION_CHECK_SSL_SESSION_ID

Als Schutz gegen *ssl-stripe*-Angriffe sendet der Webserver beim Aufruf einer Webseite einen zusätzlichen HSTS-Header, um dem Browser mitzuteilen, dass diese Website für eine bestimmte Zeit immer via HTTPS aufgerufen werden soll. Außerdem enthält Firefox die *HSTS Preload List* mit mehr als 1.000 Webseiten, die nur via HTTPS aufgerufen werden dürfen. Das verhindert einen Downgrade auf unverschlüsselte HTTP-Verbindungen.

S. Greenhalgh hat ein Verfahren publiziert, wie man HSTS für das Tracking von Surfern verwenden kann.[75] Entwickler bei Apple haben im März 2018 beobachtet, dass dieses Verfahren in-the-wild eingesetzt wird, veröffentlichten aber keine Details. Sie schlagen eine Modifikation des Standards vor, um Tracking via HSTS-Cookies zu verhindern.[76]

Mit dem Nur-HTTPS-Modus von Firefox ist man gegen dieses exotische Tracking geschützt.

4.16.6 Tracking-Risiko durch seltsame Auswahl der SSL/TLS-Cipher

Wenn der Browser eine SSL-verschlüsselte Verbindung zu einem Webserver aufbauen will, dann sendet er eine Liste der unterstützten TLS-Features, Cipher und der nutzbaren elliptischen Kurven für EC-Crypto. Die Reihenfolge und der Inhalt der Listen ist unterschiedlich für verschiedene Browser und Browser-Versionen.

- Firefox 53 sendet beispielsweise:

```
<e name='Firefox/53.0' protocol='771' extTypes='21 23 65281 10 11 16 5
↪  18 40 43 13'
suites='4865 4867 4866 49195 49199 52393 52392 49196 49200 49171 49172
↪  51 53'
curves='29 23 24 25 256 257' points='AA==' compress='AA=='/>
```

- Google Chrome sendet:

```
<e name='Chrome/57.0.2951.0' protocol='771' greateExt='1'
↪  extTypes='65281 0 23 35 13 5 18 16 30032 11 40 45 43 10 21'
↪  greaseSuite='1'
suites='4865 4866 4867 49195 49199 49196 49200 52393 52392 52244 52243
↪  49171 49172 156 157 47 53 10' greaseCurves='1' curves='29 23 24'
↪  points='AA==' compress='AA=='/>
```

Das sieht etwas kryptisch aus, man kann sich auf verschiedenen Webseiten aber auch anzeigen lassen, was es bedeutet.

Wenn man an den TLS-Ciphern rumspielt und schwache Cipher wie AES-CBC-SHA deaktiviert, kreiert man möglicherweise ein individuelles Erkennungsmerkmal, anhand dessen man beim Aufruf einer verschlüsselten Webseite wiedererkennbar ist. Deshalb ist es keine gute Empfehlung, an den Einstellungen für Cipher rumzuspielen. Es ist besser, einen aktuellen Firefox bzw. Firefox ESR zu verwenden und es bei den Einstellungen der Entwickler der NSS Crypto Lib zu belassen.

[75] http://heise.de/-2511258
[76] https://heise.de/-3998754

4.17 WebRTC mit Firefox

WebRTC wurde von Google und Mozilla initiiert und später vom W3C standardisiert, um der Konkurrenz von Microsoft Skype etwas entgegenzusetzen. Google und Mozilla entschieden sich dafür, die Funktionalität in die Browser zu integrieren, um sie als universelle Anwendungen für jegliche Internetkommunikation auszubauen.

Neben der Internettelefonie wird WebRTC auch auch bei Browser-basierten Videokonferenzsystemen wie Jitsi Meet eingesetzt. Bei der direkten Eins-zu-eins-Kommunikation ist für den Datenstrom eine Ende-zu-Ende-Verschlüsselung vorgesehen. Bei Konferenzsystemen ist es häufig so, dass der Konferenzserver als Endpunkt agiert, die Daten entschlüsselt und für jeden Teilnehmer neu verschlüsselt. (Verbesserte Lösungen mit durchgehender Ende-zu-Ende-Verschlüsselung für Konferenzsysteme sind in der Entwicklung.)

OpenH264-Videocodecs

Um WebRTC mit Firefox zu verwenden, wird das OpenH264-Plug-in von Cisco benötigt, das die Videocodecs bereitstellt. Das Plug-in ist Closed-Source-Software und wird beim ersten Start von Firefox automatisch heruntergeladen und im Profilverzeichnis gespeichert.

Mit folgenden Einstellungen unter *about:config* wird das OpenH26-Plug-in aktiviert:

```
media.gmp-gmpopenh264.enabled          = true
media.gmp-gmpopenh264.autoupdate       = true
media.gmp-gmpopenh264.provider.enabled = true
```

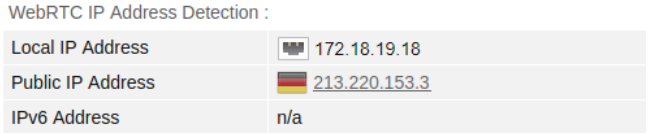
Bei einigen sicherheitsoptimierten Linux Distributionen wie RHEL oder Fedora ist das OpenH264 Plugin im Firefox standardmäßig deaktiviert und wird über die Paketverwaltung installiert:

```
> sudo dnf install mozilla-openh264
```

Internet Connectivity Establishment (ICE)

Bei WebRTC sollt der Datenstrom möglichst direkt zwischen den Teilnehmern fließen. Um eine direkte Verbindung zwischen den Clients aufzubauen, wird der ICE-Standard (Internet Connectivity Establishment) verwendet. ICE versucht im Hintergrund sehr aggressiv, die direkte Verbindung irgendwie herzustellen. Es werden Proxy-Einstellungen umgangen, via UPnP wird versucht, ein Loch in Router und Firewalls zu bohren, VPNs werden teilweise ausgetrickst usw. Dabei kommt ein STUN-Server zum Einsatz, der die verschiedenen Möglichkeiten ausprobiert. Wenn wirklich keine direkte Verbindung möglich ist, wird ein TURN-Server als Proxy für den Datenstrom verwendet.

Aufgrund dieser aggressiven Strategie zum Verbindungsaufbau können der Gegenseite folgende Informationen bekannt werden, wie der WebRTC-Test von Browserleaks[77] zeigt:



[77] https://browserleaks.com/webrtc

- Alle IP-Adressen und Interfaces des Rechners oder der VM im lokalen LAN.
  (Ein Angreifer oder Trackingservice könnte das verwenden, um mehrere Rechner innerhalb eines Firmennetzwerkes oder in einem Haushalt zu unterscheiden.)
- Die externe Adresse des Routers/Gateways zum Internet.
  (Diese Adresse sollte eigentlich geheim bleiben, wenn man einen Proxy wie Tor Onion Router oder ein VPN verwendet. Aber alle Proxys und einige VPN-Techniken können von ICE ausgetrickst werden und damit den Nutzer deanonymisieren.)
- Die externe Adresse des Proxy oder VPN-Endpunktes.
  (Diese Information lässt sich natürlich nicht geheim halten.)

Firefox bietet einige Möglichkeiten, die Datenschutzprobleme von ICE zu reduzieren:

1. Bei privater Nutzung kann man davon ausgehen, dass man innerhalb der Wohnung mündlich kommuniziert und nicht via WebRTC. Die internen Adressen aus dem LAN müssen nicht publiziert werden. Mit folgenden Optionen kann man dies abschalten:

   ```
   media.peerconnection.ice.default_address_only = true
   media.peerconnection.ice.no_host              = true
   ```

2. Wenn man verhindern möchte, dass die Gegenseite die externe IP-Adresse des Routers erfährt und damit Schlussfolgerungen über den Standort via Geolocation zieht, kann man direkte Verbindungen generell ausschließen und immer eine Verbindung über einen TURN-Proxy-Server erzwingen:

   ```
   media.peerconnection.ice.relay_only = true
   ```

3. Wenn man den STUN/TURN-Servern des Videokonferenzanbieters nicht vertraut, kann man eigene Server verwenden:

   ```
   media.peerconnection.use_document_iceservers = false
   ```

   Die eigenen Server muss man in der folgenden Variable definieren:

   ```
   media.peerconnection.default_iceservers = <Serverliste>
   ```

4. Wenn man WebRTC nur via VPN verwenden möchte, aber nicht, wenn man ohne VPN surft, dann kann man die zulässigen Netzwerkinterfaces definieren:

   ```
   media.peerconnection.ice.force_interface = tun1
   media.peerconnection.ice.no_host         = true
   ```

   Wenn das VPN nicht aktiviert wurde und damit das virtuelle VPN-Interface *tun1* nicht vorhanden ist, kann man ganz normal surfen, aber eine WebRTC-Verbindung wird nicht akzeptiert. Nur wenn das VPN aktiv ist, ist eine WebRTC-Verbindung möglich, deren Daten immer durch das VPN geschickt werden.

5. Ähnlich wie bei den VPNs kann man auch die Verwendung eines Proxy erzwingen und WebRTC nur via Proxy zulassen:

   ```
   media.peerconnection.ice.proxy_only = true
   ```

   In den meisten Fällen wird WebRTC mit dieser Einstellung nicht funktionieren, da HTTP- oder SOCKS-Proxys wie Tor Onion Router nicht UDP-fähig sind.

Media Device Enumeration

Um WebRTC nutzen zu können, muss Firefox wissen, welche Media-Input-Devices vorhanden sind, und nach Zustimmung durch den Nutzer Zugriff darauf erlangen können:

```
media.navigator.enabled       = true
media.navigator.video.enabled = true
```

Trackingdienste können die Media Device Enumeration von WebRTC ausnutzen, um Daten über Kamera und Mikrofon zu sammeln und sie für das Hardware-Fingerprinting zu verwenden. Der Surfer wird dabei nicht um Zustimmung für einen Zugriff auf Kamera oder Mikrofon gebeten. Der WebRTC-Test von Browserleaks demonstriert es:

Abbildung 4.25: Media Device Enumeration via WebRTC

Firefox verwendet als Device-IDs einen gesalzenen Hash. Der Salt für die Berechnung des Hashes wird beim ersten Start festgelegt und immer erneuert, wenn Cookies und Cache-Daten gelöscht werden. Außerdem ist der Salt in Surfcontainern unterschiedlich. Damit ist die Device-ID in gleicher Weise wie langlebige Cookies für das Tracking geeignet. Als Schutz gegen Tracking anhand der Device-IDs kann man deshalb die Empfehlungen für Cookies umsetzen.

Empfohlene Einstellungen für mehr Privatsphäre

Es wird häufig von anderen Projekten empfohlen, die Features Media Peerconnection (WebRTC) und Media Device Enumeration abzuschalten, um das Tracking zu erschweren. Da die Abschaltung dieser Javascript-APIs aber recht einfach von den Trackingdiensten registriert werden kann, schafft sie ein seltenes Merkmal für den Browser-Fingerprint und ist kontraproduktiv.

Unauffälliger ist es, das Auslesen der Multimedia-Devices (Mikrofon, Kamera) mit dem Add-on JS-Restrictor zu faken und das Auslesen der Host-IP-Adresse zu verhindern:

```
media.peerconnection.enabled                    = true
media.navigator.enabled                         = true
media.navigator.video.enabled                   = true
media.peerconnection.ice.default_address_only   = true
media.peerconnection.ice.no_host                = true
```

```
media.gmp-gmpopenh264.enabled          = false
media.gmp-gmpopenh264.autoupdate       = false
media.gmp-gmpopenh264.provider.enabled = false
media.gmp-gmpopenh264.visible          = false
```

4.18 DNS-over-HTTPS mit Firefox

DNS (Domain Name Service) ist das Telefonbuch des Internet. Es übersetzt lesbare URLs wie *www.privacy-handbuch.de* in die IP-Adresse des Servers, der diese Webseite zur Verfügung stellt. Eine ausführliche Anleitung zu diesem zentralen Internetdienst findet man im Kapitel Domain Name Service (DNS).

Firefox kann DNS-over-HTTPS nutzen, um die DNS-Daten beim Surfen zu verschlüsseln und eine Zensur durch die DNS-Server der Provider zu umgehen. Das Feature heißt TRR (Trusted Recursive Resolver). Die Konfiguration ist einfacher, als einen DNS-Daemon mit DNS-over-TLS-Support oder DNSCrypt zu installieren. Sie schützt allerdings nur den DNS-Datenverkehr beim Surfen mit Firefox, alle andere Anwendungen nicht.

Da DNS ein zentraler Dienst für alle Internet-Anwendungen ist, ist eine zentrale Konfiguration der DNS-Server sinnvoller als die Konfiguration einzelner Webbrowser.

Konfiguration von DNS-over-HTTPS in den Einstellungen

Unter *Einstellungen* → *Datenschutz & Sicherheit* kann man DNS-over-HTTPS aktivieren und man kann die Adresse des bevorzugten DoH Server eintragen (Abb. 4.26).

- Beim *Standardschutz* entscheidet Firefox, ob DNS-over-HTTPS verwendet wird oder nicht.
- Bei *erhöhtem Schutz* wird der DNS-over-HTTPS Server bevorzugt aber ohne Nachfrage umgeschaltet, wenn der DNS-over-HTTPS Server nicht erreichbar ist.
- Bei *maximalem Schutz* wird nur der DNS-over-HTTPS Server verwendet. Wenn der DNS-over-HTTPS Server nicht verfügtbar ist, wird eine Warnung angezeigt.

Einige DNS-over-HTTPS Server, die man als benutzerdefinierte Server verwenden kann:

- Freifunk München: https://doh.ffmuc.net
- Digitalen Gesellschaft (CH): https://dns.digitale-gesellschaft.ch/dns-query
- dnsforge.de (mit Ad-Filter): https://dnsforge.de/dns-query
- BlahDNS DE (mit Ads-Filter): https://doh-de.blahdns.com/dns-query
- BlahDNS FI (mit Ads-Filter): https://doh-fi.blahdns.com/dns-query
- Mullvad DNS (mit Ads-Filter): https://adblock.doh.mullvad.net/dns-query
- Mullvad DNS (ohne Ads-Filter): https://doh.mullvad.net/dns-query
- AdGuard (mit Ads-Filter): https://dns.adguard-dns.com/dns-query
- AdGuard (ohne Ads-Filter): https://unfiltered.adguard-dns.com/dns-query
- Njalla: https://dns.njal.la/dns-query
- Quad9-DNS-over-HTTPS-Server: https://dns.quad9.net/dns-query

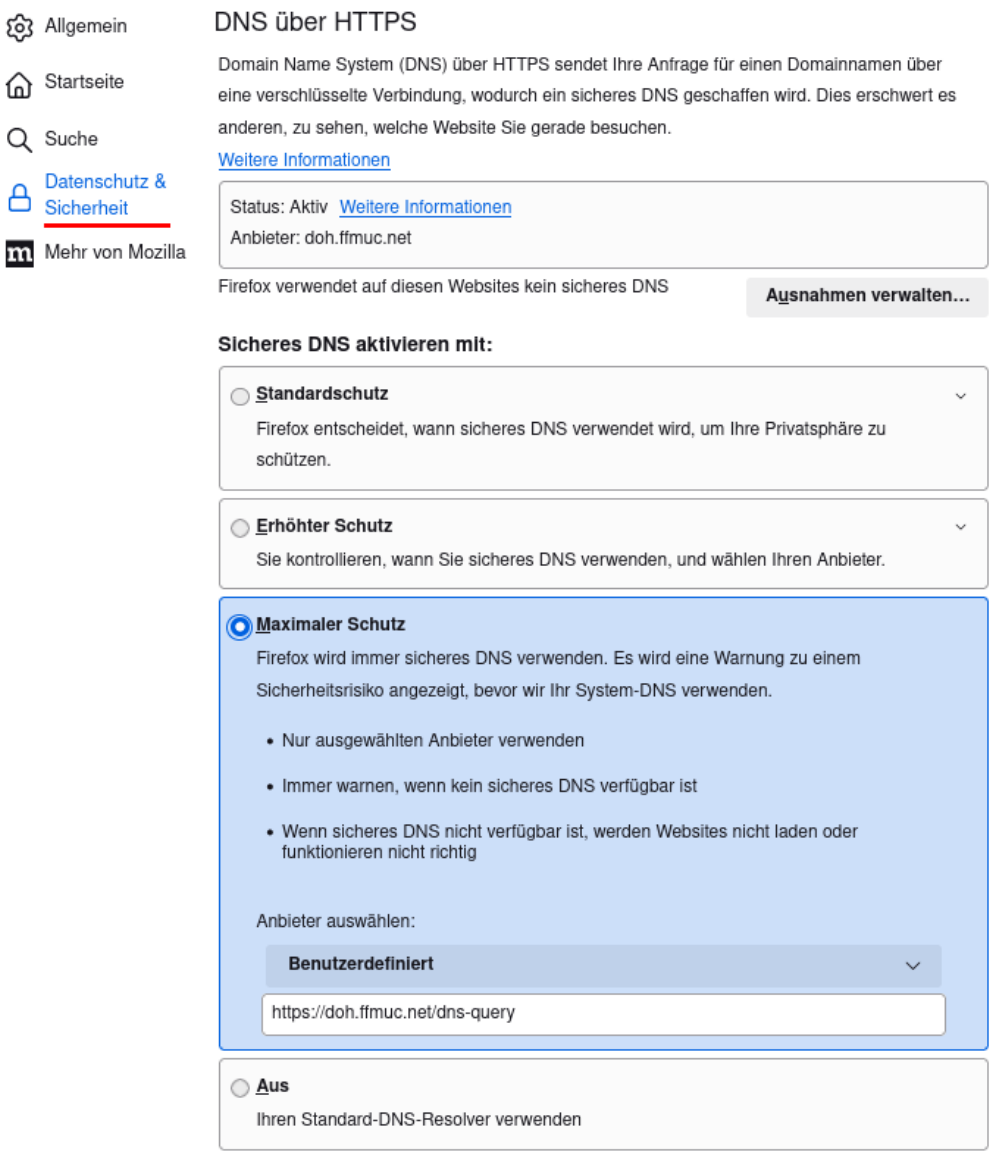


Abbildung 4.26: Konfiguration von DNS-over-HTTPS

Konfiguration für Experten

Mit folgenden Werten könnte man TRR in Firefox unter *about:config* konfigurieren:

- Mit dem TRR-Mode kann man auswählen, wie DNS-over-HTTPS verwendet wird:

```
network.trr.mode = 0 (Firefox bzw. Mozilla entscheidet, was verwendet
↪  wird.)

network.trr.mode = 1 (Frage System-DNS und TRR und verwende
↪  schnellstes Ergebnis.)

network.trr.mode = 2 (Verwende TRR und System-DNS nur als Fallback.)
```

```
network.trr.mode = 3 (Verwende ausschließlich TRR nach dem Start.)

network.trr.mode = 4 (TRR parallel zum System-DNS, aber nicht
↪ verwenden.)

network.trr.mode = 5 (Abgeschaltet durch den Nutzers.)
```

Firefox für Windows deaktiviert DNS-over-HTTPS unabhängig von den Einstellungen für network.trr.mode in folgenden Fällen: wenn ein VPN genutzt wird, wenn ein Proxy in den Windows-Systemeinstellungen konfiguriert wurde oder wenn mittels NRPT spezielle DNS-Server für einzelne Domains festgelegt wurden. Wenn man mit Firefox für Windows trotz VPN, Proxy oder NRPT einen DNS-over-HTTPS-Server verwenden möchte, muss man folgende Einstellungen aktivieren:

```
network.trr.enable_when_vpn_detected   = true
network.trr.enable_when_proxy_detected = true
network.trr.enable_when_nrpt_detected  = true
```

- Wenn man TRR-Mode 1–3 verwenden möchte, dann muss man die zwingend notwendige Validierung von SSL-Zertifikaten via OCSP-Server abschalten. Ansonsten beißt sich die Katze in den Schwanz. Firefox will das SSL-Zertifikat des DNS-over-HTTPS-Servers prüfen und braucht dafür die IP-Adresse des OCSP-Servers vom DNS-over-HTTPS-Server. Deshalb entweder OCSP komplett deaktivieren:

  ```
  security.OCSP.enabled = 0
  ```

  Oder nicht zwingend auf einer OCSP-Antwort bestehen:

  ```
  security.OCSP.required = false
  ```

- Die URL des DNS-over-HTTPS-Servers wird mit *network.trr.uri* angegeben, Beispiel:

  ```
  network.trr.uri = https://doh.ffmuc.net
  ```

  Die IP-Adresse des DoH-Servers wird beim Start zuerst mit dem System Resolver ermittelt. Danach wird der DoH-Server für die weiteren DNS-Anfragen verwendet.

  Wenn keine IP-Adresse für den konfigurierten DoH-Server gefunden wird, würde Firefox im TRR-Mode 2 weiter den System-DNS verwenden, ohne dass der Nutzer im TRR-Mode 2 etwas davon bemerkt (grafische Konfiguration). Zensierende DNS-Server könnten dieses Verhalten ausnutzen und die DNS-Namen der populären DoH-Server blockieren (zensieren), um eine Umgehung der Zensur mittels DNS-over-HTTPS zu blockieren. Um solche Angriffe zu verhindern, könnte man die IP-Adressen der DoH-Server in die *hosts* Datei eintragen(für Linuxer: */etc/hosts*):

  ```
  185.95.218.42 dns.digitale-gesellschaft.ch
  5.1.66.255 doh.ffmuc.net
  176.9.1.117 dnsforge.de
  193.19.108.3 adblock.doh.mullvad.net
  194.242.2.2 doh.mullvad.net
  94.140.14.14 dns.adguard-dns.com
  94.140.14.141 unfiltered.adguard-dns.com
  9.9.9.9 dns.quad9.net
  ```

- TESTEN: Unter der Adresse *about:networking* kann man sich auf dem Reiter *DNS* anschauen, ob der Trusted Recursive Resolver funktioniert und verwendet wird.
- Wenn man mit dem Browser auch den Router konfigurieren oder auf Ressourcen im privaten LAN zugreifen möchte und dafür den DNS Namen verwendet, muss man diese Domains von der Namensauflösung via DNS-over-HTTPS ausnehmen, da der öffentliche DNS-Server diese Informationen nicht kennen kann.

  Um eine oder mehrere Domains nicht via DNS-over-HTTPS aufzulösen, kann man folgende Variable unter *about:config* setzen (Beispiel für einen Fritz!Box-Router):

  ```
  network.trr.excluded-domains = fritz.box
  ```

- Road-Warrior, die häufig an Wi-Fi-Hotspots unterwegs sind, können nach dem Login im Portal des Hotspots automatisch auf DNS-over-HTTPS umschalten:

  ```
  network.trr.wait-for-portal = true
  network.captive-portal-service.enabled = true
  ```

  (Die Wi-Fi-Hotspot Portalerkennung ist in unserer Firefox-Config deaktiviert.)

4.19 Firefox Activity-Stream

Der Activity-Stream ist auf der NewTab-Page und der Startseite aktiv. Unter einem Suchfeld werden häufig besuchte Webseiten sowie individuell optimierte Vorschläge für populäre Webseiten angezeigt, die von Pocket ausgewählt werden. Außerdem verkauft Mozilla Plätze für Werbung in den Empfehlungen, die als *Gesponsert von ...* gekennzeichnet sind.

- Das Suchfeld könnte man als praktisch, aber überflüssig bezeichnen, da man in der Adressleiste bereits ein Suchfeld hat.
- Häufig besuchte Webseiten und zufällige Vorschläge aus der History sind überflüssig, wenn man diese Daten nicht speichert.
- Die individuell optimierten Vorschläge, die von Pocket aus einer handverlesenen Liste von 900+ Top-Webseiten ausgewählt werden, sind datenschutzrelevant.

Laut Datenschutz-Statement verwendet Pocket Cookies und andere Technologien (EverCookies?), um einen optimalen Service basierend auf unseren Aktivitäten und Interessen(!) anzubieten. Klickt man auf einen der angebotenen Vorschläge, signalisiert man Interesse an dem Thema und der Klick wird von Pocket registriert. Außerdem sammelt Pocket Telemetriedaten über den Aufruf des Activity-Stream und Informationen darüber, ob er vom User abgeschaltet wurde.

(Also wieder jemand, der sich für unsere Interessen interessiert, um tolle individuelle Vorschläge zu machen damit ein bisschen Werbung zu verteilen.)

Beim Test der Funktion wurden Webseiten wie Bild.de, YouTube.com u. Ä. vorgeschlagen. Ist Bild.de wirklich eine Webseite, die man an erster Stelle empfehlen muss? Oder hat der Springer Verlag dafür bezahlt? Durch den Aufruf der NewTab-Page wurden auf einem nackten Firefox 57.0 mehrere Tracking-Cookies für Bild.de reproduzierbar neu gesetzt (siehe Abb. 4.29: *wt3_eid* und *wt3_sid* sind Tracking-Cookies von WebTrekk), obwohl www.Bild.de nie aufgerufen wurde.

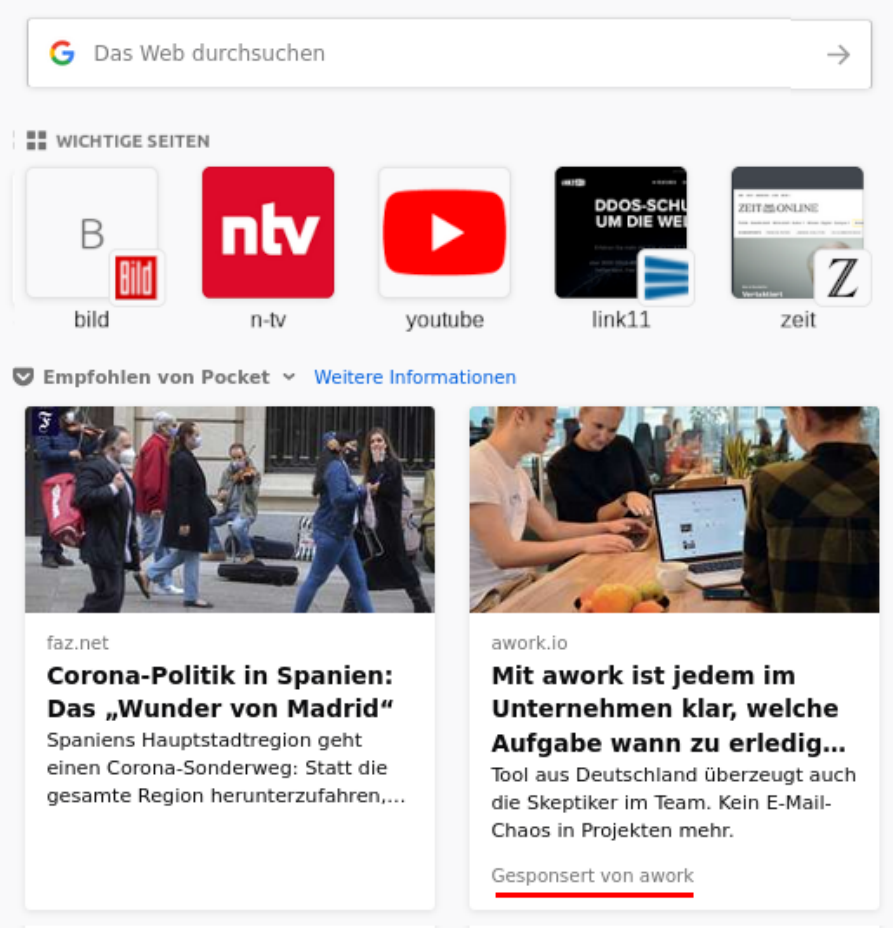


Abbildung 4.27: Gesponserte Empfehlungen auf der NewTab-Page und auf der Startseite

Wie konnte die Webseite Bild.de die Tracking-Cookies setzen? Um die NewTab-Page darzustellen (seit Firefox 61 auch die Startseite), holt Firefox eine JSON-Datei von Mozilla, die eine Liste der URLs für die darzustellenden Icons aller 900+ Top-Webseiten enthält. Für Bild.de findet man folgenden Eintrag:

```
{
"domains": ["bild.de"]
"image_url": "https://bilder.bild.de/fotos/bild-de-..../3.bild.png"
}
```

Das Icon für Bild.de wird also von dem Webserver *bilder.bild.de* geholt und dieser nutzt die Möglichkeit, einige Tracking-Cookies zu setzen. Dies ist auch bei anderen Empfehlungen möglich.

Activity-Stream deaktivieren

Mit Firefox 57 hat Mozilla den Activity-Stream in die NewTab-Page integriert und mit Firefox 61 auch in die Startseite, die standardmäßig genutzt wird. Außerdem wurde in Firefox 61 eine grafische Konfigurationsmöglichkeit eingebaut, um den Activity-Stream zu deaktivieren. Seit Firefox 78 erscheinen bei Eingabe einer URL zusätzlich Vorschläge aus dem Activity-Stream und seit Firefox 83 werden Plätze in den Empfehlungen als Werbeflächen verkauft.

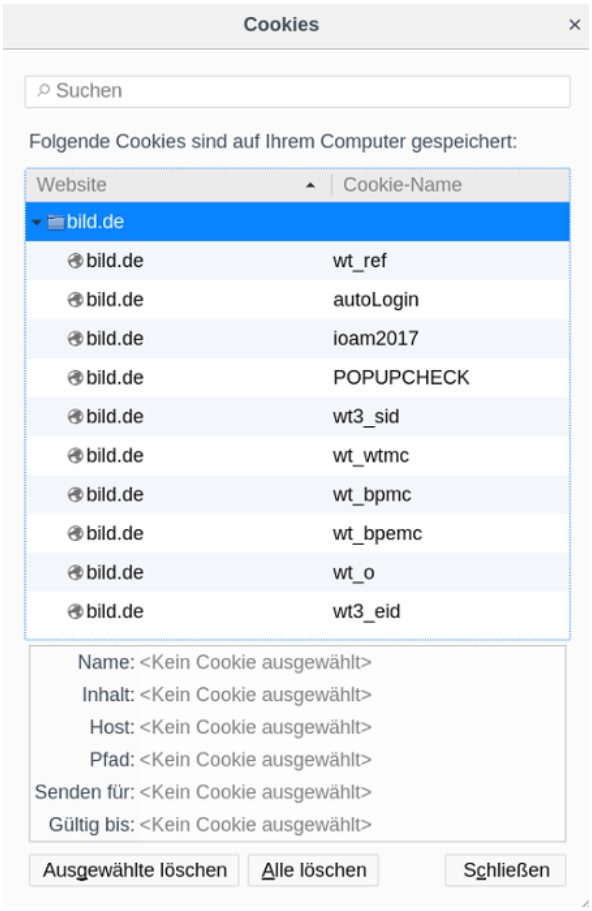


Abbildung 4.28: Cookies von Bild.de nach Aufruf eines neuen Tab

Unter der Adresse *about:config* kann man ebenfalls Einstellungen vornehmen und den Activity-Stream für die Startseite und für neue Tabs abschalten:

```
browser.startup.page       = 0
browser.newtabpage.enabled = false
```

Wenn man eine eigene Startseite verwenden möchte, die nicht Privacy-invasiv ist, kann man folgende Parameter unter *about:config* setzen:

```
browser.startup.page     = 1
browser.startup.homepage = <URL>
```

Bezahlte Werbeeinblendungen deaktiviert man mit folgenden Einstellungen:

```
browser.newtabpage.activity-stream.showSponsored         = false
browser.newtabpage.activity-stream.showSponsoredTopSites = false
```

Oberflächlich sieht damit alles ok aus: Man hat eine Startseite sowie eine NewTab-Page ohne überflüssigen Schnickschnack und wird nicht mit handverlesenen Empfehlungen belästigt. Beim Starten kontaktiert Firefox aber weiterhin die Server mit den Empfehlungen und holt die aktuellen Dateien. Das kann man Firefox mit folgenden Optionen abgewöhnen:

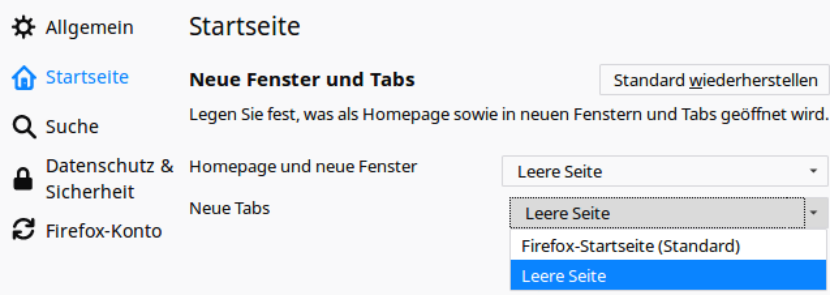


Abbildung 4.29: Leere Seite für Startseite und neue Tabs konfigurieren

```
browser.topsites.contile.enabled                              = false
browser.newtabpage.activity-stream.feeds.topsites             = false
browser.newtabpage.activity-stream.feeds.snippets             = false
browser.newtabpage.activity-stream.section.highlights.includePocket = false
browser.newtabpage.activity-stream.feeds.system.topsites = false
```

Im Hintergrund sendet Firefox außerdem Telemetrie-Pings an den Pocket-Server und teilt diesem damit laufend mit, dass man *Activity-Stream-Feeds* deaktiviert hat. Um diese Telemetrie-Pings ebenfalls zu deaktivieren, muss man noch einige weitere Werte unter *about:config* setzen:

```
browser.newtabpage.activity-stream.telemetry       = false
browser.newtabpage.activity-stream.feeds.telemetry = false
```

Auch die Ping-Centre-Funktion für den Datenversand ist zu deaktivieren:

```
browser.ping-centre.telemetry = false
```

Firefox speichert Screenshots von jeder besuchten Webseite auf der Festplatte, um sie später als Thumbnails im Activity-Stream einzublenden. Diese Speicherung gefällt mir nicht, weil ich mein Surfverhalten nicht protokollieren möchte, auch nicht auf dem eigenen Rechner. Da man diese Thumbnails nicht mehr benötigt, wenn statt des Activity-Stream eine leere Seite angezeigt wird, kann man eine neue Variable vom Typ Boolean unter *about:config* erstellen, um die Speicherung der Screenshots zu deaktivieren:

```
browser.pagethumbnails.capturing_disabled = true
```

4.20 Sonstige Maßnahmen

Am Schluss der Konfiguration gibt es noch ein paar kleine Maßnahmen, um überflüssige Features im Browser zu deaktivieren, die Informationen preisgeben.

Überflüssige Cloud-Dienste deaktivieren

Firefox bietet mehrere Dienste, die die *User Experience* verbessern sollen und dafür irgendwelche Daten auf irgendwelche Cloud-Server hochladen:

Pocket-API ist eine Erweiterung, mit der man Webseiten komplett in einem sogenannten Pocket speichern und später lesen kann. In der Praxis kann man natürlich auch Lesezeichen dafür nutzen oder die Download-Funktion, wenn man eine Webseite später in genau diesem Zustand lesen möchte. Die Pocket-API ist überflüssig, man kann sie unter *about:config* deaktivieren:

```
extensions.pocket.enabled = false
```

Screenshots ist eine Erweiterung, mit der man Bildschirmfotos erstellen kann. Sie besteht aus lokalen und webbasierten Komponenten und es werden Daten gesammelt:

- Die lokale Datensammlung zur Nutzung der Funktion kann man in den Einstellungen deaktivieren, indem man das Senden von Daten über Interaktionen an Mozilla verbietet.
- Die Datensammlungen der webbasierten Komponente kann man nur deaktivieren, indem man den *Do Not Track*-Header aktiviert, was wir nicht empfehlen.

Wenn man Screenshots haben möchte, dann gibt es genügend Tools, die sie ohne irgendwelche webbasierten Komponenten mit Datensammlung erstellen können. Die Screenshot-Extension von Firefox kann man unter *about:config* abschalten:

```
extensions.screenshots.disabled = true
```

Firefox Sync kann die Passwörter, Lesezeichen, Add-ons, Einstellungen, Chronik und geöffnete Tabs verschlüsselt in die Mozilla-Cloud laden und über mehrere Firefox-Instanzen synchronisieren. Welche Daten synchronisiert werden sollen, ist konfigurierbar.

Wenn man Firefox Sync nicht nutzen möchte, kann man den Service komplett abschalten und damit auch die Menüeinträge und Einstellungen verbergen:

```
identity.fxaccounts.enabled = false
```

Keine Daten beim Ausfüllen von Formularen speichern

Firefox bietet die Möglichkeit, Daten aus Formularen zu speichern und später ähnliche Formulare automatisch auszufüllen. Seit Version 55 können Adressdaten erkannt und gespeichert werden, Firefox 58+ kann Kreditkartennummern erkennen und speichern. Damit soll vor allem Power-Shoppern das Einkaufen im Internet etwas erleichtert werden.

Firefox bietet einige Schutzfunktionen gegen Phishing-Angriffe auf automatisch ausgefüllte Formulardaten. Trotzdem ist es nicht auszuschließen, dass raffinierte Angreifer Wege finden werden, um unsichtbare Formulare automatisch ausfüllen zu lassen und die Daten auslesen. Unter *about:config* kann man das Speichern von Formulardaten abschalten:

```
browser.formfill.enable = false
```

Zusätzlich kann man folgende Features deaktivieren:

```
extensions.formautofill.addresses.enabled    = false
extensions.formautofill.creditCards.enabled  = false
extensions.formautofill.heuristics.enabled   = false
```

WebGL konfigurieren oder deaktivieren

WebGL stellt eine JavaScript-API für das Rendering von 3D-Objekten bereit. Wenn die Debug-Informationen via JavaScript auslesbar sind, können Informationen über den Hersteller und das Modell der Grafikkarte ausgelesen werden. Diese Informationen sind gut für das Fingerprinting geeignet. Deshalb sollten die WebGL-Debug-Informationen in jedem Fall abgeschaltet werden:

```
webgl.enable-debug-renderer-info = false
```

WebGL kann die Performance der Grafikhardware und OpenGL-Software für das Fingerprinting verwenden, wie die Studie *Perfect Pixel: Fingerprinting Canvas in HTML5*[78] zeigt. Das Fingerprinting via WebGL kann mit folgenden Einstellungen reduziert werden:

```
webgl.min_capability_mode                       = true
webgl.disable-fail-if-major-performance-caveat = true
```

Außerdem ist WebGL ein (unnötiges) Sicherheitsrisiko, weil damit Angriffe auf das Betriebssystem möglich werden. Durch nachgeladene Schriften können Bugs in den Font-Rendering-Bibliotheken ausgenutzt werden, das gab es schon für Windows (ms11-087), Linux (CVE-2010-3855) oder OpenBSD (CVE-2013-6462). Die WebGL Shader Engines haben auch gelegentlich Bugs, wie z. B. MFSA 2016-53. Man kann WebGL komplett deaktivieren, um dieses Risiko zu reduzieren:

```
webgl.disabled      = true
webgl.enable-webgl2 = false
```

Clipboard Events deaktivieren

Mit den Clipboard-Events informiert Firefox eine Webseite, dass der Surfer einen Ausschnitt in die Zwischenablage kopiert hat oder den Inhalt der Zwischenablage in ein Formularfeld eingefügt hat. Es werden die Events *oncopy, oncut* und *onpaste* ausgelöst, auf die die Webseite reagieren kann. Man kann diese Events unter *about:config* deaktivieren:

```
dom.event.clipboardevents.enabled = false
```

Außer bei Google Docs und ähnlichen JavaScript-lastigen GUIs zur Dokumentenbearbeitung in der Cloud ist mir keine sinnvolle Anwendung dieses Features bekannt.

Spekulatives Laden von Webseiten

Firefox beginnt in einigen Situationen bereits mit dem Laden von Webseiten, wenn sich der Mauszeiger über einem Link befindet, also bevor man wirklich klickt. Damit soll das Laden von Webseiten einige Millisekunden beschleunigt werden. Wenn man Verbindungen mit unerwünschten Webservern vermeiden möchte, kann man das Feature unter *about:config* abschalten:

```
network.http.speculative-parallel-limit = 0
```

[78] https://iehost.net/pdf/w2sp12-final4.pdf

Kill-Switch für Add-ons abschalten

Die Extension blocklist[79] kann Mozilla nutzen, um einzelne Add-ons im Browser zu deaktivieren. Es ist praktisch ein Kill-Switch für Firefox Add-ons und Plug-ins. Beim Aktualisieren der Blockliste werden detaillierte Informationen zum realen Browser und Betriebssystem an Mozilla übertragen.

```
https://addons.mozilla.org/blocklist/3/%7Bec8030f7-c20a
↪  -464f-9b0e-13a3a9e97384%7D/10.0.5/Firefox/20120608001639
↪  /Linux_x86-gcc3/en-US/default/Linux%202.6.37.6-smp%20
(GTK%202.24.4)/default/default/20/20/3/
```

Ich mag es nicht, wenn jemand remote irgendetwas auf meinem Rechner deaktiviert oder deaktivieren könnte. Unter *about:config* kann man dieses Feature abschalten:

```
extensions.blocklist.enabled = false
```

Update der Metadaten für Add-ons deaktivieren

Seit Firefox 4.0 kontaktiert der Browser täglich den AMO-Server von Mozilla und sendet eine genaue Liste der installierten Add-ons und die Zeit, die Firefox zum Start braucht. Als Antwort sendet der Server Statusupdates für die installierten Add-ons. Diese Funktion ist unabhängig vom Update-Check für Add-ons, es ist nur eine zusätzliche Datensammlung von Mozilla. Unter *about:config* kann man diese Funktion abschalten:

```
extensions.getAddons.cache.enabled = false
```

Healthreport und Übertragung von Telemetriedaten deaktivieren

Die Übertragungen von Telemetriedaten, Crashreports, Healthreports usw. an Mozilla unterbindet man mit folgenden globalen Kill-Switches:

```
browser.tabs.crashReporting.sendReport     = false
datareporting.policy.dataSubmissionEnabled = false
datareporting.healthreport.uploadEnabled   = false
```

Eine Abschaltung einzelner Telemetriefeatures (*toolkit.telemetrie.*.enabled=false*) wird oft empfohlen, ist aber unvollständig und überflüssig. Mit den oben genannten Einstellungen wird die Übertragung von Telemetriedaten an Mozilla abgeschaltet.

Im August 2018 hat Mozilla festgestellt, dass es keine Daten darüber gibt, wie viele Nutzer die Übertragung der Telemetriedaten abgeschaltet haben. Deshalb hat Mozilla im September 2018 das Add-on Telemetrie Coverage eingebaut und an 1 % der Nutzer verteilt. Das Add-on ignoriert die Einstellungen zu Telemetrie und sendet folgende Daten an Mozilla: Firefox-Version, Update-Channel, Betriebssystem und -version sowie die Information, ob die Übertragung von Telemetriedaten deaktiviert wurde. Um diese Datenübertragung an Mozilla zu deaktivieren, muss man unter *about:config* folgende Variablen neu anlegen:

[79] https://addons.mozilla.org/en-US/firefox/blocked/

```
toolkit.coverage.endpoint.base     = ""    (leerer String)
toolkit.coverage.opt-out           = true  (laut Mozilla-Doku)
toolkit.telemetry.coverage.opt-out = true  (im Code verwendet)
```

Außerdem kann man das *Ping-Centre* für Datenerhebung und -versand deaktivieren:

```
browser.ping-centre.telemetry = false
```

Firefox Location Tracking

Seit Firefox 80 trackt Firefox den Standort der Nutzer. Bei jedem Start wird der Server *location.services.mozilla.com* angepingt und anhand der IP-Adresse das Land ermittelt, in dem der Nutzer sich aufhält. Die Daten werden in zwei Variablen gespeichert:

```
Region.current  (das aktuelle Land, in dem der Nutzer sich aufhält)
Region.home     (das vermutete Heimatland des Nutzers)
```

Laut Dokumentation verwendet Mozilla diese Daten, um irgendwelchen relevanten Content auszuwählen und die Standardsuchmaschine zu definieren (in Abhängigkeit von den Verträgen, die Mozilla mit unterschiedlichen Suchdiensten abgeschlossen hat).

Das Aktualisieren des Standortes verhindert man mit folgendem Schalter:

```
browser.region.update.enabled = false
```

Mozillas Werbung nach einem Update

Nach jedem Update von Firefox wird eine andere Startseite aufgerufen, die Mozilla für Werbung sowie statistische Auswertungen nutzt und die ein bisschen nervt. Unter der Adresse *about:config* kann man diese Einblendung abschalten:

```
browser.startup.homepage_override.mstone = ignore
```

Contextual Feature Recommender (CFR)

CFR ist ein Werbesystem für Firefox Add-ons und Features. Es ist unklar, nach welchen Richtlinien Mozilla die Empfehlungen auswählt. Mit der Empfehlung für Add-ons hat Mozilla schon öfter danebengegriffen und ein Tracking-Add-on als Trackingschutz empfohlen (Bugzilla: 1483995) oder ein angebliches Security-Add-on beworben, das massenweise Daten gesammelt hat.[80]

Man sollte Add-ons nicht wahllos aufgrund irgendwelcher Empfehlungen installieren, die nicht nachvollziehbar sind. Konzeptloses Zusammenwürfeln von irgendwelchen Datenschutz-Add-ons, wie es Mozilla z. B. im Blogartikel *Make your Firefox browser a privacy superpower with these extensions*[81] empfiehlt, ist kein sinnvoller Ansatz. Deshalb kann man den Contextual Feature Recommender abschalten, um nicht belästigt zu werden.

In den Einstellungen findet man die Option im Bereich *Allgemein* unter *Browsing* (Abb. 4.30). Unter *about:config* kann man folgende Variablen setzen:

[80] https://www.tagesschau.de/inland/tracker-online-103.html
[81] https://blog.mozilla.org/firefox/make-your-firefox-browser-a-privacy-superpower-with-these-extensions/

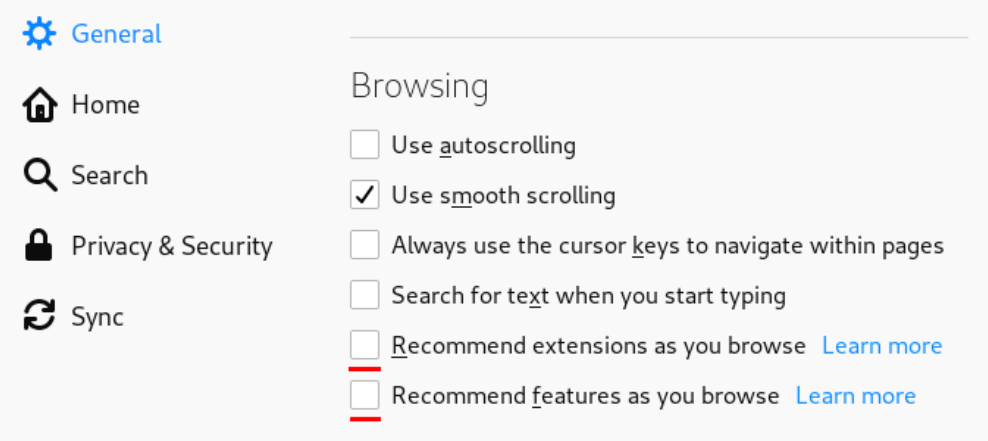


Abbildung 4.30: Contextual Feature Recommender (CFR) deaktivieren

```
browser.newtabpage.activity-stream.asrouter.userprefs.cfr.addons   = false
browser.newtabpage.activity-stream.asrouter.userprefs.cfr.features = false
```

Außerdem werden in der Add-on-Verwaltung von Firefox Empfehlungen angezeigt, die den Nutzer zur Installation verführen sollen. Die Empfehlungen werden als iFrame von einem Mozilla-Server geladen und als Erstes beim Aufruf der Add-on-Verwaltung angezeigt. Diese Empfehlungen kann man mit folgenden Einstellungen unter *about:config* abschalten und die Add-on-Verwaltung von Firefox sieht dann wieder viel übersichtlicher aus:

```
extensions.htmlaboutaddons.recommendations.enabled  = false
extensions.ui.lastCategory        = addons://list/extension
```

Safebrowsing deaktivieren

Wenn die Safebrowsing-Funktion aktiv ist, dann holt Firefox alle 30 Minuten aktualisierte Blocklisten von den Safebrowsing-Providern. Alle Seitenaufrufe werden lokal mit den Listen abgeglichen. Bei einem Treffer sendet Firefox einen Hash der URL an den Safebrowsing-Provider, um zu prüfen, ob die Seite noch auf der Liste steht.

Unter Windows werden außerdem alle Downloads von ausführbaren Anwendungen geprüft. Firefox sendet Informationen zur heruntergeladenen Datei (Name, Herkunft, Größe, Hash) an den *Google Safe Browsing Service*. Dafür gilt Googles Datensch(m)utz-Policy.

Unter *about:config* kann man Safebrowsing deaktivieren:

```
browser.safebrowsing.phishing.enabled                          = false
browser.safebrowsing.malware.enabled                           = false
browser.safebrowsing.blockedURIs.enabled                       = false
browser.safebrowsing.downloads.enabled                         = false
browser.safebrowsing.downloads.remote.enabled                  = false
browser.safebrowsing.downloads.remote.block_dangerous          = false
browser.safebrowsing.downloads.remote.block_dangerous_host     = false
browser.safebrowsing.downloads.remote.block_potentially_unwanted  = false
browser.safebrowsing.downloads.remote.block_uncommon           = false
```

```
browser.safebrowsing.downloads.remote.url          =        (leerer String)
browser.safebrowsing.provider.*.gethashURL         =        (leerer String)
browser.safebrowsing.provider.*.updateURL          =        (leerer String)
```

Gegen Phishing-Angriffe schützen keine technische Maßnahmen vollständig, sondern in erster Linie das eigene Verhalten. Und gegen Malware schützen regelmäßige Updates des Systems besser als Virenscanner und schnell veraltende URL-Listen.

Mozillas Werbung für VPNs

Wenn Firefox im Private Browsing Mode erkennt, dass man einen öffentlichen Wi-Fi-Accesspoint verwendet, wird man mit Werbung für das Mozilla-VPN belästigt. Empfehlungen für VPNs gibt es im Kapitel Virtual Private Networks (VPNs) und man kann diese Werbung von Mozilla unter *about:config* mit folgender Option abschalten:

```
browser.vpn_promo.enabled = false
```

Mozillas Bewertungsfeature

Im Rahmen von Stichproben bittet Mozilla die Nutzer, ihre Erfahrungen mit Firefox zu bewerten. Die Bewertungsfunktion baut bei jedem Start von Firefox eine Verbindung zum Mozilla-Server auf. Mit folgender Option unter *about:config* deaktiviert man die Bewertungsfunktion und den Verbindungsaufbau:

```
app.normandy.enabled = ignore
```

Deaktivierung der Add-ons auf Mozillas Webseiten

Standardmäßig werden Add-ons auf folgenden Webseiten deaktiviert, um die Funktionalität sicherzustellen, da sie auch für interne Funktionen von Firefox genutzt werden:

```
accounts-static.cdn.mozilla.net
accounts.firefox.com
addons.cdn.mozilla.net
addons.mozilla.org
api.accounts.firefox.com
content.cdn.mozilla.net
discovery.addons.mozilla.org
install.mozilla.org
oauth.accounts.firefox.com
profile.accounts.firefox.com
support.mozilla.org
sync.services.mozilla.com
```

Damit gibt es auf diesen Webseiten zum Beispiel praktisch keinen Trackingschutz mehr, obwohl sie teilweise Trackingcode einbinden, den uBlock Origin blockieren würde.

Man kann die Deaktivierung der Add-ons auf diesen Webseiten verhindern, wenn man folgende Variable unter *about:config* auf einen leeren String setzt:

```
extensions.webextensions.restrictedDomains =
```

Diese Einstellung kann aber in Abhängigkeit von den installierten Add-ons auch zu Problemen bei einigen internen Funktionen von Firefox führen, die diese Webdienste nutzen.

Systemfarben der Desktop-Umgebung

Die CSS-Attribute von HTML-Elementen für Farbe und Hintergrund können die Systemfarben der Desktop-Umgebung verwenden. Damit sieht die Webseite einer nativen Desktop-Anwendung ähnlich. Diese individuellen Farben können via JavaScript ausgelesen und für das Fingerprinting des Browsers verwendet werden. Gleiches gilt für den Darkmode.

Um das Auslesen der Desktop-Einstellungen zu verhindern, kann man die eingebauten Standardwerte für die Systemfarben verwenden und den Darkmode deaktivieren:

```
ui.use_standins_for_native_colors = true
ui.systemUsesDarkTheme            = 0
```

In der Empfehlung *CSS Color Module Level 3*[82] ist die Verwendung von Systemfarben als *veraltet* markiert.

Wi-Fi-Hotspot Portalerkennung-deaktivieren

Firefox erkennt die Portalseiten von Wi-Fi-Hotspots und öffnet sie in einem neuen Tab. Für diese Wi-Fi-Hotspot-Portalerkennung ruft Firefox beim Start und bei einigen weiteren Ereignissen die Adresse *http://detectportal.firefox.com/success.txt* mit einem XMLHttpRequest ab. Wenn dabei statt der erwarteten Antwort ein Redirect gefunden wird, öffnet Firefox den Hinweis zum notwendigen Login auf einer Portalseite.

- Wenn man einen Computer im eigenen LAN nutzt, ist die Wi-Fi-Portalerkennung überflüssig. Unter *about:config* kann man sie deaktivieren:

  ```
  network.captive-portal-service.enabled = false
  ```

  (Wenn man gelegentlich (selten) einen Wi-Fi-Hotspot nutzt, kann man die Variable kurzzeitig per Hand auf *true* setzen, damit es funktioniert.)

- Wenn man häufig mit dem Laptop unterwegs ist, kann die Wi-Fi-Portalerkennung ganz nützlich sein. In diesem Fall könnte man die Adresse für den XMLHttpRequest anpassen und einen eigenen Server für den Test verwenden, um nicht ständig den Mozilla-Server zu kontaktieren.

  Am einfachsten lädt man die Datei *success.txt* herunter und speichert sie auf dem eigenen Webserver. Unter *about:config* passt man die URL an:

  ```
  network.captive-portal-service.enabled = true
  captivedetect.canonicalURL = http://www......../success.txt
  ```

  Hinweis: die Datei muss via HTTP abrufbar sein, also ohne SSL-Verschlüsselung. Anderenfalls ist kein Redirect möglich.

[82] https://drafts.csswg.org/css-color-3/

Connectivity-Service deaktivieren

Bei jedem Start und bei einem Wechseln der Netzwerkverbindung kontaktiert Firefox außerdem den Server detectportal.firefox.com, um die IPv4- und IPv6-Verbindungen zu testen. Diese Verbindungen kann man, ohne Nachteile erwarten zu müssen, mit folgender Einstellung deaktivieren:

```
network.connectivity-service.enabled = false
```

Connect zu Mozilla Services Server beim Start deaktivieren

Bei jedem Start von Firefox kontaktiert der Browser den Server firefox.settings.services.mozilla.com, um Aktualisierungen für die installierten Language-Packs herunterzuladen. Dabei werden Informationen zu Betriebssystem und Browserversion an Mozilla gesendet. Das ist überflüssig, da die Aktualisierungen nur minimal sind und man sie auch durch regelmäßige Updates des Browsers bekommt. Um die Verbindungen zu deaktivieren, kann man die Adresse des Servers auf einen ungültigen Wert setzen.

```
services.settings.server = https://s.%.c.invalid/v1
```

4.21 Der Unsinn vom Spoofen der User-Agent-Kennung

Bei jedem Aufruf einer Webseite oder dem Laden von Bilder o. Ä. sendet der Browser in den HTTP-Request-Headern Informationen wie die bevorzugten Dateitypen, die bevorzugte Sprache oder die User-Agent-Kennung mit Daten über den verwendeten Browser, die Version des Browsers und das Betriebssystem. Firefox 72 für Linux sendet zum Beispiel:

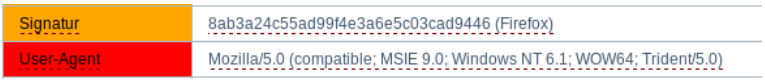
```
Mozilla/5.0 (X11; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
```

Aus unterschiedlichen Gründen wird immer wieder empfohlen, die User-Agent-Kennung zu modifizieren (faken). Linuxer und MacOS Nutzer sollen als Fake die Kennung von Google Chrome für Windows verwenden, weil dieser Browser häufiger verwendet wird und man damit angeblich besser in der Masse untertaucht. Windows-Nutzer sollen ein Linux spoofen, um sich gegen Drive-by-Downloads von Malware zu schützen, u. a. m.

Es ist nahezu unmöglich, die User-Agent-Kennung eines Browsers plausibel zu faken. Eine unsachgemäße Änderung kann zu einem einzigartigen Gesamtbild führen, welches das Tracking enorm erleichtert und man erreicht das Gegenteil des Beabsichtigten. Der Anonymitätstest von JonDonym entlarvte viele Fehler, ist aber nicht mehr online:

HTTP Header: Die einzelnen Browser sind durch individuelle Headerzeilen und -reihenfolgen im HTTP-Request beim Aufruf einer Webseite unterscheidbar. Eine Tarnung mit dem User-Agent eines anderen Browsers ist oft leicht als Fake zu identifizieren. Viele Add-ons zum Spoofen der User-Agent-Kennung machen diesen Fehler.

Das Add-on *User-Agent-Overrider* (Version 0.2.5.1) sollte im Test einen Internet Explorer 9.0 für Win64 faken. Die Header-Signatur entlarvt den Browser jedoch als einen Firefox, der sich als IE tarnen will.



Das Add-on *Random-Agent-Spoofer* (Version 0.9.5.2) sollte im Test einen Google Chrome Browser 41.0 für Win64 faken. Die Header-Signatur entlarvt den Browser ebenfalls als Firefox, der sich tarnen will.

Firefox-Release-Versionen und Firefox-ESR-Versionen unterscheiden sich nicht nur in der Version in der User-Agent-Kennung, sondern auch in anderen Eigenschaften. Firefox 68.x ESR und Firefox 72+ unterscheiden sich im HTTP-Accept-Header:

```
Firefox 68: ...application/xml;q=0.9,*/*;q=0.8
Firefox 72: ...application/xml;q=0.9, image/webp,*/*;q=0.8
```

Es ist deshalb nicht sinnvoll, ein User-Agent-Fake für Firefox ESR zu aktivieren, wenn man eine Firefox-Release-Version verwendet. Die resultierende Kombination von Eigenschaften ist selten und erleichtert das Tracking via Fingerprinting. (Aus diesem Grund ist die Option *privacy.resistFingerprinting* nur für Firefox ESR sinnvoll nutzbar, da damit ein User-Agent-Fake als Firefox ESR für Windows aktiviert wird.)

JavaScript: Das Add-on User Agent Platform Spoofer macht aus einem Firefox für Windows einen Firefox für Linux und umgekehrt, um die automatische Installation von Malware im Drive-by-Download zu erschweren. Auch hier ist der Fake nicht vollständig, wie ein kurzer Test unter Linux zeigt. Mit Javascript kann der genutzte Browsertyp und das Betriebssystem ermittelt werden:

```
User-Agent via HTTP Header:  Mozilla/5.0 (Windows NT 10.0; Win64...
Browsertyp via JavaScript:   Mozilla/5.0 (X11) 20100101/...
```

CSS-Attribute: Durch unterschiedliche Font-Rendering-Bibliotheken ergeben sich Abweichungen bei CSS-Attributen, die mit Javascript ausgelesen werden können. Anhand des CSS-Attributes *line-height* kann man zum Beispiel bei Verwendung hoch- und tiefgestellter Zeichen Schlussfolgerungen über das Betriebssystem ziehen. Es ergeben sich unterschiedliche Werte bei gleichem HTML-Code, beispielsweise 19 px für Linux, 19.5167 px für MacOS und 19.2 px oder 20 px für Windows.

Seltsamkeiten: Der Browser hängt in vielen Dingen von Bibliotheken des Betriebssystems ab. Durch Auswertung einiger Seltsamkeiten lässt sich das real verwendete Betriebssystem teilweise identifizieren oder zumindest ein User-Agent-Fake entlarven. Ein Beispiel OS-spezifischer Seltsamkeiten ist das Ergebnis der folgenden Berechnung:

```
Math.tan(-1e300) = -4.987183803371025 (Windows)
Math.tan(-1e300) = -1.4214488238747245 (Linux, iOS)
```

Es ist nahezu unmöglich, die User-Agent-Kennung von Firefox plausibel in allen Punkten zu faken. Ein unvollständiger Fake-Versuch ist aber ein gutes Identifizierungsmerkmal für Trackingdienste, da man sich von der großen Masse der Surfer stärker unterscheidet.

4.22 Firefox-Profile

Es ist nicht immer möglich, alle Wünsche mit einer einzigen Firefox-Konfiguration abzudecken. Manchmal gibt es unterschiedliche Anforderungen, die unvereinbar sind.

- Man möchte spurenarm im Internet surfen und nimmt dafür auch kleine Einschränkungen in der Funktionalität in Kauf, wenn es den Trackingschutz verbessert.
- Für Videokonferenzen braucht der Browser Zugriff auf Mikrofon und Kamera.
- Man möchte sich unterwegs auch mal an einem Wi-Fi-Hotspot anmelden können.
- Einige (vertrauenswürdige) Webdienste funktionieren mit moderaten oder strengen Einstellungen nicht.
- Bei der heimischen Cloud bzw. dem Router gibt es keine Trackinggefahr und man möchte Probleme durch restriktive Browserkonfigurationen vermeiden, weil es die Fehlersuche verkompliziert.
- ...

Mit den Profilen bietet Firefox eine Möglichkeit, unterschiedliche Konfigurationen, Add-ons, Lesezeichen usw. zu verwalten. Jedes Profil ist ein individuell konfigurierter Browser. Man kann den Profilmanager auf der Kommandozeile mit der Option -P starten:

```
> firefox -P
```

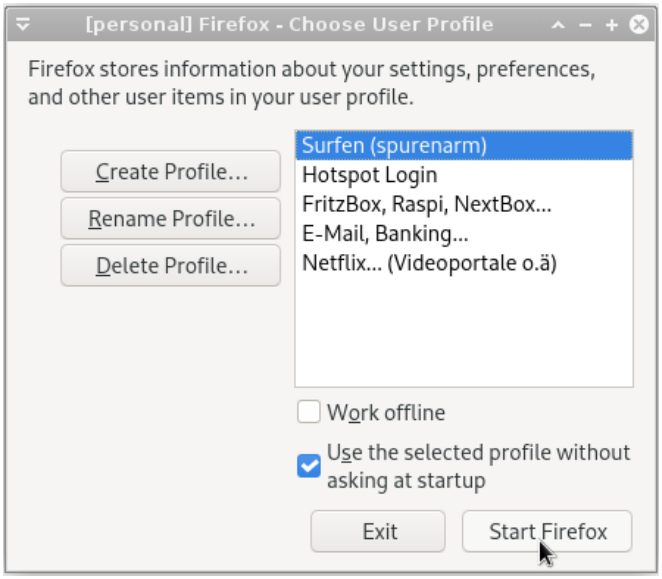


Abbildung 4.31: Firefox Profilmanager

(Wenn man die Option *Use the selected profile without asking at startup* deaktiviert, wird Firefox bei jedem Start fragen, welches Profil gestartet werden soll – bei häufigem Wechsel der Profile evtl. eine brauchbare Variante.)

Außerdem findet man im Firefox unter der Adresse *about:profiles* eine Profilverwaltung. Diese Adresse kann man als Lesezeichen speichern, um schnell das Profil zu wechseln.

Man kann ein bestimmtes Firefox-Profil auch via Kommandozeile starten oder dieses Kommando als Starter auf dem Desktop oder im Startmenü ablegen:

```
> firefox --profile <Path> -no-remote
```

Der <Path> entspricht dem Wurzelordner des Profils, den man unter *about:profiles* findet und die Option *-no-remote* ermöglicht es, das gewählte Profil unabhängig von einer bereits laufenden Firefox-Instanz zu starten.

4.23 Zusammenfassung der Einstellungen

Um die Werte nicht alle per Hand anpassen zu müssen, haben wir Beispielkonfigurationen für Firefox 60+ vorbereitet, die man herunterladen und im Firefox-Profil speichern kann. Man kann nicht alle Wünsche mit einer Konfiguration abdecken, deshalb gibt es mehrere Vorschläge, die man von der Webseite des Privacy-Handbuches herunterladen kann:
https://www.privacy-handbuch.de/handbuch_21u.htm

Die Vorschläge sind Teil eines Gesamtkonzeptes und es wird davon ausgegangen, das die Add-ons *uBlock Origin* und *CanvasBlocker* mit den empfohlenen Konfigurationen installiert wurden. Daraus ergeben sich einige Unterschiede zu vergleichbaren Projekten.

Basis-Einstellungen: ist für Nutzer geeignet, die ohne Beschränkungen von Features surfen wollen, aber ein bisschen Wert auf etwas mehr Privatsphäre legen.

- Deaktivierung von Spielereien, die Mozilla eingebaut hat (Activity Stream, Pocket, Telemetrie, Datareporting, Ping-Centre, Captive Portal Check, Safebrowsing, Family Safety, die bunte NewTabPage und Startseite).
- Löschen von Cache, Cookies usw. beim Beenden des Browsers und die Surfcontainer *Total Cookie Protection* und *userContext* sind als Trackingschutz aktiviert.
- Außerdem werden einige allgemeine Sicherheitsfeatures aktiviert (AutoFill für Formulare deaktiviert, Anzeige von unsicheren Verbindungen als Text+Icon usw.)
- Der HTTPS-First-Mode ist aktiviert, bei Eingabe einer verkürzten URL wird zuerst HTTPS probiert. Wenn ein Fehler auftritt, wird automatisch die HTTP-Seite aufgerufen.

Moderate Einstellungen: es werden zusätzlich einige HTML5-Features deaktiviert, die häufig zum Tracking genutzt werden. Die Funktion normaler Webseiten wird damit in der Regel nicht beeinflusst. Es kann aber vereinzelt zu Problemen kommen.

- Da installierte Schriftarten häufig für das Fingerprinting verwendet werden, ist die Verwendung von individuellen Schriften für HTML-Dokumente deaktiviert. Man sollte deshalb gut lesbare Standardschriften konfigurieren. Einbindung externer Webicon-Fonts für Navigationselemente ist zulässig.
- HTTPS-only-Mode ist aktiviert. Es wird eine Warnung angezeigt, wenn HTTPS nicht funktioniert und man kann mit einem Klick die HTTP-Seite aufrufen.
- Googles Safebrowsing und Mozillas Add-on Blocklist sind deaktiviert.

- Der Captive Portal Service ist abgeschaltet, da er ständig einen Mozilla Service kontaktiert. Für Hotspot-Logins braucht man ein extra Profil mit der passenden Konfiguration.

Medium-strenge Einstellungen: Es werden zur Verbesserung der Sicherheit beim Surfen weitere Funktionen deaktiviert, die keinen Einfluss auf die Darstellung von Webseiten haben, aber die Angriffsfläche beim Surfen vergrößern könnten.

- Video- und Audiodaten werden nicht mehr automatisch abgespielt. Closed Source Codes zum Abspielen von DRM-geschützten Videos sind standardmäßig deaktiviert, können bei Bedarf aber mit einem Klick aktiviert werden.
- Die OpenH264-Videocodecs von Cisco für WebRTC werden deaktiviert. Man kann diese Konfiguration also nicht für Videokonferenzen nutzen.
- Es werden keine Passwörter gespeichert (stattdessen kann man KeepasXC verwenden) und die Option zur Synchronisation der Daten in die Cloud ist deaktiviert.
- JavaScript-Just-in-Time-Compiler sind aus Sicherheitsgründen deaktiviert, was die Ausführung von JavaScript auf einigen Webseiten verlangsamt.
- Bei der Darstellung von PDF-Dokumenten im Browser ist Scripting verboten.
- Der Mozilla Push Service wird deaktiviert und damit die Websocket Verbindung zum Server *push.services.mozilla.com* abgeschaltet.

Strenge Einstellungen: blockieren einiges mehr, was für Angriffe auf Browser und Betriebssystem ausgenutzt werden könnte, weil potentiell kompromittierbare Daten aus dem Internet an Bibliotheken des Betriebssystems weitergeleitet werden (z. B. Font Rendering).

Viele Webseiten werden durch diese Einschränkungen deutlich verunstaltet! Der Download von externen Schriftarten ist auch für Navigationssymbole deaktiviert. Um die resultierenden Einschränkungen etwas abzumildern, kann man häufig genutzte Webicon-Fonts wie den Awesome Webicon Font installieren. Linux-Distributionen enthalten die passenden Pakete:

```
Ubuntu: > sudo apt install fonts-font-awesome
Fedora: > sudo dnf install fontawesome-fonts fontawesome-fonts-web
```

Diese Einstellungen sind für Risikogruppen geeignet, die für höhere Sicherheit Einschränkungen beim Surfen in Kauf nehmen, und sollten mit NoScript kombiniert werden.

Hotspot Login: ist eine strenge user.js mit aktiviertem Captive Portal Service. Sie könnte in einem Profil eingesetzt werden, dass man nur für den Login bei Wi-Fi-Hotspots nutzt.

Die gewählte Datei *user.js* ist im Firefox-Profil zu speichern und wird beim Start von Firefox eingelesen. Die Werte überschreiben die Einstellungen in *prefs.js*. Damit ist sichergestellt, dass man beim Start die gewünschten Einstellungen hat.

Das Firefox-Profil ist ein Unterverzeichnis mit seltsamen Buchstaben, das man in folgenden Verzeichnissen findet:

- Windows: %APPDATA% → Mozilla → Firefox → Profiles → ...
- MacOS: Library → Application Support → Firefox → Profiles → ...
- Linux: $HOME/.mozilla/firefox/...

Hinweis: Wenn man feststellt, das die gewählte Variante zu restriktiv ist und man auf eine weniger restriktive Variante wechseln möchte, dann muss man im Profilverzeichnis die Dateien *user.js* und *prefs.js* löschen. Wenn man etwas dazwischen will, kann man man die weniger restriktive Variante wählen und die Einstellungen unter *about:config* ergänzen.

4.24 Snakeoil für Firefox (Überflüssiges)

Auf der Website für Firefox Add-ons findet man tausende Erweiterungen. Man kann nicht alle vorstellen. Es kommen immer wieder Hinweise auf dieses oder jenes datenschutzfreundliche Add-on. Deshalb gibt es an dieser Stelle ein paar Dinge, die nicht empfehlenswert sind.

Als Grundsicherung ist die Kombination von *Total Cookie Protection + Netzwerkpartitionierung + uBlock Origin* und einem Add-on zum variieren des Browserfingerprint empfehlenswert. Viele Add-ons bieten Funktionen, die von dieser Kombination bereits abgedeckt werden. Andere sind einfach nur überflüssig.

4.24.1 Do-Not-Track ist am Lobbyismus gescheitert

Do-Not-Track (DNT) wurde 2009 von der EEF.org vorgeschlagen. Mit einem zusätzlichen HTTP-Header sollte der Browser den grundsätzlichen Wunsch des Nutzers übermitteln, nicht getrackt zu werden. Im Dezember 2010 erklärte die FTC die Unterstützung für DNT und 2012 begann das W3C mit der Standardisierung des Features.

Der eindeutige Wunsch der Nutzer, den die Aktivierung von DNT im Browser zum Ausdruck bringen sollte, wurde von der Trackingbranche ignoriert. Empirische Studien zeigten, dass sich das Tracking beim Surfen damit um weniger als 2 % verringerte.

Es war ein genialer Schachzug von Microsoft, DNT im IE10 standardmäßig ohne Interaktion des Nutzers zu aktivieren. Das widersprach eindeutig den Intentionen des W3C Standard, der ausdrücklich definierte, das ein DNT-Header nur vom Browser gesendet werden darf, wenn der Nutzer damit einen Wunsch aktiv zum Ausdruck bringen möchte:

> *The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed.*
> ...
> *A user agent MUST have a default tracking prefernce of* ***unset*** *unless a specific tracking preference is implied by the user decision...*

Diese Aktivierung *by Default* gab der Trackingbranche den Vorwand, DNT offiziell zu ignorieren, da man nicht mehr davon ausgehen könne, dass ein Nutzer sich aktiv dafür entschieden habe. Yahoo erklärte im Mai 2014, dass alle Dienste des Konzerns DNT ignorieren werden, es folgten Google und Facebook im Juni und Twitter zwei Jahre später.

Beim Start der Diskussion zu einer neuen, europäischen ePrivacy-Verordnung im Januar 2017 sollte ursprünglich die Respektierung von „Do-Not-Track“ als verpflichtend definiert werden. In dem 2019 vorgelegten Diskussionspapier zur ePrivacy-Verordnung wurde dieser Punkt gestrichen.

Die DNT-Arbeitsgruppe beim W3C hat 2019 die finale Spezifikation für DNT vorgelegt und die Arbeit beendet. In der Spezifikation wird unter 10.2 darauf hingewiesen, dass die Umsetzung neue Ansätze für das Fingerprinting des Browsers bieten könnte. *Do-Not-Track* ist aber politisch gescheitert.

Laut Bloomberg haben nur 12 % der Nutzer weltweit DNT aktiviert. Da DNT nicht nennenswert gegen Tracking schützt, schafft man mit der Aktivierung von DNT nur ein Differenzierungsmerkmal für das Fingerprinting des Browsers. Apple hat DNT deshalb aus dem Browser Safari entfernt.

In Firefox deaktiviert man DNT unter *about:config* mit folgenden Optionen:

```
privacy.donottrackheader.enabled   = false
privacy.trackingprotection.enabled = false
```

Stattdessen sind uBlock Origin oder AdGuard empfehlenswert.

4.24.2 Private Browsing Mode

Mit grafischem Pomp signalisiert Firefox, dass man im *Private Browsing Mode* (auch *Porno-Mode* genannt) irgendwie anonym im Netz unterwegs wäre, was aber falsch ist.

- Im Private Browsing Mode speichert Firefox keine Cookies, besuchte Webseiten, Suchbegriffe, Formulardaten, Passwörter usw. dauerhaft auf der Festplatte. Es bleiben also keine Spuren von besuchten Webseiten (Pornowebseiten?) auf der Festplatte.

  In den Einstellungen kann man das auch für das normale Surfen konfigurieren.

- Im Private Browsing Mode wird der (löchrige) strenge Trackingschutz mit allen weiteren Features wie Total Cookie Protection usw. aktiviert.

  uBlock Origin oder AdGuard sind trotzdem erforderlich und sinnvolle Features wie Total Cookie Protection usw. sollte man auch beim normalen Surfen aktivieren.

- Außerdem wird mit strengem Trackingschutz auch der Do-Not-Track-Header aktiviert, was bezüglich Browser-Fingerprinting kontraproduktiv ist (siehe oben).

- Eine Webseite kann via JavaScript feststellen, dass der Private Browsing Mode im Browser aktiviert wurde, und könnte diese Information für das Fingerprinting des Browsers verwenden. Firefox deaktiviert bspw. die IndexedDB-API im Private Browsing Mode. Um die Erkennung zu erschweren, könnte man unter *about:config* folgenden Wert setzen:

  ```
  dom.indexedDB.privateBrowsing.enabled = true
  ```

  Die Webseite Fingerprint.com[83] demonstriert diese Erkennung des Private-Browsing-Mode und zeigt außerdem, dass dieser nicht gegen moderne Trackingmethoden wie Browser-Fingerprinting schützt. Das Surfverhalten im normalen Surfmodus kann mit dem Surfen im Private Browsing verknüpft werden.

Schlussfolgerung: es ist besser, den normalen Surfmode datenschutzfreundlich zu konfigurieren, statt im Private-Browsing-Mode von der Masse der Surfer unterscheidbar zu sein.

4.24.3 Web of Trust (WOT)

WOT war ein Add-on, das den Surfer über die Reputation der besuchten Webseite informierte. Das Add-on wurde häufig empfohlen und auch von Mozilla in Add-on-Empfehlungen promotet.

Während des Surfens sammelte WOT Daten über den Besuch jeder Webseite und übertrug die Daten an die Betreiber des Dienstes. Die Daten werden mit schwacher Anonymisierung zu Profilen verknüpft und auch an die Werbeindustrie verkauft, wie Reporter des NDR zeigten[84]. Die

[83] https://fingerprint.com
[84] https://www.tagesschau.de/inland/tracker-online-103.html

Daten konnten relativ einfach deanonymisiert werden und lieferten umfangreiche Informationen zu Krankheiten, sexuellen Vorlieben und Drogenkonsum einzeln identifizierbarer Personen.

Unschön, wenn über einen Richter bekannt wird, dass er eine Vorliebe für Sado-Maso-Praktiken hat, oder wenn sich Valerie Wilms, Bundestagsabgeordnete der Grünen, aufgrund der Daten erpressbar fühlt.

Man sollte nicht irgendwelche Add-ons auf Grundlage dubioser Empfehlungen installieren.

4.24.4 Google Analytics Opt-Out

Das Add-on von Google verhindert die Ausführung des JavaScript-Codes von Google-Analytics. Die Scripte werden jedoch trotzdem von den Google-Servern geladen und man hinterlässt Spuren in den Logdaten. Google erhält die Informationen zur IP-Adresse des Surfers und welche Webseite er gerade besucht. Außerdem gibt es über hundert weitere Surftracker, die ignoriert werden.

AdBlocker wie *uBlock Origin* erledigen diese Aufgabe besser.

Kapitel 5

Surfen mit dem Mullvad Browser

Der Mullvad Browser wird vom VPN Provider Mullvad in Zusammenarbeit mit TorProject.org bereitgestellt. Es ist ein TorBrowserBundle, bei dem der Tor Onion Router entfernt und durch ein bisschen Werbung für den Mullvad VPN Dienst ersetzt wurde.

Mit dem Browser möchter Mullvad die typische Trackingproblemen beim anonymen Surfen via VPNs addressieren. Der Mullvad Browser kann aber auch ohne VPN verwendet werden.

Beim Schutz gegen Tracking folgt der Mullvad Browser dem Konzept von TorProjekt.org (keine Daten langfristig speichern und Abtauchen in einer Anonymitätsgruppe). Dieses Konzept wird nur funktionieren, wenn der Browser von einer hinreichend großen Gruppe mit dem gleichen Betriebssystem verwendet wird. Aufgrund der Popularität des TorBrowseBundles kann man vermutlich davon ausgehen, das der Mullvad Browser weltweit hinreichend große Nutzerzahlen erreichen wird.

5.1 Installation

Nach dem Download von der Download Webseite[1] bei Mullvad ist das Archiv zu entpacken und der Browser kann gestartet werden. Dafür werden keine Administratorrechte benötigt.

Windows Nutzer starten das selbstenpackende EXE Archiv. Als erstes muss man bestätigen, dass man die aus dem Internet heruntergeladene EXE-Datei wirklich ausführen will.

Am Ende der Installation kann man entscheiden, ob man den Browser sofort starten will (muss man nicht). Aber es ist wichtig, im letzten Schritt den Eintrag für den Mullvad Browser im Startmenü und auf dem Desktop anzulegen.

Linuxer entpacken das Archiv mit dem bevorzugten Archiv-Manager ins $HOME Verzeichnis oder erledigt es auf der Kommandozeile mit mit folgendem Kommando:

```
> tar -xavf mullvad-browser-linux*.tar.xz -C $HOME
```

Danach kann man den Mullvad Browser starten, indem man das Startscript auf der Kommandozeile aufruft oder mit einem Klick im Dateimanager startet:

```
> $HOME/mullvad-browser/start-mullvad-browser.desktop
```

[1] https://mullvad.net/de/download/browser/

Mit einem kleinen Kommando kann man den Mullvad Browser im Startmenü des Desktops in der Gruppe *Internet* hinzufügen, um den Start zu vereinfachen:

```
> cd $HOME/mullvad-browser
> ./start-mullvad-browser.desktop --register-app
```

Mäuschenschubser, die das Full-Text-Adventure nicht mögen, könnten nach dem Entpacken mit einem Rechstklick im Dateimanager einen Programmstarter im Panel erstellen.

Man kann den Mullvad Browser mit folgendem Kommando im **Firejail** zu starten:

```
> firejail --private=~/mullvad-browser ./start-mullvad-browser.desktop
```

...oder man legt eine Datei *mullvadbrowser-firejail.desktop* auf dem Desktop/Panel an:

```
[Desktop Entry]
Name=Mullvad Browser im Firejail
Exec=firejail --private=~/mullvad-browser
↪  ./start-mullvad-browser.desktop
Icon=/home/<username>/mullvad-browser/Browser/browser/chrome/icons/def
↪  ault/default48.png
Terminal=false
Type=Application
```

5.2 Anpassung der Konfiguration

Da das Anonymitätskonzept beim Mullvad Browser darauf beruht, dass möglichst viele Nutzer den Browser in der gleichen Konfiguration nutzen, um betriebssystem-spezifische Anonymitätsgruppen zu bilden, sind nur wenige Konfigurationsänderungen sinnvollerweise empfehlenswert.

- Die Größe des Browserfensters sollte man nicht ändern, da es ein häufig genutztes Trackingmerkmal ist. Der Browser startet mit den optimalen Werten für die Anonymitätsgruppe.
- Die Lesezeichensymbolleiste kann man ständig anzeigen lassen mit der Tastenkombination STRG+SHIFT+B. Da keine Surfhistory gespeichert wird, braucht man öfters Lesezeichen.
- Das Mullvad Icon mit der Werbung für den VPN Dienst kann man aus der Toolbar entfernen (wenn es stört). Dafür klick man mit der rechten Maustaste auf die Toolbar und wählt den Menüpunkt *Customize Toolbar...* Via Drag & Drop kann man dann das Icon herausziehen.
- Wie beim TorBrowser kann man den Sicherheitslevel mit zwei Klicks anpassen und gefährliche Webtechniken einschränken. Der mittlere Level ist ein guter Kompromiss.
- Weitere Suchmaschinen könnte man installieren. Einige Such-Plugins werden auf der Webseite vom Privacy-Handbuch[2] angeboten, die man mit einem Rechtsklick in der Adressleiste installieren könnte. Auf den Startseiten von Suchmaschinen kann weitere Plugins ebenfalls so hinzufügen.

  In den Einstellungen kann man danach die bevorzugte Standardsuchmaschine auswählen.

[2] https://www.privacy-handbuch.de/handbuch_21_mullvad.htm

Kapitel 6

Spurenarm surfen mit Librewolf

Librewolf ist ein Firefox-Klon mit datenschutzfreundlichen Default-Einstellungen. Die standardmäßig gesetzten Werte für Cookies, Container, HTTPS, Referer usw. entsprechen unseren Empfehlungen und sind abgesehen von kleinen Abweichungen vergleichbar mit der moderaten Konfiguration im Kapitel Firefox.

Telemetrie, Firefox-Sync und weitere Features wurden entfernt. Auch der Captive-Portal-Check wurde entfernt, sodass man Librewolf nicht für Logins bei Wi-Fi-Hotspots nutzen kann. Für Wi-Fi-Hotspot-Logins benötigt man zusätzlich einen anderen Browser.

Da er für spurenarmes Surfen vorkonfiguriert ist, erspart man sich bei Nutzung des Librewolf die Spielerei mit Updates einer user.js-Konfiguration oder Anpassungen der einzelnen Werte unter *about:config* per Hand.

6.1 Installation

Auf der Librewolf-Webseite[1] ist die Installation für verschiedene Systeme beschrieben:

- Für populäre Linux-Distributionen (Debian, Ubuntu, Fedora, Arch, Gentoo) gibt es Repositorys, sodass man Librewolf mit dem bevorzugten Paketmanager installieren und regelmäßig aktualisieren kann.
- Für Windows Nutzer gibt es neben einem Setup-Paket für die Installation auch eine portable Version als ZIP-Archiv, dass man nur entpacken muss. Außerdem kann Librewolf mit verschieden Paketmanagern installiert werden (Chocolatey, Winget, Scoop).
- MacOS Nutzer können Librewolf mit *brew* oder als Disc-Image installieren.

6.2 Anpassungen der Konfiguration

1. **uBlock Origin** ist bereits standardmäßig enthalten. Man kann die vom PrHdb-Team vorbereiteten Konfigurationen herunterladen und importieren.[2]
2. Zum Schutz gegen Javascript Fingerprinting ist *ResistFingerprinting* aktiviert, was TorProject.org für den TorBrowser zum Schutz gegen Fingerprinting entwickelt hat.

[1] https://librewolf.net
[2] https://www.privacy-handbuch.de/handbuch_21d2.htm

- Außerhalb der Welt des Anonymisierungsdienstes Tor hat RFP ein paar kleine Nachteile wie z.B. den TimeZoneMissmatch und den UserAgentMissmatch bei Linux und MacOS.
- Außerdem zeigt die Demo Fingerprint.com, dass dieser Trackingservice den Librewolf mit Standardkonfiguration trotz Aktivierung von ResistFingerprinting verfolgen kann.

ResistFingerprinting (RFP) arbeitet in der Kombination mit den anderen Einstellungen im Librewolf suboptimal. Die Fingerprinting Protection (FPP) von Firefox funktioniert besser. FPP wird im Librewolf automatisch aktiviert, wenn man RFP abschaltet.

Abbildung 6.1: ResistFingerprinting in den Einstellungen von Librewolf deaktivieren

3. Das Add-on **Skip Redirect** entfernt Umleitungen in der URL. Diese Umleitungen werden genutzt, um die Klicks auf Links zu externen Domains zu tracken.
4. Das Add-on **Binnen-I be gone** ersetzt ideologisch motivierte Sprachverhunzungen wie *Politiker*innen* oder *Panzerfahrer:innen*, die man nicht aussprechen oder in andere Sprachen übersetzen kann, die laut Duden kein korrektes Deutsch sind und auch vom Rat für Deutsche Rechtschreibung nicht empfohlen werden, durch das grammatikalische Generikum. Wer sich einmal an das Add-on gewöhnt hat, möchte es nicht mehr missen.
5. Als Suchmaschine ist DuckDuckGo vorinstalliert. Weitere Suchmaschinen kann man wie für Firefox beschrieben nachinstallieren und als Standardsuche setzen.

Kapitel 7

Passwörter und Zwei-Faktor-Authentifizierung

Wenn man sich bei einem Webdienst anmeldet, um personalisierte Angebote zu nutzen (z. B. bei einem E-Mail-Dienst, bei Twitter, Facebook oder einem Webshop), muss man sich als berechtigter User authentifizieren. Für diese Authentifizierung gibt es mehrere Methoden, die man grob in folgende Gruppen einteilen kann:

Authentifizierung durch Wissen: Man muss nachweisen, dass man Kenntnis von einem Geheimnis hat, das Dritten nicht bekannt sein sollte (z. B. ein Passwort oder die Antwort auf eine Sicherheitsfrage). Ein Angreifer sollte dieses Geheimnis nicht von einem Zettel ablesen, es nicht erraten oder durch Ausprobieren knacken können.

Unter den Bedingungen der zunehmenden Videoüberwachung öffentlicher Plätze muss man auch damit rechnen, dass die Passworteingabe bei Nutzung von Smartphones durch Dritte beobachtet werden kann.

Risiko-basierte Authentifizierung (RBA) soll die Sicherheit von Accounts verbessern, die nur mit einem Passwort geschützt sind. Bei einem Login-Versuch wird anhand von Merkmalen ein Risikolevel berechnet, ob möglicherweise ein missbräuchlicher Login erfolgt. Übersteigt der Risikolevel einen Grenzwert, wird eine zusätzliche Verifizierung gefordert. In der Regel muss der Nutzer ein zusätzliches Token eingeben, das per E-Mail, SMS o. Ä. an eine vorher verifizierte Adresse gesendet wird.

Zur Berechnung des Risikolevels könnten die Zeit seit dem letzten Login, der Standort im Vergleich zum letzten Login, Uhrzeit, IP-Adresse, Browserversion, Tippverhalten bei der Eingabe des Passwortes oder andere Merkmale verwendet werden.

Die Akzeptanz von RBA ist bei den Nutzern wesentlich höher als eine Zwei-Faktor-Authentifizierung (2FA), da sie im Normalfall nur das Passwort eingeben müssen. Eine Zwei-Faktor-Authentifizierung wird i. d. R. nur bei hohen Sicherheitsanforderungen akzeptiert.

RBA ist bei vielen großen Plattformen (Google, Amazon, PayPal, LinkedIn usw.) und auch bei Projekten wie Mastodon im Hintergrund aktiv, wenn man eine Adresse für die Verifikation angibt. Implikationen für die Privatsphäre muss man gegen den Sicherheitsgewinn abwägen. Wenn man Zwei-Faktor-Authentifizierung verwendet, wird RBA meist deaktiviert.

RBA wird häufig *eine Art Zwei-Faktor-Authentifizierung* genannt, was aber nicht ganz korrekt ist. Man muss nicht den physischen Besitz eines Gerätes nachweisen, wie bei 2FA

üblicherweise gefordert, sondern nur lesenden Zugriff auf eine Zieladresse, an die das Token gesendet wird. Die Sicherheit ist also geringer als bei 2FA.

Authentifizierung durch Besitz: Man muss nachweisen, dass man ein besonderes bzw. individuell konfiguriertes *Token* besitzt, das ein Angreifer nicht besitzen kann. Dabei unterscheidet man zwei Formen:

- *Harter Besitz* ist ein physisch vorhandenes, individuell konfiguriertes *Token*, welches nicht kopierbar ist (Yubikey, FIDO2-Stick, ePA, NitroKey usw.);
- *Weicher Besitz* ist eine Anhäufung speziell konfigurierter Bits und Bytes, die evtl. auf einem anderen Gerät gespeichert, aber prinzipiell kopierbar sind (z. B. OTP-Apps oder X509-Zertifikate).

Im Consumer-Bereich wird am häufigsten OTP (One-Time-Passwörter) mit Smartphone-Apps oder Hardware-Token angeboten. OTP schützt gegen Keylogger und Mitleser unter den Bedingungen der Videoüberwachung. Es schützt nicht(!) bei Einbrüchen auf dem Server. Da bei OTP von Server und Client der gleiche Algorithmus ausgeführt wird, könnte ein Angreifer bei erfolgreichem Einbruch auf dem Server die Parameter auslesen und clonen.

Die modernere Variante ist WebAuthn/FIDO2 mit Public-Key-Kryptografie. Es wird nur ein Public-Key für die Authentifizierung auf dem Server gespeichert. Damit sind die Daten auch für einen Einbrecher wertlos. Allerdings wird WebAuthn/FIDO2 nur von wenigen Anbietern unterstützt. Die breite Einführung dauert noch etwas.

Die Verwendung von Zertifikaten gibt es eher bei Business-Anwendungen, Serveradministration (SSH) oder für hoheitliche Aufgaben (ePA).

Biometrische Merkmale (Fingerabdruck, Iris) sind für starke Authentifizierung eher ungeeignet, weil man sie bei einer Kompromittierung nicht ändern kann.

Im privaten Bereich bieten viele moderne Smartphones inzwischen die Freigabe des Sperrbildschirms via Fingerabdruck-Scan. In diesem Fall würde ich die Verwendung des Fingerabdrucks gegenüber der oft üblichen Wischgeste bevorzugen, da man die Wischgeste leicht beobachten und kann, während der Fingerabdruck sehr viel komplizierter zu faken ist.

Prinzipiell ist es aber möglich, einen Fingerabdruck zu fälschen, wenn sich der Aufwand für ein *High Value Target* lohnt. Auf dem 31C3 demonstrierte Starbug, wie er den Fingerabdruck von Frau v. d. Leyen und den Iris-Scan von Bundeskanzlerin Merkel mit einem hochauflösenden Kameraobjektiv während einer Pressekonferenz kompromittierte. Der Fingerabdruck von W. Schäuble wurde vom CCC ebenfalls kompromittiert und in einer PR-Aktion publiziert, um die Schwächen biometrischer Merkmale für die Authentifizierung zu zeigen.

7.1 Hinweise für Passwörter

Jeder kennt das Problem mit den Passwörtern. Es sollen starke Passwörter sein, sie sollen für jede Site unterschiedlich sein und außerdem soll man sich das alles auch noch merken und auf keinen Fall auf einem Zettel „speichern“.

Was ist ein starkes Passwort?

Diese Frage muss man unter Beachtung des aktuellen Stands der Technik beantworten. Wörterbuchangriffe sind ein alter Hut. Das Passwort darf kein Wort aus einem Wörterbuch wie z. B.

dem Duden sein, denn solche Passwörter sind einfach zu knacken. Für zufällige Kombinationen aus Buchstaben, Zahlen und Sonderzeichen kann man Cloud-Computing für Brute-Force-Angriffe nutzen. Dabei werden alle möglichen Kombinationen durchprobiert.

Ein sechsstelliges Passwort zu knacken, kostet 0,10 Euro. Eine 8-stellige Kombination hat man mit 300 Euro wahrscheinlich und mit weniger als 800 Euro sicher geknackt. Um eine 15-stellige Kombination aus zufälligen Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen oder eine Diceware-Passphrase aus 6 Wörtern mit 50 % Wahrscheinlichkeit zu knacken, würde man viele, viele Jahre benötigen.

Für eine gute Passphrase zum Schutz wichtiger Accounts wie E-Mail, Bank-Account, Cloud-Speicher oder VPN-Zugängen sollte man mindestens 12 zufällige Zeichen verwenden (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) oder eine Diceware-Passphrase mit mindestens 5 Wörtern.

Wie findet man eine starke Passphrase?

Eine gute Passphrase muss eine wirklich zufällige Kombination von Zeichen oder Wörtern sein. Es gibt mathematisch begründete Verfahren, um starke Passwörter zu generieren:

- Passwortspeicher wie KeepasXC enthalten einen Generator für wirklich zufällige Zeichenkombinationen. Für eine gute Passphrase sind mindestens 65 Bit Entropie nötig.

Abbildung 7.1: KeepassXC Passwortgenerator

  Passwortspeicher sind die einzige brauchbare Methode für selten verwendete Passwörter, an die man sich nach einigen Wochen nicht mehr erinnern kann.

- Ein memorierbares Passwortsystem hat den Vorteil, dass man nicht von zusätzlichen Tools abhängig ist und bei einem Crash des Computers kein aktuelles Backup braucht. Allerdings sollte man diese Passwörter häufiger eingeben müssen, damit man sie nicht vergisst.

  Die Akronym-Methode leitet den festen Teil aus den Anfangsbuchstaben der Wörter eines leicht merkbaren Satzes ab und den variablen Anteil aus der Verwendung:

  – Merksatz: *Die Sonne schien am ganzen Sonntag nur für uns.*
  – Passwort für die Webseite Heise.de: *DSsagSn4u-HEIS*

  - Passwort für den Jabber Account: *DSsgaSn4u-XMPP*
  - ...

  Die Collage-Methode verwendet ein Wort in mehreren Übersetzungen und lässt die Vokale weg. Variable Anhängsel sind ebenfalls möglich:

  - *Ergebnis:Result=42* könnte folgendes Passwort ergeben: rgbns:Rslt=42
  - *Pferd?Horse!Cheval* könnte folgendes Passwort ergeben: Pfrd?Hrs!Chvl

- Beim Diceware-Verfahren werden zufällige Kombinationen aus Wörtern aus einer Liste statt zufälliger Zeichenkombinationen verwendet. Wortkombinationen kann man sich leichter merken als sinnlose Zeichenketten.

  Für den klassischen Weg zur Erstellung einer Diceware-Passphrase benötigt man eine Wortliste (bspw. die *DeReKo Liste*[1] mit den häufigsten deutschen Wörtern laut Leibnitz-Institut) und einen Würfel. Für jedes Wort würfelt man fünf Mal und erhält damit eine Zahlenkombination. Diese Kombination sucht man in der Wortliste und wiederholt den Vorgang für 5–7 Wörter.

  ```
  26431 gebilde
  53612 schmal
  42221 macht
  66123 zauber
  34641 karwoche
  ```

  Ein Sonderzeichen zur Worttrennung kann man sich aussuchen. Und die gewürfelte Diceware-Passphrase ist dann: *gebilde-schmal-macht-zauber-karwoche*.

  Wenn man keine Würfel im Haushalt findet, könnte man auch online würfeln.[2]

Passwörter NICHT mehrfach verwenden

- Der Hack von ANONYMOUS gegen HBGary zeigte, dass es ein erhebliches Risiko ist, die gleichen Passwörter mehrfach zu verwenden. Den Aktivisten von ANONYMOUS gelang es, Zugang zur User-Datenbank des Content-Management-Systems der Website zu erlangen. Die gleichen Passwörter wurden vom Führungspersonal für weitere Dienste genutzt: E-Mail, Twitter, Linked-In usw. Die veröffentlichten 60.000 E-Mails waren peinlich für HBGary.[3]

- Im Sommer 2018 kursierten mehrere tausend Login-Daten (Benutzername, Passwort) für den Dienst MEGA in den einschlägigen Darknet-Foren. Die Login-Credentials stammten nicht aus einem Hack von MEGA sondern wurden durch automatisiertes Ausprobieren von Benutzername-Passwort-Kombinationen aus anderen erfolgreichen Hacks ermittelt. Gegen dieses **Credential-Stuffing** kann man sich nur schützen, indem man unterschiedliche Passwörter für verschiedene Dienste verwendet.

[1] https://www.privacy-handbuch.de/download/diceware-dereko.txt
[2] https://online-wuerfel.de/5-wuerfel
[3] https://www.heise.de/ct/artikel/Ausgelacht-1195082.html

7.1.1 Firefox build-in Passwortspeicher

Wie alle anderen Browser hat auch Firefox einen Login-Manager. Wenn man auf einer Webseite Login-Credentials eingibt, fragt Firefox standardmäßig, ob er die Zugangsdaten für diese Webseite speichern soll. Zukünftig wird dann beim nächsten Aufruf der Webseite das Login-Formular automatisch mit den passenden Daten ausgefüllt.

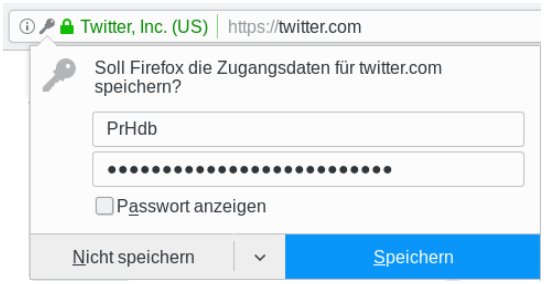


Abbildung 7.2: Login-Credentials für eine Webseite in Firefox speichern

Wenn man in der Konfiguration ein Master-Passwort setzt, werden die Passwörter (nur die Passwörter, nicht die Webseiten und Usernamen) mit AES verschlüsselt.

Risiken bei der Nutzung des Passwortspeichers im Browser

1. Einige Trackingdienste exploiten die Build-in-Passwortspeicher von Browsern, indem ihre Trackingscripte ein verdecktes Login-Formular generieren. Wenn der Surfer einen Account bei der Webseite hat, werden die Formulare vom Browser automatisch ausgefüllt. Trackingscripte interessieren sich für den Usernamen. Ein MD5-Hash des Usernamens wird dann als nicht löschbare, eindeutige Tracking-ID genutzt.

   Die Studie *Web trackers exploit browser login managers* hat 1.110 Webseiten gefunden, bei denen diese Trackingtechnik in-the-wild eingesetzt wird.[4]

2. Mit XSS-Angriffen können ebenfalls verdeckte Login-Formulare generiert werden, die vom Browser automatisch ausgefüllt werden, wenn man einen Account für diese Webseite hat. Das Konzept ist das gleiche wie bei den Trackingdiensten. Allerdings muss der Angreifer sein Script ohne Unterstützung des Webmasters in die Webseite hinein manipulieren. Außerdem wollen diese Angreifer nicht nur den Usernamen als eindeutige Tracking ID verwenden sondern auch das Passwort abgreifen.

3. Es gibt seit Jahren immer wieder Viren und Trojaner, die es gezielt auf die Passwortdatenbank von Firefox abgesehen haben und diese Datenbank zu ihrem Master of Control senden. Deshalb sollten die Passwörter unbedingt mit einem Master-Passwort gesichert werden. Das schützt die Passwörter, der Angreifer erhält aber trotzdem die Informationen, welche Accounts das Opfer auf welchen Webseiten nutzt.

Anpassungen für die Firefox-Konfiguration

- Wer kompromisslos auf strenge Privatsphäre Wert legt, kann den Passwortspeicher von Firefox deaktivieren und memorisierbare Passwörter oder externe Passwortspeicher wie Kee-

[4] https://freedom-to-tinker.com/2017/12/27/no-boundaries-for-user-identities-web-trackers-exploit-browser-login-managers/

PassXC verwenden. Zur Deaktivierung des Passwortspeichers setzt man unter *about:config* folgenden Wert:

```
signon.rememberSignons = false
```

- Wer man es etwas moderater bevorzugt und den Built-in-Passwortspeicher verwenden möchte, kann man das Risiko verringern, indem man das automatische Ausfüllen von Formularen deaktiviert. Dann muss man die ersten Buchstaben des Usernamens in das Formular schreiben und kann in dem sich öffnenden Drop-Down Menü mit einem Mausklick den Usernamen und das Passwort übernehmen.

```
signon.rememberSignons = true
signon.autofillForms   = false
```

7.1.2 Passwortspeicher

Passwortspeicher sind kleine Tools, die Username-Passwort-Kombinationen und weitere Informationen zu verschiedenen Accounts in einer verschlüsselten Datenbank verwalten. Es gibt mehrere Gründe, die für die Verwendung eines Passwortspeichers sprechen:

- Im Gegensatz zum Firefox-Build-in-Speicher werden alle Informationen verschlüsselt gespeichert, nicht nur die Passwörter.
- Viele Programme (z. B. Pidgin) speichern Passwörter unverschlüsselt auf der Festplatte, wenn man die Option zur Speicherung der Passwörter nutzt (nicht empfohlen!). Andere Programme bieten keine Möglichkeit zur Speicherung von Passwörtern, fordern aber die Nutzung einer möglichst langen, sicheren Passphrase.
- Bei vielen Accounts muss man sich neben Username und Passwort weitere Informationen merken wie z. B. die Antwort auf eine Security-Frage oder PINs bei Bezahldienstleistern.
- In der Regel enthalten Passwortspeicher einen Passwortgenerator, der wirklich zufällige und starke Passwörter generieren kann.
- Das Backup wird deutlich vereinfacht. Man muss nur die verschlüsselte Datenbank auf ein externes Backup-Medium kopieren.

Es gibt Passwortmanager, die die gespeicherten Login Credentials in die Cloud schieben, damit man einfach von unterschiedlichen Geräten darauf zureifen kann. Natürlich sind die Daten sicher verschlüsselte (behaupten die Anbieter). Diese Cloud-Passwortspeicher sind immer wieder Ziel von erfogreichen Angriffen wie *Passwort-Manager von Click Studios gehackt* (2021) oder *NortonLifeLock Passwortmanager gefährdet - Nutzer sollten handeln* (2022) und manchmal stellt sich heraus, dass die Daten möglicherweise doch nicht so ganz sicher verschlüsselt waren, wie beim Zugriff auf die Passworttresore der Kunden bei LastPass (2022).[5] [6] [7]

[5] https://www.heise.de/news/Passwordstate-Passwort-Manager-von-Click-Studios-gehackt-6027188.html

[6] https://www.heise.de/news/NortonLifeLock-Hersteller-warnt-vor-potenziell-geknackten-Passwortmanagern-7459886.html

[7] https://www.heise.de/news/Passwortmanager-LastPass-Hacker-haben-Zugriff-auf-Kennworttresore-von-Kunden-7441929.html

Mir gefällt **KeePassXC** (Windows, MacOS, Ubuntu 18.04+, Fedora 28+) sehr gut. KeePassXC ist eine Weiterentwicklung der Community von KeepassX. Für Smartphones gibt es KeePassDX (Android) oder StrongPass (iPhone), die die Datenbanken von KeePassXC nutzen können.

Neben der Übergabe der Passwörter via Zwischenablage (die u.U. unsicher ist) kann KeePassXC sichere Möglichkeiten nutzen, um die Login Credentials in Formularen einzugeben:

- Mit der AutoType Funktion simuliert KeePassXC eine virtuelle Tastatur und kann die Login Credentials direkt im Browserformular eingeben ohne die Zwischenablage zu benutzen.
- Mit dem Add-on KeePassXC-Browser[8] für Firefox stellt der Browser eine direkte Verbindung zu KeePassXC her und kann auch Einträge in die Datenbank schreiben.

  Bei dieser Integration wird auch die URL der Seite überprüft und damit verhindert, dass die Login Credentials auf einer Phishingseite eingegeben werden.

  Damit sich das Add-on mit einer KeepassXC Datenbank verbinden kann, muss man in den Einstellungen von KeePassXC die Browserintergration aktivieren.

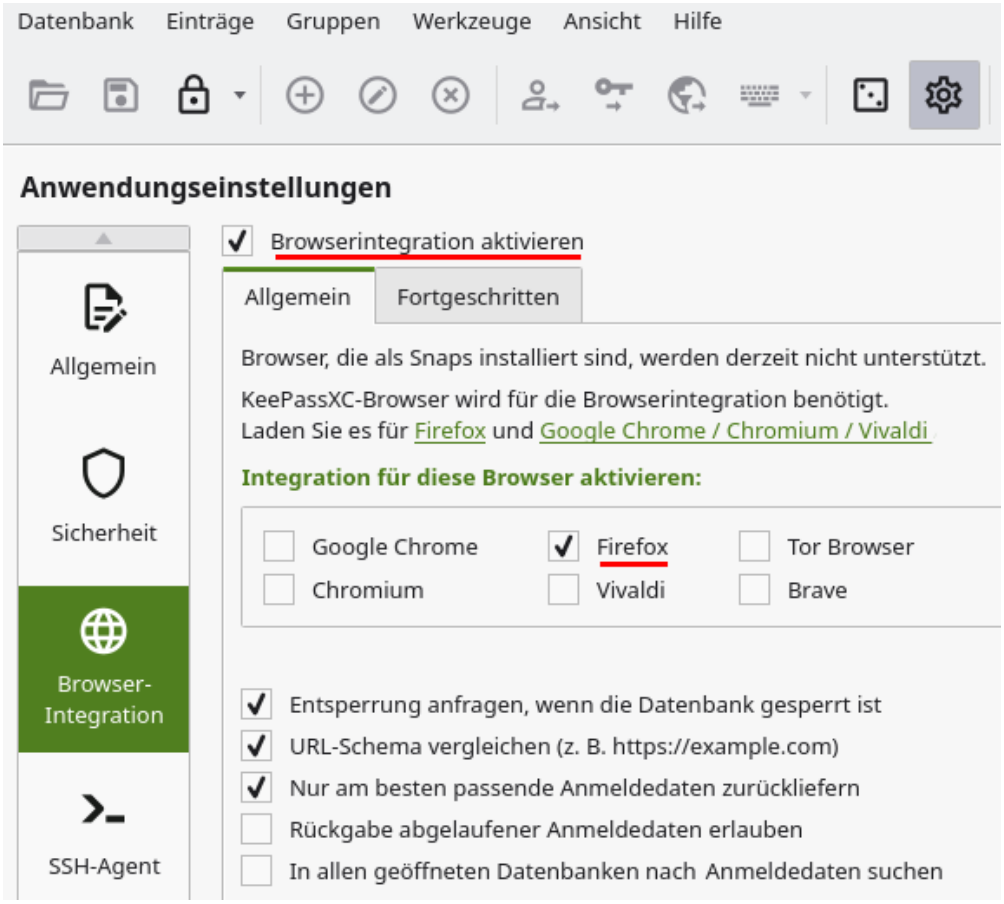


Abbildung 7.3: KeepassXC: Browserintergration aktivieren

- KeePassXC Version 2.7.7+ kann Kombination mit dem Browser Add-on KeePassXC-Browser in Firefox, Google Chrome oder Edge auch die Speicherung von Passkeys übernehmen. Somit muss man seine Passkeys nicht in die Google oder Apple Cloud schicken sondern kann sie in einer lokalen Datenbank verwalten, die man selbst kontrolliert.

[8] https://addons.mozilla.org/de/firefox/addon/keepassxc-browser/

(Damit hat man aber auch die Verantwortung für das Backup und Sync auf andere Geräte!)

Um Passkeys in KeePassXC speichern zu können, muss man in den Einstellungen im Browser Add-on die Unterstützung für Passkeys aktivieren (standardmäßig deaktiviert).

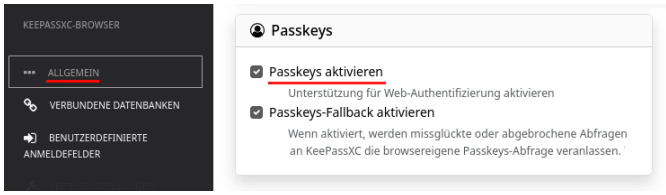


Abbildung 7.4: Passkey Unterstützung im Add-on KeePass-Browser aktivieren

Wenn man neue Passkeys in KeePassXC speichern möchte, muss man den Anleitungen für FIDO2 Token als Passkey Speicher folgen (bei einem Google Account *Passkey erstellen* → *Anderes Gerät verwenden* wählen und nicht *Passkey erstellen* → *Weiter*).

Die Passkeys findet man in der KeepasXC Datenbank nicht in den hierachischen sortierten Listen der Passwörter sondern unter dem Menüpunkt *Datenbank* → *Passkeys*.

Bei intensiver Nutzung von KeePassXC ist es hilfreich, die Anwendung beim Login automatisch zu starten, damit es verfügbar ist. Wenn die Datenbank im Hintergrund gesperrt ist, kann man sie mit einem Klick auf das KeepassXC Icon in der Toolbar des Browsers oder im Eingabeformular entsperren ohne in das Hauptfenster von KeePassXC wechseln zu müssen.

Warnung: Zwischenablage für Linux-Desktops

Die Linux-Desktops wie KDE, Gnome oder XFCE enthalten Tools zur Verwaltung der Zwischenablage. Diese Tools speichern die letzten(n) Einträge, die in die Zwischenablage kopiert wurden, und schreiben diese Einträge in der Standardkonfiguration meist unverschlüsselt auf die Festlatte.

- Klipper (KDE Desktop) speichert die Daten in *$HOME/.kde/share/apps/klipper/history2.lst*.
- Clipman (XFCE Desktop) speichert die Daten *$HOME/.cache/xfce4/clipman/textsrc*.

Wenn man Passwortmanager wie KeepassX verwendet und die Passwörter wie vorgesehen via Zwischenablage kopiert, dann landen auch diese sensiblen Informationen unter Umständen unverschlüsselt auf der Festplatte und die verschlüsselte Speicherung in der Passwortdatenbank wird sinnlos. Um diese Lücke zu vermeiden, müssen die Tools zur Verwaltung der Zwischenablage vernünftig konfiguriert werden. Sie sollten nur wenige Einträge speichern und auf keinen Fall Daten unverschlüsselt auf die Festplatte schreiben oder nicht automatisch gestartet werden, wenn die Speicherung nicht deaktivierbar ist.

Als Beispiel zeigt Abb. 7.5 die Konfiguration für die KDE-Zwischenablage Klipper und Abb. 7.6 zeigt, wie man den automatischen Start der Verwaltung der Zwischenablage Clipman in den XFCE-Einstellungen für Sitzung und Startverhalten deaktiviert.

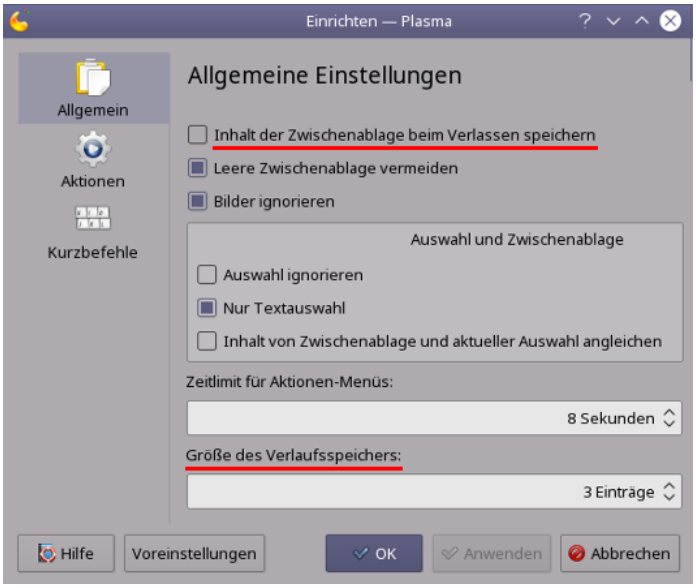


Abbildung 7.5: Konfiguration der KDE-Zwischenablage Klipper

7.2 Zwei-Faktor-Authentifizierung

Einige Webdienste bieten Zwei-Faktor-Authentifizierung (2FA) als Alternative zum einfachen Login mit Username/Passwort an. Die Webseite http://www.dongleauth.info/ bietet eine Übersicht zu Webdiensten, die OTP oder U2F für den sicheren Login unterstützen.

Bei der Zwei-Faktor-Authentifizierung muss man als ersten Faktor in der Regel ein Wissen nachweisen (Passwort, PIN) und als zweiten Faktor den Besitz eines kleinen Gerätes (OTP-Generator o. Ä.) oder einer Chipkarte wie bei Bankaccounts. Das Verfahren ist durch Nutzung von EC- und Kreditkarten jedem bekannt. Im Internet verwendet man statt Chipkarte meist One-Time-Passwort-Generatoren oder Security-Sticks (U2F, WebAuthn).

Wenn ein Angreifer durch Phishing, Videoüberwachung oder mit einem Keylogger den Usernamen und das Passwort für einen Account erbeutet, dann sollte es ohne den zweiten Faktor wertlos und nicht nutzbar sein. Das Passwort wird damit nicht überflüssig, es muss aber kein hochkomplexes, sicheres Passwort mehr sein. Eine 6-stellige Zahlenkombination ist nach NIST Special Publication 800-63B ausreichend.

2-Faktor-Authentifizierung für das Online Banking

Mit der europäischen Zahlungsrichtlinie PSD2 wird für die Online-Abwicklung von Bankgeschäften die Zwei-Faktor-Authentifizierung auch für den Login bei Webseiten zur Zahlungsabwicklung zwingend vorgeschrieben. Banken haben unterschiedliche Lösungen entwickelt, die sich von den üblichen Möglichkeiten für Zwei-Faktor-Authentifizierung bei anderen Webdiensten unterscheiden. Sie verwenden in der Regel einen TAN-Generator als zweiten Faktor und definieren den Geschäftsfall *Login*, da die Technik für die Autorisierung von Transaktionen vorhanden ist.

chipTAN, Sm@rt-TAN verwenden Hardware-TAN-Generatoren, welche die EC-Chipkarte der Bank für die Generierung einer TAN verwenden. Sie sind für hohe Sicherheitsanforderungen geeignet, da sie ein separates Gerät verwenden, das nicht mit dem Internet verbunden ist. Die Daten für die Generierung einer TAN können entweder optisch zwischen PC und

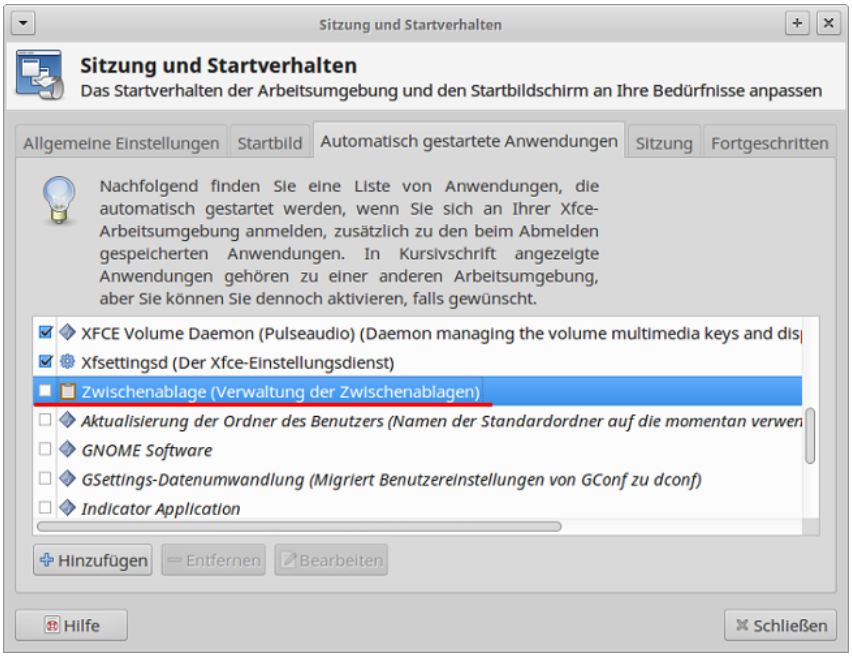


Abbildung 7.6: Starten von Clipman deaktivieren (XFCE Desktop)

TAN-Generator übertragen werden (durch Scannen eines Code, der auf dem Bildschirm angezeigt wird) oder manuelle Eingabe.

photoTAN, SecureGo verwenden Smartphone Apps für die Generierung einer TAN. Die Verfahren sind für den Kunden billiger, da er kein zusätzliches Gerät kaufen muss. Sie sind aber weniger sicher, da ein Smartphone leichter kompromittiert werden kann.

Außerdem enthalten Smartphone-Apps immer wieder unterschiedliche Tracker, die das Nutzungsverhalten verfolgen. Die *SecureGo-App* der Fiducica & GAT IT AG enthält zwei Tracker, unter anderem Google Firebase Analytics. Ein positives Beispiel ist die *photoTAN-App* der Commerzbank, die keine Tracker enthält.

Welche Optionen man hat, muss man beim Kundensupport der Bank erfragen. Auch wenn es etwas umständlicher ist, würde ich beim Umgang mit Geld immer die sicherste Lösung bevorzugen und Hardware-TAN-Generatoren in Kombination mit meiner EC-Chipkarte nutzen.

2-Faktor-Authentifizierung für Webdienste

Für den Login bei Webdiensten werden für die Zwei-Faktor-Authentifizierung andere Verfahren genutzt als beim Online-Banking:

OTP: Bei der Zwei-Faktor-Authentifizierung mit zusätzlichem One-Time-Passwort besteht das Passwort aus zwei Komponenten, die nacheinander oder manchmal auch zusammen in das gleiche Passwortfeld eingegeben werden müssen. Der erste Teil ist üblicherweise eine n-stellige PIN, die man wissen muss. Der zweite Teil ist das One-Time-Passwort. Es wird von einem kleinen Spielzeug (Tokengenerator) geliefert und ist nur einmalig verwendbar.

Es gibt mehrere Verfahren für die Zwei-Faktor-Authentifizierung mit OTP:

- **HOTP** (HMAC-based OTP) nutzt One-Time-Passwörter, die aus einem HMAC-SHA1-Hashwert abgeleitet werden, der aus einem Zähler und einem gemeinsam Secret berechnet wurde. Sie sind beliebig lange gültig, aber die Verwendung eines Token mit größerem Zählerwert erklärt auch alle Token mit niedrigerem Counter für ungültig.

  Tipp: Wenn man seinen OTP-Generator nicht in den Urlaub o. Ä. mitnehmen möchte, kann man sich eine Liste von HOTP-Token generieren lassen und diese Zahlenkombinationen nacheinander zum Login unterwegs verwenden. Außerdem ist es schwieriger, ein HOTP-Token zu klonen, ohne entdeckt zu werden.

- **TOTP** (Time-based OTP) nutzt One-Time-Passwörter, die auf Basis der aktuellen Uhrzeit berechnet werden und nur innerhalb einer kurzen Zeitspanne einmalig verwendet werden können.

  Die HOTP- oder TOTP-Passwörter können von einem Hardware-Token (z. B. *Nitrokey Pro* mit der Nitrokey-App) generiert werden oder mit einer Smartphone-App (*FreeOTP* für Android oder *OTP Auth App* für iPhone). Wenn ein Smartphone genutzt wird, muss man die angezeigte Zahlenkombination per Hand in das Login-Formular abtippen. Bei der Verwendung von TOTP hat man dafür 30 bzw. 60 Sekunden Zeit.

- **YubicoOTP** ist ein proprietäres Protokoll der Firma Yubico. Es wird ein USB-Stick genutzt, der sich wie eine Tastatur verhält. Man aktiviert das Passwortfeld und drückt dann eine Taste auf dem USB-Stick. Damit wird das One-Time-Passwort in das Eingabefeld geschrieben und man kann das Formular abschicken. Neben dem einfachen Yubico Stick gibt es den Yubico NEO, der auch als OpenPGP-Smartcard und als U2F-SecurityStick genutzt werden kann.

  Der Webdienst, bei dem man sich anmeldet, sendet das Einmal-Passwort i. d. R. über eine API an die YubiCloud und lässt es dort verifizieren. Nur wenige Webdienste bieten gebrandete Yubikeys und betreiben einen eigenen Server zur Validierung. Bezüglich Schutz gegen Phishing gilt das Gleiche wie für TOTP/HOTP.

Zwei-Faktor-Authentifizierung mit One-Time-Passwörtern (OTP) erschwert Phishing-Angriffe. Das ist das Angreifermodell, und nur dagegen bietet OTP verbesserten Schutz. OTP macht Phishing-Angriffe aber nicht unmöglich. Bruce Schneier hat in der Theorie bereits 2009 darauf hingewiesen. Im Jahr 2018 haben potente Hacker begonnen, Zwei-Faktor-Authentifizierung mit OTP in größerem Umfang auszutricksen.

Angriffe auf 2-Faktor-Authentifizierung mit OTP Token:

- Die Sicherheitsfirma CERTFA berichtete Dezember 2018 in einem Blog-Artikel von einer Spear-Phishing-Kampagne iranischer Hacker gegen Google- und Yahoo!-Accounts, welche die Zwei-Faktor Authentifizierung austricksen konnte.[9]
- Amnesty International berichtete ebenfalls von einer Phishing-Angriffswelle aus Nahost gegen die Accounts von Aktivisten, welche die Zwei-Faktor-Authentifizierung von ProtonMail, Tutanota, Google und Yahoo! austricksen konnte.[10]
- Auf Github findet man Muraena/NecroBrowser[11] oder evilginx2[12] als Open Source, die Phishing-Angriffe auf Zwei-Faktor-Authentifizierung mit OTP automatisiert ausführen können. Der Angreifer lockt das Opfer mit Phishing-E-Mails o. Ä. zum Login auf seine Webseite. Dort arbeitet ein Reverse-Proxy, der sich unbemerkt zwischen Nutzer und Webdienst einschleicht und die Authentifizierung an den richtigen Server weiterleitet.

[9] https://blog.certfa.com/posts/the-return-of-the-charming-kitten/
[10] https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/
[11] https://github.com/muraenateam
[12] https://github.com/kgretzky/evilginx2

Nachdem die Session aufgebaut wurde, extrahiert der Reverse-Proxy die Session-Cookies und reicht sie an einen Browsers weiter. Das Schließen der Session (Logout) wird blockiert und dem Nutzer wird vorgegaukelt, er hätte sich abgemeldet. Danach kann der Angreifer mit den geklauten Session-Cookies im eigenen Browser unbemerkt den Account übernehmen.

- Wenn es einem Angreifer gelingt, zwei oder mehr TOTP-Token abzugreifen und den Zeitpunkt der Verwendung zu protokollieren, kann er mit dem Tool *hashcat* versuchen, die Secret-Keys ermitteln und dann selbst gültige TOTP-Token erzeugen.

  1. Die abgeschorchelten Token schreibt man zusammen mit dem Zeitstempel im Format in eine Textdatei (in diesem Beispiel: *inputs.txt*):

     ```
     833060:1263384780
     549115:1528848780
     ```

  2. Mit dieser Datei füttert man *hashcat* und protokolliert die Ergebnisse:

     ```
     > hashcat -m17300 -a3 -o totp.potfile inputs.txt
     ↪  ?l?l?l?l?l?l?l
     ```

  3. Nach einigen Stunden oder Tagen Rechenzeit (abhängig von Rechenleistung und Qualität der Keys) schaut man sich die Ergebnisse an:

     ```
     > cut -d: -f3 totp.potfile | sort | uniq -c | sort -nr | head
     ```

     Die Ergebnisliste kann man von oben beginnend ausprobieren. Nach weiteren fünf Minuten hat man einen TOTP-Secret-Key, der die Generierung gültiger Token ermöglicht, und man kann den Account übernehmen:

     ```
     > oauthtool --base32 --totp "Secret Key" -d 6
     ```

- OTP schützt nicht bei Einbrüchen auf dem Server. Da bei OTP der Server und der Client den gleichen Algorithmus zur Berechnung und Verifizierung des One-Time-Passworts ausführen, kann ein Angreifer bei einem erfolgreichen Einbruch auf dem Server die OTP-Parameter auslesen und somit gültige OTP-Token berechnen. Insbesondere für TOTP ist es einfach, dabei unentdeckt zu bleiben:

  ```
  > oauthtool --base32 --totp <Secret Key> -d 6
  ```

  Aus dem gleichen Grund schützt Zwei-Faktor-Authentifizierung mit OTP nicht beim Zugriff staatlicher Behörden auf Passwort-Hashes, wie es in dem im Februar 2020 von der Regierung beschlossenen *Gesetz zur Bekämpfung von Rechtsterrorismus und Hasskriminalität*[13] vorgesehen ist. Und das schließt die Parameter zur Berechnung der OTP ein. Gegen diesen Angriff ist ausschließlich die Stärke des ersten Faktors (Passwort) und das Hash-Verfahren relevant, welches der Provider zum Schutz des gespeicherten Passwortes einsetzt.

FIDO-U2F: ist ein kryptografisches Private/Public-Key-Verfahren zur Authentifizierung mit einem kleinen SecurityStick (z. B. *Nitrokey U2F*[14] oder verschiedene *Yubikeys*[15]), das im Oktober 2014 standardisiert wurde.

Das Verfahren läuft im Hintergrund automatisch ab, man muss nur den U2F-Stick vor dem Login anschließen. Der Server sendet ein zufälliges Challenge an den Client (Browser). Der Browser gibt diesen Input zusammen mit der Login-URL, die er sieht, an den U2F-Stick weiter, der mit einem geheimen Schlüssel eine Signatur über diese Daten berechnet.

[13] https://www.golem.de/news/hasskriminalitaet-regierung-will-passwortverschluesselung-nicht-aushebeln-2002-146727.html
[14] https://www.nitrokey.com/de
[15] https://www.yubico.com/products/yubikey-hardware/

Diese Signatur wird als Response an den Server zurückgeschickt und kann dort mit dem passenden Public-Key verifiziert werden. Dabei wird für jeden Web-Account ein anderer Key verwendet.

Vorteile von FIDO-U2F gegenüber One-Time-Passwörtern:

1. Da asymmetrische Kryptografie genutzt wird, kennt der Server nur einen Public-Key. Wenn ein Angreifer den Server kompromittiert, kann er die U2F-Authentifizierung nicht aushebeln.
2. Da die Login-URL, die der Browser sieht, in die Berechnung der Signatur einfließt, schützt U2F auch gegen alle Angriffe mit Phishing-Webseiten. Um Software wie Muraena + NecroBrowser gegen FIOD-U2F-Authentifizierung einzusetzen, müsste der Angreifer die TLS-Verschlüsselung knacken und sich als *Man-in-the-Middle* in die TLS-verschlüsselte Kommunikation zwischen Browser und Webdienst einklinken.

WebAuthn/FIDO2 ist ein Standard des W3C, der im März 2019 verabschiedet wurde und von den Großen der IT-Branche unterstützt wird. WebAuthn ist eine Weiterentwicklung von FIDO-U2F und soll den Login mit Username und Passwort komplett ersetzen können.

Das Protokoll nutzt asymmetrische Kryptografie ähnlich wie FIDO-U2F und verwendet gleichfalls Security-Token. Es können FIDO2-USB-Sticks oder das Trustet Platform Module des Computers (TPM) verwendet werden, um die privaten Keys zu speichern. Außerdem ist WebAuthn/FIDO2 kompatibel mit FIDO-U2F.

WebAuthn/FIDO2 erweitert FIDO-U2F um folgende Punkte:

1. Die User-ID (Username) wird ebenfalls auf dem Security Token gespeichert und könnte beim Login automatisch an den Server gesendet werden. Man könnte auf die Eingabe des Usernames im Login Formular verzichten.
2. Außerdem kann man den Zugriff auf das Security-Token mit einer PIN bzw. einem Passwort zu sichern. Damit wird der erste Faktor der Authentifizierung (Wissen) lokal beim Nutzer überprüft und müsste nicht mehr durch den Server validiert werden.

   Dafür müsste der Anwender bei einem neu gekauften FIDO2 Token aber zuerst mal selbst eine PIN setzen (mindestens 6-stellig, empfehlen BSI und NIST).

   - Mäuschenschubser können dafür den Browser Google Chrome (oder Chromium) nutzen. In den Einstellungen unter *Datenschutz & Sicherheit* → *Sicherheit* → *Sicherheitsschlüssel verwalten* kann man die PIN für den/die FIDO2 Token konfigurieren.
   - Für echte Linuxer gibt es das Paket *fido2-tools*, das man mit der Paketverwaltung installieren kann. Die PIN setzt man dann mit folgendem Kommando:

     ```
     > fido2-token -S /dev/hidraw1
     ```

     Mit folgendem Kommando kann man die PIN später bei Bedarf ändern:

     ```
     > fido2-token -C /dev/hidraw1
     ```

   Die Passworteingabe auf der Webseite könnte damit ganz entfallen. Aus Gründen der Kompatibilität mit FIDO-U2F wird dieses Feature leider nicht oft genutzt.

Auf der Webseite https://webauth.io kann man spielerisch mit seinem Token einen Account erstellen und sich mit dem Umgang beim Login vertraut machen.

Hinweis: Man sollte einkalkulieren, dass man ein FIDO2-Security-Token auch mal verlieren kann. Ohne dieses Token wird ein Reset des Passwort oder Rückfall auf Login nur mit

Username und Passwort nicht möglich sein. (Falls der Webdienst das anbietet, hat er 2FA nicht verstanden.) Man muss also mindestens zwei Token für einen Login registrieren!

Hinweis für Linuxer: Wenn FIDO2- oder U2F-Sticks nicht out-of-the-box funktionieren, muss man die UDEV Regeln installieren:

```
Ubuntu: > sudo apt install libu2f-udev
Fedora: > sudo dnf install u2f-hidraw-policy
```

Passkey wurde 2022 standardisiert und soll die Benutzbarkeit von WebAuthn/FIDO2 vereinfachen. Es wird die gleiche Kryptografie verwendet aber man benötigt nicht unbedingt ein Hardware Token wie bei FIDO2 (aber man kann FIDO2 Token nutzen). Die Schlüssel können auch auf einem Smartphone gespeichert und mit der Klaut (iCloud, Google Cloud) synchronisiert werden, um einen einfachen Gerätewechsel zu ermöglichen.

Wenn man das Smartphone wechselt, muss man das neue Phone nicht überall als neuen Authenticator registrieren (wie bei FIDO2 Token nötig), sondern kann die Schlüssel für die Authenfizierung aus der Cloud wiederherstellen und sofort das neue Phone für den Login verwenden. Das ist der große Vorteil gegenüber der Nutzung von FIDO2 Security Token.

Bei iPhones muss die 2-Faktor-Auth. für die iCloud aktiviert und bei Androids ein Google Account mit Cloud Synchronisierung eingerichtet sein, um Passkeys verwenden zu können!

Außerdem können Passwortdatenbanken wie KeePassXC für Passkeys genutzt werden, wenn der Browser mit dem passenden Add-on mit der Passwortdatenbank verkuppelt wird.

Auf der Testseite https://passkeys.io/ kann man das Verfahren testen und ein bisschen spielen, um sich mit dem Verfahren vertraut zu machen.

- Meistens wird ein Smartphone als Authentikator verwendet werden. Zur Registrierung des Smartphones als Passkey Authenticator oder später für den Login auf der Webseite scannt man den vom Browser gezeigten QR-Code mit dem Smartphone und authorisiert die Aktion auf dem Smartphone mit PIN Eingabe oder Fingerabdruckscan.

  Das smarte Phone sendet einen Auth.-Response zum Server und man ist drin.

  Wenn Passkey auf der Webseite richtig implementiert wurde, muss man keine E-Mail Addr. oder Account-ID angeben. Einfach nur *Login mit Passkey* anklicken + Scan.
- Alternativ kann man auch FIDO2 Token als Speicher verwenden, da beide kryptografisch kompatibel sind. Da Passkey zugunsten der Benutzbarkeit die Sicherheit aufweicht, bleibt es dem Anwender überlassen, den Zugriff auf das FIDO2 Security Token mit einer PIN zu schützen (wie, ist oben beschrieben) oder darauf zu verzichten.

  Man hat es richtig gemacht, wenn der Browser beim Login via Passkey nach der PIN für das FIDO2 Token fragt. Anderenfalls kann jeder Tunichgut, der das FIDO2 Token findet, beschlagnahmt oder irgendwie entwendet den Account übernehmen.

  Da Passkey mit Smartphone in Firefox für Linux oder MacOS noch nicht implementiert ist, muss man mit diesen Firefoxen FIDO2 Token für den Passkey Login verwenden.

Verwendet man den Browser Google Chrome auf dem PC und Android Phone als Passkey Authenticator, kann die Kopplung beim Login auch via Bluetooth erfolgen.

Bisher funktioniert die Synchronisierung der Passkeys nur zwischen Android Smartphones mit der Google Cloud oder mit iPhones und der iCloud aber nicht zwischen den Welten.

SMS: SMS-basierte Verfahren zur Authentifizierung gelten nicht mehr als sicher. Es gibt mehrere Publikationen zu dem Thema. Das NIST, BSI u. a. empfehlen, SMS nicht mehr für die Authentifizierung zu nutzen.[16]

SMS-basierte Verfahren können mit SIM-Swap-Angriffen oder SS7-Hijacking ausgehebelt werden. Das musste Twitter-CEO Jack Dorsey lernen, als sein Twitter-Account trotz aktivierter Zwei-Faktor-Authentifizierung kompromittiert wurde. Ein Fehler beim Mobilfunkanbieter sei schuld gewesen, erklärte Twitter später, was auf einen erfolgreichen SIM-Swap hindeuten könnte.

ePerso: In Auswertung des US-Wahlkampfes von 2016 und des erheblichen Einflusses von gehackten E-Mail-Accounts auf das Wahlverhalten der amerikanischen Bevölkerung hat die Bundesregierung die Cyber-Sicherheitsstrategien überarbeitet. Nach Ansicht der Bundesregierung ist die Sicherheit mit dem klassischen Benutzername/Passwort-Verfahren nicht mehr gegeben. Im Rahmen der Cyber-Sicherheitsstrategien will die Regierung die Bürger stärker zur Nutzung der Onlineausweisfunktion des Personalausweises animieren.

Bezüglich des klassischen Benutzername/Passwort-Verfahrens stimmen wir mit der Bundesregierung überein. Wir empfehlen aber die Onlineausweisfunktion des ePerso nicht. Stattdessen sollte man Hardware-Token nutzen, die nicht an eine ID-Karte gebunden und vollständig durch den Nutzer konfigurierbar sind.

7.3 Phishing-Angriffe

Phishing ist eine der Plagen im Internet. Der Lagebericht des BSI zur IT-Sicherheit von 2017 nennt diese Angriffe als zweitgrößte Gefahr nach den Erpressungstrojanern. Es gibt dabei ganz unterschiedliche Intentionen der Angreifer, um die Kontrolle über einen Account des anvisierten Opfers zu erlangen:

- Geheimdienste versuchen, die Accounts von politischen Oppositionellen zu hacken, um das Kontaktnetzwerk zu analysieren und die Kommunikation zu beobachten. Mit diesem Hintergrund wurden die Twitter-Accounts von Erdogan-Kritikern durch türkische Hacker angegriffen.
- Der *CEO-Hack* ist eine spezielle Version von Phishing-Angriffen, bei dem gezielt die E-Mail-Accounts von Führungspersonen in Firmen angegriffen werden. Dabei werden die Phishing-Mails optimal auf die Zielperson zugeschnitten. Ziel ist es, die E-Mail-Kommunikation zu beobachten und gezielt einzelne E-Mails wie z. B. Rechnungen zu manipulieren um Zahlungen auf andere Konten umzuleiten. B. Schneier beschreibt in seinem Blog ein Beispiel für einen erfolgreichen *CEO-Hack* gegen eine Galerie:[17]

  > Criminals hack into an art dealer's email account and monitor incoming and outgoing correspondence. When the gallery sends a PDF invoice to a client following a sale, the conversation is hijacked. Posing as the gallery, hackers send a duplicate, fraudulent invoice from the same gallery email address, with an accompanying message instructing the client to disregard the first invoice and instead wire payment to the account listed in the fraudulent document.
  >
  > Once money has been transferred to the criminals' account, the hackers move the money to avoid detection and then disappear. The same technique is used to intercept payments made by galleries to their artists and others.

[16] https://pages.nist.gov/800-63-3/sp800-63b.html
[17] https://www.schneier.com/blog/archives/2017/11/cybercriminals_.html

- Auch ganz normale, nicht exponierte Internetnutzer werden mit Phishing-Angriffen konfrontiert. Für Kriminelle ist dabei alles interessant, was mit Geld zu tun hat (z. B. PayPal.com, Amazon-Konten o. Ä.). Spammer versuchen, verifizierte E-Mail-Accounts zu kapern und das Adressbuch des Opfers zu nutzen, um dann bei Empfängern der Spam-Nachrichten das Vertrauen in den bekannten Absender auszunutzen. Dabei kann es manchmal zu kuriosen Missverständnissen kommen:

  > *My religious aunt asked why I was trying to sell her viagra!*

  In der Regel werden normale Internetnutzer mit Bulk-Phishing attackiert. Die Angreifer versenden eine E-Mail mit alarmierendem Inhalt an tausende Empfänger in der Hoffnung, dass ein kleiner Teil der Empfänger so naiv ist und auf den Link-Button in der Mail klickt, um die Login Credentials auf der Phishing Webseite einzugeben.

  Beispiele für den Inhalt von ganz normalen Phishing E-Mails:

  - *Das Passwort für Ihren Account wurde kompromittiert! Bitte loggen Sie sich sofort ein und ändern Sie ihr Passwort.*
  - *Ihr PayPal Account muss neu verifiziert werden, bitte loggen Sie sich hier ein und...*
  - *Ihr Amazon Konto wurde deaktiviert, bitte loggen Sie sich ein und...*
  - *Ihre Lieferung wurde storniert, weitere Informationen finden Sie hier.*

  Professionelle Phishing-Mails sind dem Design der originalen E-Mails sehr gut nachgemacht und für Laien schwer erkennbar. IT-Profis könnten sich die Header der Mails anschauen oder die Links genauer prüfen, aber das möchte man auch nicht für jede E-Mail ständig machen. Deshalb gibt es keine weitere Ratschläge für diesen Ansatz.

Schutz gegen Phishing-Angriffe

Als Schutz gegen Phishing-Angriffe empfehlen wir, Webseiten mit Formularen zur Eingabe von Login-Credentials IMMER über Lesezeichen oder durch Eingabe der URL per Hand zu öffnen. Man sollte NIE auf die Link Buttons in irgendwelchen E-Mails klicken, um Login-Seiten für Accounts aufzurufen. Dabei ist es egal, wie vertrauenswürdig eine Mail aussieht.

Es ist verführerisch einfach, schnell mal auf den Button oder Link zu klicken, wenn die Phishing-Mail gut gemacht ist. Aber es ist auch nicht viel komplizierter, ein Lesezeichen oder die URL aus einem Passwortmanager wie KeePassXC aufzurufen.

Außerdem kann man die Zwei-Faktor-Authentifizierung nutzen, wenn der Webdienst sie unterstützt. Das erschwert einfache, primitive Phishing-Angriffe. (Es gibt allerdings technisch ausgefeiltere Angriffe, die auch die Zwei-Faktor-Authentifizierung mit OTP aushebeln können.)

Abbildung 7.7: Beispiel für eine Phishing-Mail

Kapitel 8

Bezahlen im Netz

PayPal.com ist zweifellos der bekannteste Bezahldienstleister im Internet. Die Firma wurde von Peter Thiel gegründet, der u. a. den Datensammler Rapleaf.com aufgebaut hat. Als einer der Hauptinvestoren hat er die Entwicklung von Facebook maßgeblich mitbestimmt und gehört zum Steering-Committee der Bilderberg-Konferenzen. Das Credo von P. Thiel ist eine totale Personalisierung des Internets.

Die Nutzung von PayPal.com ist das Gegenteil von anonym. Bei jedem Zahlungsvorgang wird eine Verknüpfung von persönlichen Daten (E-Mail-Adresse, Kontoverbindung) und gekauften Waren hergestellt. Die Daten werden zum Monitoring der Überweisung an mehr als 100 Firmen übertragen.

PayPal.com nutzt seine Marktposition für die Durchsetzung politischer Interessen der USA. Gemäß der Embargo-Politik der USA werden Internetnutzer in über 60 Ländern ausgesperrt. Internationales Aufsehen erregte die Sperrung der Konten von Wikileaks. Daneben gibt es viele weitere Fälle. Mehr als 30 deutschen Online-Händlern wurden die Konten gesperrt[1], weil sie kubanische Produkte (Zigarren, Rum, Aschenbecher) in Deutschland anboten. Die Sperre wurde mit einem amerikanischen Handelsembargo gegen Kuba begründet, das für Europäer belanglos ist.

Aufgrund dieser politischen Instrumentalisierung hat ANONYMOUS zum Boykott von PayPal.com aufgerufen und an Nutzer appelliert, ihre Accounts bei diesem Bezahldienst zu kündigen.

Zukünftig möchte PayPal.com auch in der realen Welt präsent sein. Das Bezahlsystem soll in zwei Jahren die Geldbörse ersetzen, wie Ebay-Chef John Donahoe sagte, natürlich mit den üblichen Schnüffeleien:

> *Beim Einsatz von PayPal in den Geschäften könnten die Einzelhändler mehr über Vorlieben ihrer Kunden erfahren und sie entsprechend besser bedienen.*

Rechnung oder **Überweisung** (Vorkasse) sind datenschutzfreundliche Bezahlmethoden, da nur die beiden Kreditinstitute von Käufer und Verkäufer in den Bezahlprozess eingebunden sind. Außerdem sind es sichere Bezahlmethoden, die nicht durch (unzulässige) Speicherung von Daten kompromittiert werden können. Via Online-Banking ist es auch am PC nutzbar. Leider werden diese Methoden nicht überall angeboten.

Kreditkarten werden von einer Bank ausgegeben. Die Abwicklung des Bezahlvorgangs wird bei Visa und Mastercard aber von sogenannten Payment-Processors übernommen. Teilweise

[1] http://heise.de/-1320630

sammeln diese Payment-Processors Daten über Online- und Offline-Einkäufe und verkaufen die Daten an große Datensammler wie Acxiom oder BlueKai, wo sie mit anderen persönlichen Daten zusammengeführt werden.

Außerdem haben VISA und Mastercard selbst Programme zur Datensammlung, um Firmen anhand der Bezahlvorgänge bei der Auswertung von Werbekampagnen zu unterstützen. Die Kreditkartenfirma Mastercard demonstriert mit einem Patent (Dezember 2016), wie man sich die Monetarisierung des gesammelten Datenreichtums vorstellen könnte. In dem Patent wird beschrieben, wie die Kreditkartenfirmen aus den Einkäufen anhand der Konfektions- und Schuhgrößen die Größe und das Gewicht des Karteninhabers ermitteln können. Diese Daten könnten an Fluggesellschaften verkauft werden, die damit die Sitzverteilung für die Passagiere optimieren könnten.

Die Sicherheit von Kreditkarten als Zahlungsmittel wird öfters durch unsachgemäße Datenspeicherung beim Verkäufer oder einem Partner des Verkäufers kompromittiert. Eine dreistellige Prüfziffer soll den Missbrauch von Kreditkartennummern für unberechtigte Einkäufe zu Lasten des Karteninhabers verhindern. Wenn aber der Payment-Processor oder sein Sub-Contractor die Prüfziffer zusammen mit der Kartennummer dauerhaft speichert und die Datenbank unzureichend gesichert ist – dann haben Kunden möglicherweise ein Problem, z. B. Millionen Hotelgäste, die via Booking.com oder Expedia gebucht hatten.[2]

Virtuelle Kreditkarten werden inzwischen von vielen Geldinstituten angeboten. Wenn man bereits einen verifizierten Account bei dem Kreditinstitut hat, ist die Erstellung einer virtuellen Kreditkarte online mit wenigen Klicks erledigt. Man bekommt die Kartennummer, Ablaufdatum und Prüfziffer sofort digital zugestellt, aber keine Plastikkarte. In der Regel handelt es sich dabei um Debit-Karten, die man vor der ersten Verwendung erst mal aufladen muss.

Die Kosten für virtuelle Kreditkarten sind meist geringer als vergleichbare echte Kreditkarten vom gleichen Anbieter, aber sehr unterschiedlich. Bei KREDU kosten sie 149,- Euro pro Jahr + Zinsen für den Kredit, bei der Sparkasse 12,- Euro pro Jahr ...

Virtuelle Kreditkarten könnte man regelmäßig wechseln (z. B. jährlich) und damit einige Sicherheitsprobleme bei der Nutzung von Kreditkarten im Internet reduzieren. Außerdem erschwert man Datensammlern die Verknüpfung von Online- und Offline Aktivitäten, wenn man online und offline verschiedene Kreditkarten nutzt.

Disposable Virtual Cards werden von besonders innovativen Kreditinstituten angeboten. Bei diesen Kreditkarten ändern sich die Kartennummern automatisch. Nach jeder Transaktion wird eine neue Kartennummer generiert. Falls die Datenbanken der Online-Händler später von Hackern kompromittiert werden, sind alte Kreditkartennummern wertlos. Außerdem wird die Auswertung für Datensammler erschwert, da Einkäufe nicht anhand von Kreditkarten verknüpft werden können.

Die Schweizer Revolut bietet Disposable Virtual Cards für ihre Premiumkunden, ecoPayz bietet dieses Feature ab Silver Level, Eno von Capital One u. a. m.

Disposable Virtual Cards sind sicherer und datenschutzfreundlicher, aber nicht anonym.

Google Pay und **Amazon Pay** sind aus technischer Sicht ebenfalls Payment-Processors für Kreditkarten. In der Google-Datensch(m)utz Policy wird benannt, welche Daten bei Nutzung dieser Bezahlmethode gesammelt werden:

[2] https://www.golem.de/news/datenleck-daten-von-millionen-hotelgaesten-ungeschuetzt-im-netz-2011-152005.html

> *Bei jeder Transaktion über Google Pay können wir Informationen zur Transaktion erheben. Hierzu zählen: Datum, Uhrzeit und Betrag der Transaktion, Händlerstandort und -beschreibung, eine vom Verkäufer bereitgestellte Beschreibung der gekauften Waren oder Dienste, Fotos, die Sie der Transaktion beigefügt haben, der Name und die E-Mail-Adresse des Verkäufers und Käufers bzw. des Absenders und Empfängers, die verwendete Zahlungsmethode [...].*

Kein weiterer Kommentar nötig – ist ein ganz normaler Google-Service.

SOFORT-Überweisung ist ein Online-Zahlungssystem zur bargeldlosen Zahlung im Internet. Beim Bezahlvorgang stellt der Kunde dem Zahlungsdienstleister Sofort GmbH die notwendigen Credentials für den Online-Zugriff (PIN usw.) auf sein Konto zur Verfügung. Die Sofort GmbH nutzt diese Informationen, um sich Daten über Kontostand u. Ä. zu holen und danach die Transaktion auszuführen.

Würde man das Verfahren in die Offline-Welt übertragen, könnte man die Dienstleistung der SOFORT-Überweisung wie folgt beschreiben: Weil man selbst zu faul ist, gibt man einem Fremden auf der Straße die EC-Karte und PIN, damit er zum Bankautomaten geht und sich über den Kontostand und die letzten Transaktionen informiert, um danach die gewünschte Überweisung auszuführen.

In den AGBs verbieten es alle Banken und Sparkassen den Kunden, die Credentials für den Online-Zugriff Dritten zur Verfügung zu stellen. Mit der Nutzung von SOFORT-Überweisung verstößt man also gegen die AGBs der Finanzinstitute.

Das Landgericht Frankfurt am Main hat in einem Urteil klar formuliert, dass die Nutzung des Dienstes unzumutbar ist, egal, welche Sicherheitsgarantien von der Sofort GmbH versprochen werden:

> *Die Nutzung des Dienstes Sofortüberweisung ist unabhängig von seiner Bewertung durch Kreditinstitute für den Verbraucher unzumutbar, da er hierzu nicht nur mit einem Dritten in vertragliche Beziehungen treten muss, sondern diesem Dritten auch noch Kontozugangsdaten mitteilen muss und in den Abruf von Kontodaten einwilligen muss. Hierdurch erhält ein Dritter umfassenden Einblick in die Kunden-Kontoinformationen. Hierbei handelt es sich um besonders sensible Finanzdaten, die auch zur Erstellung von Persönlichkeitsprofilen genutzt werden könnten. Daneben muss der Kunde dem Zahlungsdienstleister seine personalisierten Sicherheitsmerkmale (zum Beispiel PIN und TAN) mitteilen. Dies birgt erhebliche Risiken für die Datensicherheit und eröffnet erhebliche Missbrauchsmöglichkeiten. Dabei kommt es im Ergebnis nicht auf die konkrete Sicherheit des Dienstes Sofortüberweisung an, sondern auf die grundsätzliche Erwägung, dass der Verbraucher nicht gezwungen werden kann, seine Daten diesem erhöhten Risiko auszusetzen.*

Der Bundesgerichtshof hat in dem Urteil Az.: KZR 39/16 diese Rechtsauffassung letztinstanzlich bestätigt.

Paysafecard entstand aus einem Forschungsprojekt der EU. In vielen Geschäften oder Tankstellen kann man Gutscheincodes kaufen. Die Webseite von Paysafecard bietet eine Umkreis-Suche nach Verkaufsstellen. Diese Codes kann man ähnlich anonym wie Bargeld im Web zur Bezahlung verwenden (wenn der Händler PSC akzeptiert).

Bei der Bezahlung wird man von der Webseite des Händlers zur Webseite von Paysafecard weitergeleitet. Dort gibt man den gekauften Code ein und der Händler erhält die Information, dass die Bezahlung erfolgt ist.

Eine Paysafecard ist 12 Monate uneingeschränkt gültig. Danach werden für jeden weiteren Monat 2 Euro vom Guthaben abgezogen. Es ist also sinnvoll, bei Bedarf kleinere Guthaben zu kaufen. Das verhindert auch eine technisch mögliche Verkettung mehrerer Einkäufe über den gleichen Gutscheincode.

Nach praktischen Erfahrungen sind die Verkäufer im Supermarkt, Tankstellen u. Ä. nicht immer über die angebotene Möglichkeit des Verkaufes von Paysafecard-Gutscheinen informiert. Es hilft jedoch, hartnäckig zu bleiben und die Verkäuferin auf das Paysafecard Symbol im GUI der Kasse hinzuweisen.

Durch Verschärfung der Sicherheitsvorkehrungen kommt es häufig zu gesperrten Gutscheinen, wenn die Gutscheine von verschiedenen IP-Adressen genutzt oder abgefragt werden. Nachfragen beim Support von Paysafecard, wie man die Sperrung der Gutscheincodes vermeiden kann, wurden bisher nicht beantwortet. Wenn ein Gutschein gesperrt wurde, muss man sich an den Support von Paysafecard wenden. Restbeträge kann man sich unter Angabe der eigenen Kontonummer erstatten lassen.

Aufgrund des Gesetzes gegen Geldwäsche ist Paysafecard gezwungen, die Anonymität des Zahlungsmittels einzuschränken. Deutsche Nutzer sollen (aber müssen nicht) auf der Website unter *My PaySafaCard* einen Account erstellen und können diesen Account mit Gutscheincodes aufladen. Wer mehr als 100,- Euro pro Monat nutzen möchte, muss sich mit Ausweisdokumenten identifizieren. Probleme mit gesperrten Gutscheinen soll es dann nicht geben.

Eine Nutzung von mehreren Gutscheinen mit Restbeträgen für einen Bezahlvorgang ist seit September 2012 NICHT mehr möglich! Restbeträge kann man sich unter Angabe der Kontonummer erstatten lassen. Damit wird die Anonymität des Zahlungsmittels leider ausgehebelt. Passende Paysafecards gibt es nicht immer, es gibt nur Gutscheine für 10, 15, 20, 25, 30, 50 oder 100 Euro.

Seit Ende Oktober 2014 sperrt Paysafecard Anonymisierungsdienste. Will man bei der Bezahlung anonym bleiben und nutzt einen Anonymisierungsdienst wie Tor, dann erhält man eine Fehlermeldung. Der Gutschein-Code wird bei 1–2 Versuchen nicht gesperrt, man kann ihn ohne Anonymisierungsdienst weiter verwenden.

8.1 Bargeld

Man kann im Internet nicht mit Bargeld bezahlen, trotzdem soll es kurz erwähnt werden, weil das anonyme Bezahlen mit Bargeld immer weiter eingeschränkt wird. Angesichts der ungebremsten Schuldenentwicklung und des unzureichenden Wachstums wird die Politik immer radikalere Maßnahmen ergreifen. Ein Bargeldverbot passt durchaus ins Konzept.

In Italien, Spanien, Frankreich, Griechenland und Zypern wurden Bargeldzahlung über einen Höchstsatz von 1.000-3.000 Euro bereits verboten, in Frankreich wurde ab August 2015 die Höchstgrenze für Bezahlung mit Bargeld auf 2.000 Euro abgesenkt (das Gesetz wurde nach dem Charlie-Hebbo-Attentat verabschiedet). In Dänemark wurde ein Gesetz aufgehoben, das Läden im Einzelhandel zwingt, Bargeld akzeptieren müssen. Außerdem hörte die dänische Notenbank ab 2016 auf, Geldscheine zu drucken.

Die EU hat im Jan. 2024 beschlossen, dass Bargeldzahlungen in EU Ländern bis maximal 10.000 zulässig sein sollen, wobei über 3.000 die Identität festgestellt werden muss. Unsere Fancy Innenministerin hat angekündigt, dass die Obergrenze in DE deutlich unter 10.000 liegen soll.

Erzwingen kann man das erstmal nur für Zahlungen, die man steuerlich geltend machen will. Wenn man sich privat ein schon benutztes Auto vom Gebrauchtwagenschrotthändler an der

nächsten Ecke kaufen will, kommt es nur darauf an, welche Einstellung der Händler zu Bargeld hat. (Und die Großhandelspackung Kokain wird man auch zukünftig nicht per Kreditkarte bezahlen.)

Um diesen privaten Geldfluss besser zu kontrollieren, sollen die sogenannten Financial Intelligence Units (FIUs) mehr Befugnisse erhalten (beispw. Zugriff auf Immobilien- und Kfz.-Register). In Deutschland übernimmt diese Aufgabe der Zoll, der schon jetzt sehr weitreichende Rechte hat.

Parallel dazu stellt die EU die Forderung auf, dass Transkationen mit Kryptowährungen (Bitcoin, Etherum, TONs oder Ripple) vollständig nachverfolgbar sein müssen. Handelsbörsen müssen die Inhaber von Wallets identifizieren und Transaktionen in private Wallets protokollieren.

Der Wirtschaftsweise Bofinger und der US-Ökonom Rogoff forderten im Mai 2015 nachdrücklich die Abschaffung des Bargelds. Sie appellierten an Bundeskanzlerin Merkel, dass sie sich auf dem G7-Gipfel in Elmau für eine weltweite Abschaffung des Bargelds einsetzen solle. Dafür wurden folgende Gründe genannt,[3] die ich nur kurz kommentieren will:

Stärkung der Nationalbanken: Wollen wir wirklich irgendwelche Banken stärken? Wir sollten lieber über die Einführung von Vollgeld diskutieren (wie in Island oder in der Schweiz), um die Macht der Banken zu brechen und Banken auf ihren eigentliche Funktion zurückzuführen.

Austrocknung des Schwarzmarktes: Schwarzmarkt == BÖSE (Drogen, Kipo werden genannt – klar)

Der Schwarzmarkt ist aber auch ein Regulativ zwischen der Gesetzgebung und den Bürgern. Wenn eine Regierung die Wünsche der Bürger konsequent missachtet, dann haben Bürger die Möglichkeit, auf den Schwarzmarkt auszuweichen (natürlich unter Androhung von Strafen). Je drakonischer und unbeliebter die Finanzgesetze werden, desto stärker wird der Schwarzmarkt wachsen.

Die Austrocknung des Schwarzmarktes wird also auch die Macht der Regierenden und Banken gegenüber der Bevölkerung stärken. Wollen wir diese Entwicklung?

Negativzinsen durchsetzen: *Die Zentralbanken könnten auf diese Weise leichter Negativzinsen durchsetzen. Papiergeld ist das entscheidende Hindernis, die Zentralbank-Zinsen weiter zu senken. Seine Beseitigung wäre eine sehr einfache und elegante Lösung für dieses Problem.* (US-Ökonom Rogoff)

Das würde bedeuten, dass sich die Sparer gegen diese Enteignung nicht mehr wehren könnten, indem sie das Geld einfach abheben. Einen sogenannten Bankenrun (wenn Kunden massenweise ihr Geld abheben) will keine Bank riskieren.

Kommentare zu den Vorschlägen von Bofinger/Rogoff

> *Um diese beiden Argumente ernsthaft als Vorteile durchgehen zu lassen, muss man ein Technokrat sein, der einen lückenlos organisierten Ameisenhaufen für die beste aller Gesellschaften hält. Wer Freiheit, Bürgerrechte und eine lebendige Demokratie bewahren will, den muss es schütteln, wenn jemand, der als Weiser gilt, solche Ansichten verbreitet.*[4]

Noch etwas deutlicher:

[3] http://www.manager-magazin.de/finanzen/artikel/bofinger-und-rogoff-fordern-abschaffung-des-bargelds-a-1034135.html

[4] http://bitcoinblog.de/2015/05/18/bargeld-ist-macht/

Es geht dem ehemaligen Chefökonomen des Internationalen Währungsfonds (IWF) und dem IWF neben einer umfassenden Kontrolle der Bevölkerung längst auch darum, die Grundlage für die finanzielle Repression zu schaffen, um die ausufernde Verschuldung über die Enteignung der Sparer zu lösen.[5]

Forderungen deutscher Politiker

- Der NRW-Finanzminister Walter-Borjans (SPD) beteiligt sich an der Kampagne gegen Bargeld und forderte im Juli 2015 eine Obergrenze bei Barzahlung. Bezahlungen mit Bargeld sollten in Deutschland nur bis 2.000–3.000 Euro erlaubt sein. Ein höherer Betrag würde ihn skeptisch machen. (Warum eigentlich?)
- Der NRW-Landeschef des Bundes Deutscher Kriminalbeamter (BDK), Sebastian Fiedler, unterstützt diese Ansicht. Fiedler behauptet, wenn man 70.000 Euro für ein Auto oder 200.000 Euro für eine Immobilie bar bezahlt, dann handelt es sich um Geld aus Steuerhinterziehung oder Straftaten. (Kann man ein Auto anonym zulassen oder eine Immobilie anonym ins Grundbuch eintragen lassen und die Verwendung illegaler Einnahmen damit geheim halten? Wer findet den Denkfehler?)
- Im Jan. 2016 wurde ein Plan der Bundesregierung bekannt, europaweit die Obergrenze für Barzahlungen auf maximal 5.000 Euro festzulegen, um die Finanzierung von Terrorismus zu unterbinden. Da diese Forderung in Deutschland nur schwer durchsetzbar ist und auch von Finanz- und Datenschutzexperten abgelehnt wird, versucht die Bundesregierung wieder einmal den Weg über die EU.

Kommentare zu den Forderungen deutscher Politiker

- Wer etwas gegen die Finanzierung von Terrorismus tun will, der sollte die Beziehungen zu den Staaten wie Saudi-Arabien, Katar oder USA überdenken, die weltweit als die größten Finanzgeber von Terroristen bekannt sind. Man könnte auch Druck auf die Türkei ausüben, um die Verkaufswege von Erdöl aus den von der ISIS besetzten Gebieten zu unterbinden und damit eine wesentliche Geldquelle des ISIS treffen.
- Sicher kommt es vor, dass gelegentlich ein Köfferchen mit Bargeld den Besitzer wechselt. Der Waffenschieber Schreiber hat beispielsweise im Namen von Thyssen-Krupp der CDU eine Spende von 1,3 Mio. D-Mark in einem Köfferchen übergeben, das die CDU nicht ordnungsgemäß versteuerte. Er hat W. Schäuble 100.000 D-Mark in Bar geschenkt, die ebenfalls nicht korrekt verbucht und versteuert wurden. Deshalb trat unser jetziger Finanzminister vom CDU-Parteivorsitz zurück und musste Merkel den Vortritt lassen. Derartige Praktiken wird man durch eine 5.000-Euro-Grenze für Barzahlungen aber nicht wirklich verhindern können.
- Die Steuerfahndung hat in Deutschland aber ganz andere Probleme. Der Fall Zumwinkel ist ein schönes Beispiel. Der Steuerfahnder wurde von seinen Vorgesetzten ausdrücklich angewiesen, den Fall Zumwinkel nicht weiterzuverfolgen. Er tat es trotzdem und wurde dafür mit einem psychologischen Gutachten vom Dienst suspendiert. Die Staatsanwältin, die den Fall mit über 1 Mio. Euro Steuerbetrug vor Gericht brachte, wurde strafversetzt. Die Anklage wurde verzögert, bis ein Teil der Steuerschuld verjährt war und die Summe des Betruges unter 1 Mio. Euro lag. Mehr kann man in dem Buch *Inside Steuerfahndung* (ISBN:

[5] http://www.heise.de/tp/artikel/45/45089/1.html

978-3-86883-105-4) von Frank Wehrheim und Michael Gösele nachlesen. Die Probleme liegen jedenfalls nicht in der Verfügbarkeit von Bargeld.

8.2 Bitcoin

Bitcoin ist eine digitale Peer-2-Peer-Währung ohne zentrale Verwaltung. Sie ist unabhängig von der Geldpolitik einer Zentralbank und entwickelt sich marktgetrieben durch die Aktivitäten der Teilnehmer, die Bitcoin als Zahlungsmittel akzeptieren oder verwenden.

Die Wurzeln der ökonomischen Theorie dieser virtuellen Währung liegen in der *Austrian school of economics*, die von den Ökonomen Eugen v. Böhm-Bawerk, Ludwig Mises und Friedrich A. Hayek entwickelt wurde. Die Ökonomen kritisieren das gegenwärtige System des Fiatgeldes der Zentralbanken. Sie sehen in den massiven, politisch motivierten Interventionen der Zentralbanken in den Geldumlauf eine wesentliche Ursache für den Krisenzyklus. Als Ausweg empfehlen sie eine Internationalisierung der Währungen und die Rückkehr zum Goldstandard.

Gegenwärtig ist Bitcoin der populärste Versuch zur Umsetzung einer Währung in Anlehnung an die Konzepte der *Austrian school of economics* und auch die populärste der 13.400 Kryptowährungen. Die Software löst mit kryptografischen Methoden vor allem zwei Probleme:

1. Das Kopieren und die mehrfache Verwendung der Bits und Bytes, die eine Coin repräsentieren, ist nicht möglich.
2. Die Gesamtmenge der verfügbaren Coins ist limitiert. Neue Bitcoins werden nach einem festen Schema generiert und die Gesamtzahl ist limitiert.

Darauf aufbauend könnte Bitcoin als Bezahlmethode verwendet werden. Bitcoins lassen sich in reale Währungen hin- und zurücktauschen. Der Kurswert der Bitcoins beim Tausch gegen reale Währungen (z. B. Euro) ergibt sich dabei ausschließlich aus dem Markt. Die Bezahlungen können relativ schnell am PC abgewickelt werden. Es dauert in der Regel nur 30–60 Minuten, bis das Bitcoin-Netzwerk eine Transaktion hinreichend bestätigt hat.

In der Praxis ist Bitcoin aber als Zahlungsmittel unbrauchbar geworden:

- In den letzten Jahren ist Bitcoin zu einem Spekulationsobjekt geworden. Durch gezielt verursachte Währungsschwankungen, die durch einzelne Spekulanten mit hohem finanziellen Einsatz verursacht werden, ist der Kurs sehr volatil. Wenn der Kurs in wenigen Wochen um 50 % schwankt, ist ein kalkulierter kommerzieller Einsatz kaum möglich.
- Durch die teilweise intensiven Spekulationskäufe und -verkäufe bei Kursschwankungen steigen die Transaktionsgebühren. Im Dezember 2017 musste man für eine Transaktion zeitweise bis zu 100 US-Dollar als Gebühren zahlen, um sicherzustellen, dass die Transaktion innerhalb einer vertretbaren Zeit in die Blockchain aufgenommen wird.[6]

  Transaktionsgebühren von 15 US-Dollar sind inzwischen normal. Damit liegen die Gebühren deutlich über den Kosten anderer Zahlungsmittel.
- Die Sicherheit vieler Bitcoin-Marktplätze liegt deutlich unter dem Niveau anderer Bezahldienste und Banken. Prominentestes Beispiel ist die Insolvenz von MtGox nachdem Bitcoins im Wert von 368,4 Mio. Euro verloren gingen. Möglicherweise handelte es sich dabei um

[6] https://www.heise.de/ct/ausgabe/2018-3-Allzeit-Hoch-bei-Kurs-und-Gebuehren-Taugt-Bitcoin-noch-als-Zahlungsmittel-3942392.html

einen Betrug der Betreiber. Die Betreiber der Bitcoin-Börse MyCoin sind ebenfalls in betrügerischer Absicht mit den Einlagen der Kunden verschwunden und haben Bitcoins im Wert von 342 Mio. Euro mitgenommen.

Weitere Beispiele sind die Börsen Flexcoin oder Poloniex oder die südkoreanische Bitcoin-Börse Youbit, die alle nach virtuellem Bankraub geschlossen wurden.

Die Bitcoins nur lokal in einem Wallet auf dem eigenen Rechner zu speichern, ist auch nicht immer sicher. So konnte im Januar 2018 ein Angreifer mit ein bisschen JavaScript-Code in einer Webseite aus dem Browser heraus die Wallets von Electrum leerräumen.[7]

- Der Wettkampf der Bitcoin-Miner beim Schürfen neuer Coins ist völlig außer Kontrolle geraten und ein sinnloser Einsatz von immer mehr Rechenleistung, um sich gegenseitig zu übertrumpfen. Es ist nur noch eine gewaltige Energieverschwendung.

  Die Webseite Bitcoin Energy Consumption Index[8] schätzte den Energieverbrauch im November 2017 auf 30 Terrawattstunden (TWh) pro Jahr. Zum Vergleich: Der Verbrauch von Irland liegt bei 25 TWh, von Marokko bei 29 TWh und von Dänemark bei 34 TWh jährlich. Ende Januar 2018 wurde der Energieverbrauch von Bitcoin auf 40 TWh pro Jahr geschätzt, Tendenz weiter steigend, ohne irgendeinen Nutzwert außer der Umverteilung von Geld durch Spekulation zu liefern.

  Auch wenn man die absoluten Zahlen zur Berechnung des Bitcoin Energy Consumption Index von Enthusiasten der Kryptowährung infrage stellt und meint, es seien eher 10 statt 30 TWh jährlich, kann man nicht leugnen, das Bitcoin Energie in gigantischem Ausmaß verbrennt – für nichts.[9]

Schlussfolgerung: Die real existierende Menschheit ist noch nicht in der Lage, mit einer Technologie wie Bitcoin umzugehen.

[7] https://www.heise.de/ct/ausgabe/2018-3-Bitcoin-3942380.html
[8] https://digiconomist.net/bitcoin-energy-consumption
[9] https://bitcoinblog.de/2017/11/27/bitcoin-verbraucht-mehr-strom-als-159-laender-wirklich/

Kapitel 9

E-Mail-Kommunikation

E-Mail ist eines der meistgenutzten Kommunikationsmittel. Die folgenden Seiten sollen zum Nachdenken über die die Auswahl des E-Mail-Providers anregen und Hinweise für die Konfiguration von Mozilla Thunderbird geben.

9.1 E-Mail-Provider

Als Erstes braucht man eine E-Mail-Adresse. Hier ist eine kleine Liste von empfehlenswerten E-Mail-Providern für den Alltagsgebrauch:

- **Mailbox.org**[1] (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat(E-Mail only) und ab 3,- Euro mit Cloud Funktionen, PGP und S/MIME Verschlüsselung im Webinterface integriert, verschlüsselter Mailversand und -empfang nur über SSL/TLS aktivierbar, private IP-Adressen und User-Agent werden aus dem Mail Header entfernt, anonyme Accounts möglich, Aliases und Temp.-Adresse nutzbar, OTP-Login für Webinterface, Tor Onion Service für POP3, IMAP, SMTP, Videokonferenzen für bis zu 25 Teilnehmenern. als Mailserver für die eigene Domain nutzbar);
- **Posteo.de**[2] (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, S/MIME oder PGP-verschlüsselte Inbox, verschlüsselter Mailversand und -empfang aktivierbar, DANE, IP-Adressen der Nutzer werden aus dem E-Mail-Header entfernt, aber User-Agent-Kennung nicht, anonyme Accounts möglich, anonyme Bezahlung per Brief, 2FA mit OTP suboptimal umgesetzt und unfreundliche Reaktion auf Kritik[3]);
- **Mailfence.com**[4] (belgischer Provider, kostenlose Accounts möglich, Premium ab 3,50 Euro pro Monat, POP3, IMAP, SMTP, Alias Adressen und WebDrive Speicher nur für Premium Accounts, OpenPGP im Webinterface möglich, 2-Faktor-Auth im Webinterface mittels OTP aktivierbar, als Mailserver für die eigene Domain nutzbar);
- **KolabNow**[5] (Groupware-Hosting in der Schweiz mit Adressbuch, Kalender und E-Mail, Mailaccounts für 4.41 CHF pro Monat, Groupware für 10 CHF pro Monat, IP-Adressen der Nutzer und User-Agent werden aus dem E-Mail-Header entfernt);

[1] https://mailbox.org/
[2] https://posteo.de
[3] https://www.privacy-handbuch.de/diskussion.htm#take-down-notiz-von-posteos-anwaelten
[4] https://mailfence.com
[5] https://kolabnow.com/

- **runbox.com**[6] (privacy-engagierter norwegischer E-Mail-Provider, Server stehen ebenfalls in Norwegen, Accounts ab 1,66 Dollar pro Monat, 2-Faktor-Auth mit OTP aktivierbar);
- **disroot.org** (NL) bietet neben Services wie XMPP, Etherpads usw. auch kostenfreie E-Mail-Accounts und wird durch Spenden finanziert. IP-Adressen der Nutzer und User-Agent-Kennungen werden aus dem E-Mail-Header entfernt.

  (Nach den Erfahrungen der letzten Jahre muss man leider damit rechnen, das kostenfreie, spendenfinanzierte E-Mail-Dienste wie SecureMail.biz, Xalia u. a. nur für ein paar Jahre verfügbar sind und dann eingestellt werden könnten.)

Bei diesen Vorschlägen für E-Mail-Provider geht es um Privatsphäre im Alltagschaos und nicht um Anonymität. Die Einrichtung anonymer E-Mail-Adressen wird im Kapitel 12.3.7 beschrieben.

Hinweis: es kostet Geld, einen zuverlässigen Mailservice bereitzustellen. Es ist sinnvoll, die *alles kostenlos Mentalität* für einen vertrauenswürdigen Mailprovider fallen zu lassen.

Nicht empfohlene E-Mail-Provider

Einige Gründe, warum verschiedene E-Mail-Provider mit gutem Ruf nicht in die Liste der Empfehlungen aufgenommen wurden:

- Web.de und GMX.de sammeln bei der Registrierung zu viele Daten: Vor- und Nachname, Land, PLZ und Ort, Straße, Hausnummer und die Mobilfunknummer.

  Mit der Registrierung erklärt man sich damit einverstanden, dass die Daten für Marketing-Zwecke verwendet werden. Die Daten werden an den Mutterkonzern übermittelt und mit anderen verbundenen Unternehmen geteilt. Außerdem werden die Daten für postalische Werbung sowie für Markt- und Meinungsforschung genutzt und Non-Profit-Organisationen für Werbung zur Verfügung gestellt. (Falls man sich schon öfters mal gefragt hat, woher Meinungsforschungsinstitute die Telefonnummern haben . . .)

  Der EmailPrivacyTest[7] zeigt, dass Web.de und GMX.de bei der Nutzung des Web-GUI nicht gegen Tracking-Elemente in E-Mails schützen und es damit vielen Diensten ermöglichen, die Nutzer beim Lesen der E-Mails zu beobachten. Web.de setzt selbst HTML-Wanzen in den eigenen Newslettern ein (3 Tracking-Wanzen in jedem Newsletter) und verfolgt damit die Lesegewohnheiten der Nutzer.

- Hushmail speichert zu viele Daten. Neben den üblichen Daten beim Besuch der Webseite werden die E-Mails gescannt und folgende Daten unbegrenzt lange gespeichert:

  1. alle Sender- und Empfänger-E-Mail-Adressen (VDS-artig);
  2. alle Dateinamen der empfangenen und gesendeten Attachments;
  3. Betreffzeilen aller E-Mails (nicht verschlüsselbar);
  4. URLs aus dem Text unverschlüsselter E-Mails;
  5. ... and any other information that we deem necessary.

  Diese Daten werden bei der Kündigung eines Accounts NICHT gelöscht.

  Bei der Bezahlung für einen Premium-Account werden die IP-Adresse des Kunden sowie Land, Stadt und PLZ an Dritte weitergeben. Außerdem bindet Hushmail.com Dienste von

[6] https://secure.runbox.com/
[7] https://www.emailprivacytester.com/

Drittseiten ein. Die ID des Hushmail-Accounts wird beim Besuch der Webseite nach dem Login an diese Drittseiten übermittelt. Für die Privacy-Policy dieser Drittseiten übernimmt Hushmail.com keine Verantwortung.

- In der EU-Studie *Fighting cyber crime and protecting privacy in the cloud*[8] warnen die Autoren in Kapitel 5.4 (S. 48) vor Risiken bei der Speicherung von Daten in den USA. Aufgrund des *US PATRIOT Act* (insbesondere S. 215ff) und der *4. Ergänzung des FISA Amendments Act* ist es für US-Behörden ohne juristische Kontrolle möglich, die Kommunikation von Nicht-US-Bürgern zu beschnüffeln. Dabei ist es unerheblich, ob der Cloud- oder E-Mail-Provider eine US-Firma ist oder nicht. Es reicht nach Ansicht der Amerikaner, wenn die Server in den USA stehen.

  Außerdem hat US-Präsident Trump als eine seiner ersten Handlungen die Behörden in den USA per Dekret aufgefordert, den Datenschutz für Ausländer vollständig aufzuheben. Es ist unklar, welche Auswirkungen das Dekret und die damit angedeutete Richtung im Datenschutz zukünftig für EU-Bürger haben wird.

  Aus diesem Grund ist ein Server-Standort *USA* für deutsche Nutzer eher ungeeignet. Das betrifft u. a. die E-Mail-Provider SecureNym, S-Mail, Fastmail.fm, Rise-up.net usw.

- Weitere Beispiele werden auf der Webseite des Handbuches genannt.[9]

9.2 Proton Mail und Tutanota

Die E-Mail-Dienste Proton Mail[10] (Schweiz) und Tutanota[11] (Deutschland) stellen einfache Nutzung von Verschlüsselung sowie Kompatibilität mit den gängigen E-Mail-Protokollen in den Vordergrund und bemühen sich um Schutz gegen staatlichen Zugriff.

Das Schreiben und Lesen von E-Mails erfolgte am Anfang der Entwicklung primär im Webinterface mit einem Webbrowser. Einen E-Mail Client wie Thunderbird konnte man nicht verwenden. Das ermöglicht die Realisierung einer einfach nutzbaren E-Mail Verschlüsselung.

Inzwischen gibt es bei Proton E-Mail Apps für Smartphones und bei Tutanota E-Mail Apps für Smartphones sowie Electron-Apps für Windows, MacOS und Linux PCs.

Vorteile gegenüber Web.de, GMX.de, GMail.com u. a.

ProtonMail und Tutanota bieten viele Vorteile für Normalanwender, die ihre E-Mails bisher im Webinterface von GMail, Yahoo! oder Hotmail bearbeiten.

- Die Provider respektieren die Privatsphäre der Nutzer, schnüffeln nicht in den Mails, geben keine Daten weiter und beobachten auch nicht beim Lesen von Newslettern.

- Die Daten werden verschlüsselt auf den Servern gespeichert. Auch die Betreiber haben keinen Zugang zu den Daten. Das schützt gegen Beschlagnahme von Daten durch Behörden, aber nicht gegen eine TKÜ nach §100 a/b StPO.

[8] http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050
[9] https://www.privacy-handbuch.de/handbuch_31.htm
[10] https://proton.me/mail
[11] https://tuta.com/de/

- Die Provider bieten einen einfachen Zugang zur E-Mail-Verschlüsselung für nicht IT-affine Nutzer. Man muss sich nur wenig mit der Verschlüsselung beschäftigen, um sie in der Praxis einsetzen zu können. Zwischen den Nutzern des Dienstes werden die Nachrichten automatisch verschlüsselt.
- Auch auf dem Smartphone ist verschlüsselte Kommunikation via E-Mail nutzbar. Tutanota und Protonmail bieten passende Apps im Google Playstore und für iPhones.
- Protonmail bietet vollständigen OpenPGP-Support auch für die Kommunikation mit externen Partnern. Man kann seine öffentlichen Schlüssel exportieren und dem Partner schicken. Außerdem kann man die Schlüssel der externen Partner importieren.

  Externe Nutzer, die keinen Account bei Tutanota haben, können nicht direkt via PGP-verschlüsselten E-Mails kommunizieren. Der Nutzer von Tutanota muss eine Nachricht an den externen Kontakt schicken. Die Nachricht wird verschlüsselt auf dem Server gespeichert und der Empfänger bekommt nur einen Link, unter dem er die Nachricht lesen und beantworten kann.
- Die Verwendung von E-Mail-Clients ist nur bei Proton Mail möglich. Dafür muss man die Proton-Mail-Bridge lokal auf dem eigenen Rechner installieren. Die Bridge ist ein lokales Mail-Gateway mit SMTP- und IMAP-Schnittstelle (kein POP3). Die Schlüsselverwaltung erfolgt dabei weiterhin auf dem Proton-Mail-Server.
- Die SSL/TLS-Verschlüsselung für die Webseiten wird vom Qualsys-SSL-Server-Test mit A+ bewertet und Features zur Verbesserung der Transportsicherheit für E-Mails werden zeitnah implementiert.
- Tutanota unterstützt U2F als zweiten Faktor zur Anmeldung im Webinterface.

Am besten kommen die Vorteile zur Geltung, wenn alle Kommunikationspartner einen Account bei Proton Mail bzw. Tutanota haben.

Nachteile der Verschlüsselung im Browser

Konzeptionell bedingt haben diese Mailprovider einige Schwächen. Die Verschlüsselung bietet *hinreichende Sicherheit* und ist für hohe Sicherheitsansprüche nicht geeignet. Das wird im Threat-Modell bei Proton Mail auch deutlich angesprochen:

> *If you are Edward Snowden, or the next Edward Snowden, and have a life and death situation that requires privacy, we would not recommend using Proton Mail.*

Webanwendungen bieten mehr Angriffsmöglichkeiten auf die Verschlüsselung als lokal installierte Tools. Thomas Roth demonstrierte in dem Video *Hacking protonmail - with a browser*, wie man die Verschlüsselung von ProtonMail mit einfachen XSS-Hacks angreifen konnte. Die Lücken sind inzwischen beseitigt, vergleichbare Probleme hätte es bei Thunderbird aber nie geben können.

Die alternative Nutzung starker Kryptografie mit OpenPGP Smartcards ist bei beiden Diensten nicht möglich, auch wenn man dazu in der Lage wäre.

Der Code für die Verschlüsselung wird durch die Webanwendung beim Aufruf der Webseite geladen oder aktualisiert. Außerdem werden die Schlüssel der Empfänger bei Bedarf vom Server geladen. Dieses Konzept nennt man *Server-basierte Kryptografie*. (Es ist damit nicht *Server-basierte Verschlüsselung* gemeint!) Das Konzept ist nicht neu. Es wurde bereits von Hushmail und Countermail eingesetzt (mit Java statt Javascript) oder von Cryptocat (für Chats) und die Kritikpunkte an dem Konzept kann man hier übernehmen.

- Die Server-basierte Kryptografie von Hushmail wurde bereits 2007 von der US-Drogenbehörde DEA kompromittiert[12]. Hushmail wurde gezwungen, die E-Mails von mehreren Accounts entschlüsselt bereitzustellen und musste der Aufforderungen nachkommen. Auch alle oben genannten Dienste könnten die Verschlüsselung unbemerkt kompromittieren, wenn sie es für staatliche Behörden tun müssten.
- Server-basierte Kryptografie ist für hohe Sicherheitsansprüche politischer Aktivisten nicht geeignet, wie P. Ball in einem Essay bei Wired.com[13] ausführlich dargelegt.

Tutanota und Proton Mail bieten inzwischen Apps für Android und iPhone an, die den Code für die Verschlüsselung enthalten und aus den Appstores installiert werden können. Damit entfällt diese Schwäche für Smartphone-Nutzer.

Auf dem Desktop-PC könnte man die *Proton Mail Bridge* als Mail-Gateway installieren oder die Software von Tutatnota von Github auschecken und lokal installieren. Auch das schützt gegen diese Angriffe, ist allerdings komplizierter, als OpenPGP zu konfigurieren.

Key-Recovery durch den Provider (aka Krypto-Key-Backdoor)

Die genannten Provider speichern alle Nachrichten und Kontakte verschlüsselt auf den Servern. Die Nutzer können auf die Daten zugreifen, wenn sie sich mit einem Passwort authentifizieren. Das Passwort schützt den Zugriff auf die Kryptoschlüssel.

Welche Möglichkeiten gibt es für ein Key-Recovery, wenn man sein Passwort vergisst?

- Proton Mail bietet ein Key-Recovery via externer Mailadresse, wenn man sein Passwort vergessen hat. Wenn man diese Möglichkeit nutzt, werden alle vorhandenen E-Mails und Daten gelöscht, da sie ohne das Passwort des Nutzers nicht mehr entschlüsselt werden können. Wer das Passwort vergisst, verliert zwar alle Daten, aber nicht den Account.[14]
- Tutanota bietet für normale Nutzer keine Möglichkeit des Key Recovery. Bei Tutanota Premium Accounts werden die Daten mit dem Key des Nutzers und dem Key der Account-Administratoren verschlüsselt. Das heißt, der Administrator eines Premium Accounts könnte sich Zugriff auf die Daten verschaffen, aber die Administratoren von Tutanota haben keine konzeptuelle Backdoor für den Zugriff auf die Daten.[15]

Somit gibt es bei beiden Services keine konzeptuelle Backdoor.

9.3 E-Mail-Aliases und temporäre Adressen

Die E-Mail-Adresse ist ein wichtiges Identitätsmerkmal. Datensammler wie Rapleaf verwenden sie als ein Hauptmerkmal für die Identifikation, um darauf aufbauend Profile zu erstellen. Stichproben im Internet-Traffic weisen einen hohen Anteil von Suchanfragen nach Informationen zu den Inhabern von E-Mail-Adressen aus.

[12] http://www.wired.com/2007/11/encrypted-e-mai
[13] http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/
[14] https://protonmail.com/support/knowledge-base/resetting-mailbox-password/
[15] https://tutanota.uservoice.com/knowledgebase/articles/470716-was-passiert-wenn-ich-mein-passwort-vergesse-k%C3%B6n

Man muss die eigene E-Mail-Adresse nicht bei jeder Gelegenheit im Web angeben, wenn irgendwo eine E-Mail-Adresse verlangt wird (bei der Registrierung in Foren, einfachen Blog Postings usw.). Um die eigene E-Mail-Adresse nicht zu kompromittieren und trotzdem diese Angebote zu nutzen, kann man E-Mail-Aliases, Wegwerf-Adressen oder temporäre E-Mail-Adressen nutzen.

Es ist empfehlenswert, für unterschiedliche Anwendungen auch verschiedene E-Mail-Adressen zu verwenden. Es erschwert die Profilbildung anhand der E-Mail-Adresse und verringert die Spam-Belästigung. Wenn Amazon, Ebay oder andere kommerzielle Anbieter zu aufdringlich werden, wird die mit Spam überschwemmte E-Mail-Adresse einfach gelöscht, ohne die private Kommunikation zu stören.

Neben einer privaten E-Mail-Adresse für Freunde könnte man für Einkäufe im Internet oder für politische Aktivitäten weitere E-Mail-Adressen (sogenannte Aliases) nutzen. Wenn eine E-Mail-Adresse nur einmalig oder kurzzeitig für die Anmeldung in einem Forum oder das Veröffentlichen eines Kommentars in Blogs benötigt wird, kann man *temporäre Mailadressen* nutzen.

E-Mail-Aliases nutzen

Jeder brauchbare E-Mail-Provider bietet die Möglichkeit, zusätzlich zur Hauptadresse mehrere E-Mail-Aliases für einen E-Mail-Account anzulegen. Man kann im Webinterface in den Konfigurationseinstellungen die Aliases für den Account erstellen, diese Adressen für die Kommunikation mit bestimmten Zweck (z. B. für Hotelreservierung oder Flugbuchung) für eine begrenzte Zeit nutzen und dann löschen. Konkrete Anleitungen findet man in den FAQ oder der Online-Hilfe des Mail-Providers.

Die E-Mails an die Alias-Adressen landen ganz normal in der Inbox. Mit Filterregeln könnte man sie automatisch in einen anderes Mailverzeichnis verschieben (zur Verbesserung der Übersichtlichkeit). Beim Schreiben einer E-Mail im Webinterface kann man statt der Hauptadresse auch eine Alias-Adresse als Absender auswählen.

Die Verwendung von E-Mail-Aliases hat gegenüber temporären E-Mail-Adressen und Wegwerf-Adressen einige Vorteile:

- E-Mail-Aliases können auch als Absender zum Senden von E-Mails verwendet werden. Das ist z. B. ein Vorteil, wenn man nach der Registrierung eines Accounts den Support des Anbieters kontaktieren muss. Mit temporären Adressen kann man in der Regel nur Nachrichten empfangen.
- E-Mail-Aliases werden nicht gesperrt. In vielen Diskussionsforen sind E-Mail-Adressen von Temp.-Mail-Anbietern für die Registrierung von Accounts gesperrt.
- Gute E-Mail-Provider haben eine sichere TLS-Transportverschlüsselung für ihre Mailserver. Bei den Anbietern temporärer E-Mail-Adressen werden die Mails öfters ohne oder mit schlechter TLS-Verschlüsselung durch das Internet gesendet und können von Dritten (z. B. vom BND in Rahmen der Fernmeldeaufklärung) problemlos mitgelesen werden.

E-Mail-Adress-Erweiterungen

Bei vielen E-Mail-Providern wie Mailbox.org, Runbox, Gmail, Yahoo! Mail Plus, Apple's iCloud, Outlook.com oder FastMail kann man E-Mail-Adress-Erweiterungen nutzen. Wenn man die E-Mail-Adresse *name@provider.tld* als Account oder E-Mail-Alias registriert hat, kann man beliebig viele Adressen nach dem Muster *name+extension@provider.tld* zum Empfang verwenden.

Es ist ein Standardfeature des MTA Postfix und kann auch auf eigenen Mailservern einfach aktiviert werden.

Einige E-Mail-Provider bewerben dieses Feature als Spamschutz, aber der Wert als Spamschutz ist gering. Jeder, der sich ein bisschen mehr mit E-Mail-Features beschäftigt hat (und davon kann man bei Datensammlern ausgehen), kennt das Feature und kann die Erweiterungen leicht ausfiltern. Der Vorteil von E-Mail-Adress-Erweiterungen liegt eher in der einfach konfigurierbaren, automatischen Sortierung eingehender Nachrichten und nicht beim Spamschutz.

AnonBox des CCC

Bei der AnonBox.net des CCC[16] kann ein E-Mail-Account für den Empfang von einer(!) Nachricht erstellt werden. Der Account ist bis 24:00 Uhr des folgenden Tages gültig (24–48 h) und nicht verlängerbar. Die empfangene Nachricht kann man nur im Webinterface lesen und sie wird nach dem Abrufen gelöscht. Sie kann nur 1x gelesen werden! Zusammen mit der E-Mail wird auch der Account gelöscht. Man kann praktisch nur eine Mail empfangen.

Beim Erzeugen einer E-Mail-Adresse erhält man einen Link, unter dem man die ankommende Mail lesen kann. Wenn noch nichts angekommen ist, dann bleibt die Seite leer. Der Link ist als Lesezeichen zu speichern, wenn man später nachschauen möchte.

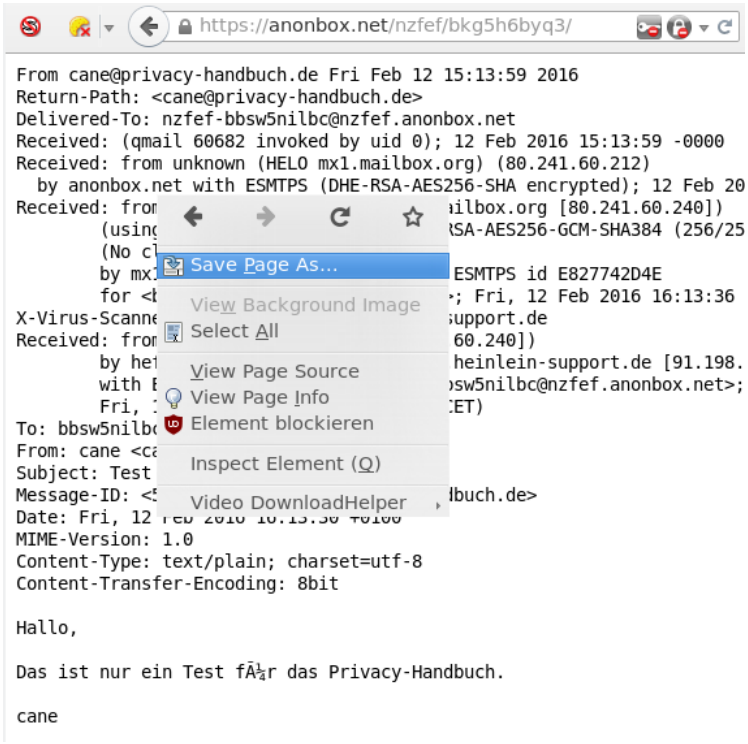


Abbildung 9.1: E-Mail im Web-GUI der AnonBox.net als Datei speichern

Eine empfangene E-Mail wird im Quelltext dargestellt. Wer aus dem Konvolut nicht schlau wird, kann mit der rechten Maustaste in die Textwüste klicken und sie als Datei speichern, wie in Abb. 9.1 gezeigt. Die Datei ist mit der Endung **.eml** zu speichern und kann dann in einem E-Mail-Client wie z. B. Thunderbird geöffnet werden (Abb. 9.2).

[16] https://anonbox.net

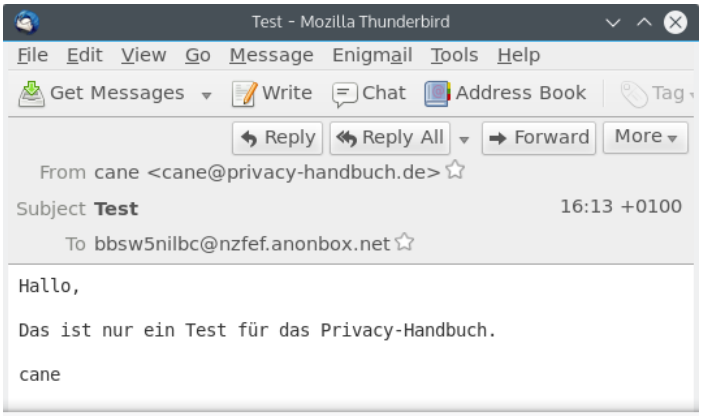


Abbildung 9.2: E-Mail aus AnonBox.net in Thunderbird geöffnet

Wegwerf-Adressen

Einige Anbieter von Wegwerf-E-Mail-Adressen bieten einen sehr einfach nutzbaren Service, der keinerlei Anmeldung erfordert und auch kein Erstellen der Adresse vor der Nutzung. E-Mail-Adressen der Form *pittiplatsch@trash-mail.com* oder *pittiplatsch@weg-werf-email.de* kann man überall und ohne Vorbereitung unbekümmert angeben. Das Postfach ist unbegrenzt gültig.

In einem Webformular auf der Seite des Betreibers findet man später alle eingegangenen Spam- und sonstigen Nachrichten für das gewählte Pseudonym. Für das Webinterface des Postfachs gibt es in der Regel keinen Zugriffsschutz. Jeder, der das Pseudonym kennt, kann die Nachrichten lesen und löschen. Wenn eine Wegwerf-Adresse für die Registrierung eines Accounts genutzt wurde, könnte ein Angreifer problemlos die Passwort-Recovery-Funktion nutzen!

Nachrichten werden nach 6–12 Stunden automatisch gelöscht. Man muss also regelmäßig den Posteingang prüfen, wenn man eine Wegwerf-Adresse nutzt.

Liste einiger Anbieter (unvollständig):

- https://discard.email/ (Passwortschutz, E-Mail schreiben möglich);
- https://www.trash-mail.com (Schreiben von E-Mails möglich);
- https://www.guerrillamail.com/ (Schreiben von E-Mails möglich);
- https://vsimcard.com/trashmails.php (bietet auch Wegwerf-SMS-Nummern);
- https://www.mailinator.com/ (bietet auch Wegwerf-SMS-Nummern);
- https://www.byom.de/ (E-Mails werden nur eine Stunde gespeichert!).

In der Regel speichern diese Anbieter die Informationen über eingehende E-Mails sowie Aufrufe des Webinterface und stellen die Informationen bei Bedarf den Behörden zur Verfügung. Es handelt sich dabei nicht um Anonymisierungsdienste.

Temporäre Adressen

Im Gegensatz zu Wegwerf-E-Mail-Adressen muss man eine temporäre E-Mail-Adresse zuerst auf der Webseite des Anbieters erstellen, die dann für 10 Minuten bis zu mehreren Stunden gültig ist.

Erst danach kann diese E-Mail-Adresse verwendet werden. Bei Bedarf kann die Verfügbarkeit der E-Mail-Adresse im Browser mehrfach verlängert werden.

Um eine temporäre E-Mail-Adresse für die Anmeldung in einem Forum o. Ä. zu nutzen, öffnet man als Erstes eine der oben angegebenen Webseiten in einem neuen Browser-Tab. Nachdem man eine neue temporäre E-Mail-Adresse erstellt hat, überträgt man sie mit Copy & Paste in das Anmeldeformular und schickt das Formular ab. Dann wechselt man wieder zu dem Browser-Tab der temporären E-Mail-Adresse und wartet auf die eingehende Bestätigungsmail. In der Regel einhält diese Mail einen Link zur Verifikation. Auf den Link klicken – fertig. Wenn der Browser-Tab mit der temporären E-Mail-Adresse geschlossen wurde, hat man keine Möglichkeit mehr, ankommende Mails für diese Adresse zu lesen.

Die folgenden Anbieter verwenden erstellte E-Mail-Adressen. Die Verwendung dieser Adressen für die Registrierung von Accounts ist sicherer, da ein Angreifer die Passwort-Recovery-Funktion des Webdienstes nicht nutzen kann, um sich ein neues Passwort zuschicken zu lassen und den Account zu übernehmen:

- **Temporäre Adressen**

  https://www.10minutemail.com/ (10 Minuten gültig, verlängerbar);

- **Temporäre Adressen**

  https://getnada.com/ (24 Stunden gültig);

- **Temporäre Adressen**

  https://temp-mail.ru/ (2 Stunden gültig).

9.4 Mozilla Thunderbird

Alle E-Mail-Provider bieten die Möglichkeit, die E-Mail-Kommunikation im Webinterface mit einem Browser zu verwalten. Dennoch ist ein E-Mail-Client empfehlenswert:

- Der Browser ist eine Sandbox zum Anzeigen von Webseiten. Aufgrund des Funktionsumfangs moderner Browser und der bösartigen Feindlichkeit des Internet muss man von viel mehr Angriffsmöglichkeiten ausgehen als bei einem Programm, dass speziell für die Bearbeitung von E-Mails optimiert wurde.
- Sichere Ende-zu-Ende-Verschlüsselung ist im Browser nicht möglich, auch wenn immer mehr E-Mail-Provider Lösungen dafür anpreisen. Diese Lösungen haben gegenüber der lokalen Verschlüsselung im E-Mail-Client Nachteile bei der Sicherheit.
- Einige E-Mail-Provider wie WEB.de und GMX.de blockieren nicht alle Tracking-Elemente in E-Mails im Webinterface (weil sie selbst Möglichkeiten zum Tracking ihrer Newsletter nutzen). Mit einem E-Mail-Client wie Mozilla Thunderbird kann man dafür sorgen, dass man seine E-Mails unbeobachtet liest.

Informationen und Downloadmöglichkeiten für Mozilla Thunderbird stehen auf der deutschsprachigen Website des Projekts[17] für Windows, Linux und MacOS zur Verfügung. Linux-Distributionen enthalten Thunderbird. Mit der Paketverwaltung kann Thunderbird und die deutsche Lokalisierung installiert werden.

Da Thunderbird den gleichen Code wie Firefox verwendet, wäre es möglich, dass die Downloads in gleicher Weise mit einer individuellen Kennung für die Telemetrie markiert werden wie Firefox. Windows- und MacOS-Nutzer können das vermeiden, indem sie Thunderbird aus dem FTP-Archiv[18] herunterladen. (Linuxer, die die Repositorys der Distribution zur Installation verwenden, sind nicht betroffen.)

9.4.1 Begriffserklärungen: SMTP, POP3, IMAP, STARTTLS

Nach dem ersten Start von Thunderbird führt ein Assistent durch die Schritte zur Einrichtung eines E-Mail-Kontos. Nach Eingabe der E-Mail-Adresse sowie des Passwortes erkennt der Assistent die nötigen Einstellungen für den Mailserver oft automatisch. Es können auch die Einstellungen eines bisher verwendeten Programms übernommen werden. Bei der Einrichtung des E-Mail-Accounts sollten einige Punkte beachtet werden.

Die Grafik in Abb. 9.3 zeigt den Weg einer E-Mail vom Sender zum Empfänger. In der Regel ist man nicht direkt mit dem Internet verbunden. Der Zugang erfolgt über ein Gateway des Providers oder der Firma.

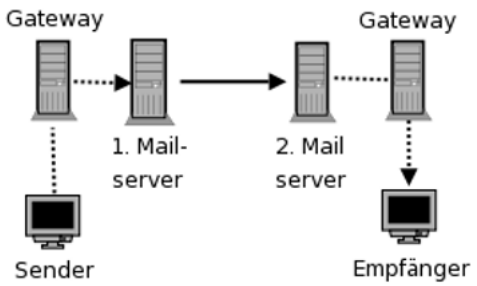


Abbildung 9.3: Der Weg einer E-Mail durch das Web

Der 1. Mailserver nimmt die E-Mail via SMTP entgegen und sendet sie an den 2. Mailserver. Hier liegt die E-Mail, bis der Empfänger sie via POP3 oder IMAP abruft und löscht. Die gestrichelten Verbindungen zu den Mailservern können mit SSL bzw. TLS kryptografisch gesichert werden. Das hat nichts mit einer Verschlüsselung des Inhalts der E-Mail zu tun. Es wird nur die Datenübertragung zum Mailserver verschlüsselt und es wird sichergestellt, dass man wirklich mit dem gewünschten Server verbunden ist.

Die Abkürzungen SMTP oder POP3 und IMAP sind für Laien erst mal verwirrend.

SMTP ist das Protokoll zum Versenden von E-Mails.

POP3 ist das Protokoll zum Herunterladen von empfangenen E-Mails auf den lokalen Rechner. Die E-Mails werden auf dem Server sofort (oder etwas später) gelöscht.

Hinweis: bei POP3 wird nur der Ordner *Posteingang* vom Server geholt. Wenn man im Webinterface des Mailproviders weitere Ordner angelegt hat und mit Filtern E-Mails

[17] https://www.mozilla.org/de/thunderbird/
[18] https://ftp.mozilla.org/pub/thunderbird/releases/

automatisch sortieren lässt, dann hat man mit POP3 keinen Zugriff auf diese Mails. Die automatische Sortierung muss in Thunderbird erfolgen.

IMAP ist ein Kommunikationsprotokoll, um die empfangenen E-Mails auf dem Server zu verwalten und nur zum Lesen temporär herunterzuladen. Auch die versendeten E-Mails und die E-Mail-Entwürfe werden bei der Nutzung von IMAP auf dem Mailserver des Providers gespeichert.

IMAP bietet damit die Möglichkeit, mit verschiedenen E-Mail-Clients von unterschiedlichen Rechnern und Smartphones auf den Account zuzugreifen und stets Zugriff auf alle E-Mails zu haben. Die Möglichkeit des weltweiten Zugriffs auf seine Mails erkauft man sich aber mit Einschränkungen des Datenschutzes.

Die auf dem Server des Providers gespeicherten E-Mails unterliegen NICHT mehr dem Telekommunikationsgeheimnis nach Artikel 10 GG, wenn der Nutzer Gelegenheit hatte, sie zu löschen. Das BVerfG hat diese Rechtsauffassung 2009 in dem Urteil 2 BvR 902/06 bestätigt.[19]

Mit der Reform der Telekommunikationsüberwachung im Dezember 2012 und die im Rahmen des Gesetzentwurfes zur Bekämpfung von Rechtsterrorismus und Hasskriminalität vorgelegten Anpassungen am Telemediengesetz von 2019 soll es jedem Dorfpolizisten ohne richterliche Prüfung erlaubt sein, diese Daten abzurufen. Es wäre u. U. unschön, wenn man dort die gesamte Kommunikation der letzten 15 Jahre vorfände.

Ein Kompromiss ist möglich, um mit mehreren Geräten (z. B. mit dem PC zuhause, vom Smartphone unterwegs usw.) auf einen E-Mail-Account zuzugreifen:

1. Das Hauptgerät (PC) greift via POP3 auf den Mailserver zu, holt sich alle E-Mails und archiviert sie. Dieser E-Mail-Client löscht alle Mails auf dem Server nach einer oder zwei Wochen oder wenn sie lokal gelöscht werden. So bleiben nur wenige E-Mails auf dem Server, man hat aber trotzdem privat ein vollständiges Archiv.
2. Alle anderen Geräte wie Smartphones u. Ä. greifen via IMAP auf den E-Mail-Account zu und können so tagesaktuelle Geschäfte erledigen und E-Mails kurzfristig unterwegs lesen und beantworten.

SSL/TLS oder STARTTLS

Wie einfach es war, unverschlüsselte Verbindungen zu belauschen, die Passwörter zu extrahieren und das Mail-Konto zu kompromittieren, wurde von T. Pritlove auf der re:publica 2007 demonstriert.[20]

Alle brauchbaren Mail-Server bieten die Möglichkeit der verschlüsselten Kommunikation zwischen Thunderbird und Mailserver. Diese Option ist in Thunderbird bei der Einrichtung eines neuen Kontos auszuwählen. Der Assistent erledigt das in der Regel automatisch anhand der Vorgaben vom Mailserver. In der Regel kann man zwischen old-style SSL/TLS oder STARTTLS wählen, wobei die Voreinstellung seltsamerweise meist STARTTLS ist.

SSL/TLS: Wenn man SSL/TLS verwendet, wird als erstes eine verschlüsselte Verbindung aufgebaut und danach beginnt die protokoll-spezifische Kommunikation. Es werden keine Daten über eine unverschlüsselte Verbindung übertragen und der Server muss sich zuerst authentifizieren, bevor der Client irgendwelche Daten sendet.

[19] https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-079.html
[20] http://tim.geekheim.de/2007/04/24/netzwerksicherheit-auf-der-republica/

STARTTLS: Wenn STARTTLS genutzt wird, beginnt die Kommunikation erst einmal unverschlüsselt. Der E-Mail-Client wartet ab, ob der Mailserver in den Capabilities mit 250-STARTTLS eine Transportverschlüsselung anbietet. Erst äußert der Client den Wunsch, verschlüsselt zu kommunizieren, was der Server nochmals bestätigen muss. Erst dann erfolgt ein Aufbau der verschlüsselten Verbindung und der Client beginnt nochmal von vorn.

Eine SMTP-Verbindung wird mit STARTTLS wie folgt aufgebaut:

```
Client: unverschlüsselter Connect
Server: 220 smtp.server.tld Simple Mail Transfer Service Ready
Client: EHLO 192.168.23.44
Server: 250-smtp.server.tld
Server: 250-SIZE 100000000
Server: 250-AUTH LOGIN PLAIN
Server: 250-STARTTLS
Client: STARTTLS
Server: 220 go ahead
SSL/TLS Handshake zwischen Client und Server
Client (TLS-verschlüsselt): EHLO 192.168.23.44
```

Wie man sieht, können dabei unter Umständen auch private Daten unverschlüsselt gesendet werden. Bei SMTP wird im ersten EHLO-Kommando die IP-Adresse oder der Hostname des Rechners aus dem internen Netz unverschlüsselt gesendet. Ein *Lauscher am Draht* kann damit u. U. den Mitarbeiter in einer Firma identifizieren.

Bewusst oder unbewusst können auch Internetzugangsprovider die sichere Übertragung deaktivieren und damit den Traffic mitlesen. Es wird einfach die Meldung des Mail-Servers 250-STARTTLS gefiltert und überschrieben (SSL strip attack). Scheinbar verfügen alle DSL-Provider über die Möglichkeit, dieses Feature bei Bedarf für einzelne Nutzer zu aktivieren.[21] Einige E-Mail-Clients bieten die Option *STARTTLS wenn möglich* an. Diese Einstellung ist genau in dem Moment wirkungslos, wenn man es braucht, weil der Traffic beschnüffelt werden soll.

STARTTLS wurde als Erweiterung für bestehende Protokolle entwickelt, um TLS-Verschlüsselung für unterschiedliche Domains mit unterschiedlichen Zertifikaten auf einem Server anbieten zu können. Es wurde nicht mit der Zielstellung entwickelt, die Sicherheit von SSL/TLS zu erhöhen. Man sollte sich nicht irritieren lassen und evtl. schlussfolgern, dass Old-Style-SSL/TLS veraltet sein könnte.

Auch die IETF empfiehlt in RFC 8314,[22] SSL/TLS gegenüber STARTTLS zu bevorzugen.

Hinweis für Nutzer der Telekom-Router

Die aktuellen Versionen der DSL-Router, die von der Telekom bereitgestellt werden, haben ein Feature, um Spambogs das Versenden von E-Mails zu erschweren. SMTP-Verbindungen auf den Ports 25, 465 und 587 sind nur für eine Whitelist von Mail-Servern erlaubt. Die empfohlenen E-Mail-Provider sind nicht alle in der standardmäßig aktivierten Whitelist enthalten.

In der Router-Konfiguration kann man im Menüpunkt *Internet → Liste der sicheren E-Mail-Server* das Feature abschalten oder den SMTP-Server des Providers hinzufügen.

[21] https://heise.de/-206233
[22] https://tools.ietf.org/html/rfc8314

Dieses Feature wird auch bei einem Update der Firmware älterer Telekom-Router aktiviert. Wenn man trotz korrekter Konfiguration in Thunderbird keine E-Mails mehr versenden kann, sollte man einen Blick in die Konfiguration des Routers werfen.

9.4.2 Konfiguration des Assistenten zur Account-Erstellung

Wenn man in Thunderbird einen neuen E-Mail-Account einrichten möchte, startet der Assistent zur Account-Konfiguration. Der Assistent versucht, die Einstellungen für die Mailserver (SMTP, POP3, IMAP) automatisch anhand der E-Mail-Adresse zu ermitteln, und geht dabei wie folgt vor:

1. Als erstes schaut der Assistent in der lokalen Installation nach, ob er die Daten für den Provider im Verzeichnis *<Installdir>/isp/* findet. Wenn er eine passende XML-Datei finden würde, wäre alles ok und die weiteren Schritte würden entfallen. Leider enthält Thunderbird keine Konfigurationsdateien für die E-Mail-Provider. Wir haben eine zusammengestellt: man kann sich das entsprechende Archiv von der Adresse https://www.privacy-handbuch.de/download/mailprovider-db.tar.bz2 herunterladen, entpacken und ins Unterverzeichnis *isp* der Thunderbird-Installation kopieren.

2. Wenn in der lokalen Installation keine passenden Daten für den Provider gefunden wurden, sucht der Assistent die Konfiguration beim E-Mail-Provider via unverschlüsseltem(!) HTTP-Request unter der URL *http://autoconfig.provider.tld/mail/config-v1.1.xml* und hängt standardmäßig die E-Mail-Adresse als Parameter an. Proxy-Einstellungen werden dabei ignoriert (falls man einen anonymen E-Mail-Account via Tor-Proxy nutzen wollte, wäre man damit praktisch deanonymisiert).

   Mit folgenden Parametern in den *Erweiterten Einstellungen* kann man HTTPS-Verschlüsselung für den Download der Autoconfig erzwingen und das Senden der E-Mail-Adresse vermeiden:

   ```
   mailnews.auto_config.fetchFromISP.sslOnly          = true
   mailnews.auto_config.fetchFromISP.sendEmailAddress = false
   ```

   Wenn man keine Autoconfig-Datei vom Provider holen möchte, könnte man das Feature auch abschalten. Dies ist aber meiner Meinung nach keine gute Idee bei normaler Nutzung des E-Mail-Accounts, da die Autokonfiguration die Erstellung des E-Mail-Accounts wirklich vereinfacht und Fehler vermeidet:

   ```
   mailnews.auto_config.fetchFromISP.enabled = false
   ```

   Sinnvoll ist es, den Download der Exchange-Autoconfig abzuschalten:

   ```
   mailnews.auto_config.fetchFromExchange.enabled = false
   ```

3. Wenn beim Provider nichts gefunden wird, fragt der Assistent bei der Mozilla ISP Database via SSL-verschlüsseltem HTTPS-Request an, ob dort eine Konfigurationsdatei vorhanden ist.

   Wenn man dieses Feature nicht nutzen will, könnte man in den *Erweiterten Einstellungen* die URL für die Mozilla ISP Database auf einen Webserver setzen, der einen sauberen HTTP-Fehler *404 – nicht gefunden* liefert. Unter Linux könnte man z. B. den CUPS-Daemon dafür missbrauchen:

```
mailnews.auto_config_url = http://localhost:631/fake404/
```

4. Wenn auch das keinen Erfolg hat, dann versucht der Assistent, die Einstellungen zu erraten, und fragt bei Mozilla nach dem MX-Record für den E-Mail-Provider. Da die Ergebnisse meist unbrauchbar sind, kann man dieses Feature deaktivieren:

   ```
   mailnews.auto_config.guess.enabled = false
   mailnews.mx_service_url            = http://localhost:631/fake404/
   ```

   Wenn man das Ausprobieren gängiger Namen nutzen möchte, sollte man es auf SSL-Verschlüsselung beschränken:

   ```
   mailnews.auto_config.guess.sslOnly = true
   ```

9.4.3 E-Mail-Account einrichten

Nachdem man die Konfiguration für den Assistenten etwas datenschutzfreundlich angepasst hat, kann man einen neuen E-Mail-Account erstellen.

1. Im ersten Schritt gibt man einen Namen, die E-Mail-Adresse und das Passwort für den Login an.
2. Anhand der E-Mail-Adresse und der Daten in der lokal installierten Datenbank oder der Autokonfiguration der Mailprovider findet der Assistent i. d. R. die nötigen Einstellungen.
3. Man kann meist zwischen IMAP- und POP3-Accounts wählen. Wenn man auf den Button *Fertig* klickt, wird das Passwort geprüft und der Account erstellt.

Hinweis 1: Bei den guten E-Mail Providern wie mailbox.org oder Posteo kann man einen oder mehrere E-Mail Alias(es) einrichten und als Adressen für die E-Mail Kommunikation nutzen. Die Hauptadresse des Accounts, die man für den Login verwendet, hält man geheim.

(Bei Providern mit geringeren Sicherheitsansprüchen wie GMX, Web.de oder Telekom bietet das keine Verbesserung, da man dort auch jeden Alias für den Login verwenden kann.)

Wenn man einen Alias als Adresse verwendet, muss man im letzten Schritt des Assistenten *Manuell einrichten* anklicken und als Benutzernamen für den Login die Hauptadresse eintragen.

Hinweis 2: Die meisten E-Mail-Provider fordern ein Passwort für die Authentifizierung. Im Mai 2022 hat Google als erster Provider OAuth2 eingeführt, was auch Zwei-Faktor-Authentifizierung in Thunderbird ermöglicht. Office365 folgte wenig später. Die OAuth2-Authentifizierung erfordert die Freigabe von Cookies für die Authentifizierung beim Provider.

Wenn die Cookies allgemein blockiert werden (z. B. wenn die Konfiguration vom PrHdb-Team für Thunderbird übernommen wurde), muss man zuerst für den OAuth-Provider in den Einstellungen unter *Datenschutz & Sicherheit* eine Ausnahme für Cookies definieren.

- Für Google Mail muss man Cookies für *https://accounts.google.com* erlauben.
- Für Office365 muss man Cookies für *https://login.microsoftonline.com* erlauben.

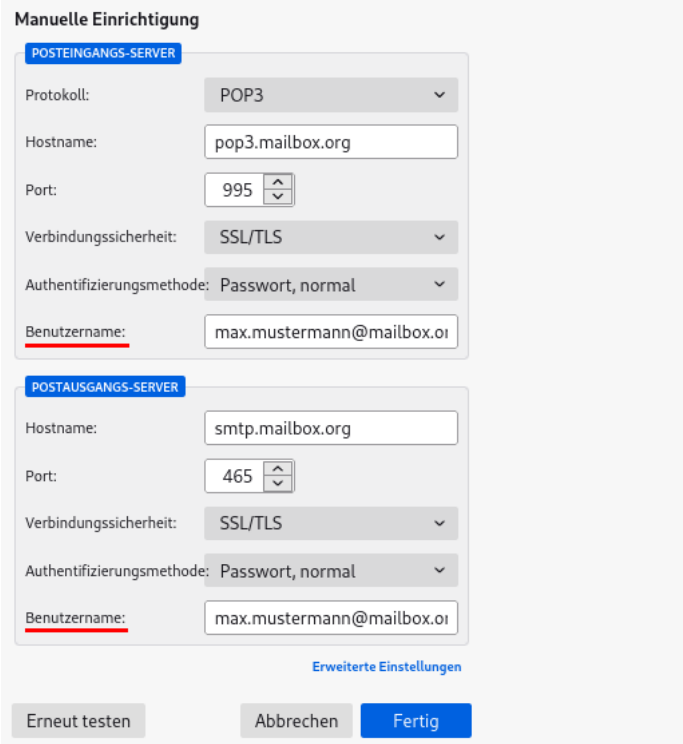


Abbildung 9.4: Anpassen der Log-in-Daten für die Mailserver bei der Verwendung eines Alias als Adresse

9.4.4 Lesen von E-Mails

Mit der Verwendung von HTML in E-Mails steht dem Absender ein ganzes Bestiarium von Möglichkeiten zur Beobachtung des Nutzers zur Verfügung: HTML-Wanzen, Java Applets, JavaScript, Cookies usw. Die Firma ReadNotify beispielsweise nutzt diese Möglichkeiten, um E-Mails für die Beobachtung des Empfängers zu präparieren (User-Tracking).

Der *E-Mail-Privacy-Test*[23] demonstriert viele Trackingmöglichkeiten. Nach der Verifikation der E-Mail-Adresse kann man sich eine Testmail schicken und wenn man diese Mail im E-Mail-Client öffnet, sieht man, welche Trackingmöglichkeiten ausgenutzt werden können.

Standardmäßig blockiert Thunderbird (fast) alle Trackingelemente und auch Spam-Mails in der HTML-Ansicht. Trotzdem ist es empfehlenswert, E-Mails als Plain Text zu lesen. Die Option findet man im Menüpunkt *Ansicht* → *Nachrichtentext* (Abb: 9.5). Das erleichtert auch die Erkennung von Phishing-E-Mails.

Alternativ kann könnte man in den erweiterten Einstellungen folgende Werte setzen:

```
mailnews.display.prefer_plaintext = true
mailnews.display.html_as = 1
```

Die Option *Anhänge eingebunden anzeigen* im Menü *Ansicht* sollte man ebenfalls deaktivieren, um gefährliche Anhänge nicht schon beim Lesen einer E-Mail automatisch zu öffnen. Der alte Trick mit einem Virus in der E-Mail wird noch immer genutzt, insbesondere wenn man ein Opfer gezielt angreifen will, um den Rechner mit Trojanern zu infizieren.

In der erweiterten Konfiguration kann man dafür folgenden Parameter setzen:

[23] https://emailprivacytester.com/

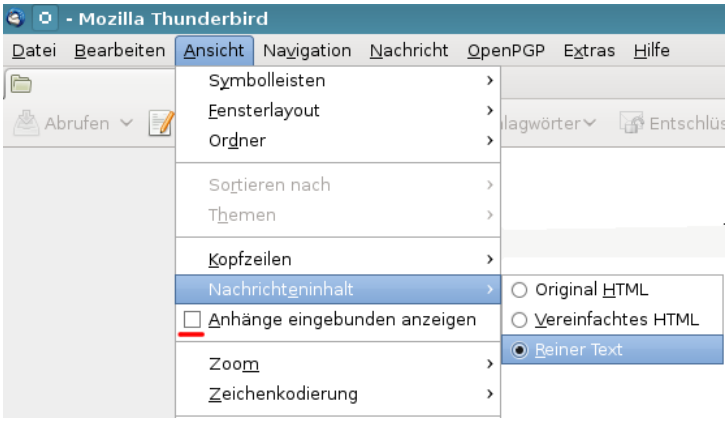


Abbildung 9.5: E-Mails als reinen Text darstellen

```
mail.inline_attachments = false
```

Es ist nicht immer möglich oder intuitiv verständlich, E-Mails als Plain Text zu lesen. Viele Newsletter sind nur als HTML-Mail lesbar, eBay verwendet bspw. ausschließlich HTML-Mails. In der Regel enthalten diese HTML-Mails mehrere Trackingelemente.

- Um diese E-Mails trotzdem lesen zu können (wenn auch nicht in voller Schönheit), kann man die Ansicht *Vereinfachtes HTML* nutzen. Man muss danach allerdings auch selbst wieder *Reinen Text* zurückschalten.
- Das Add-on *Allow-HTML-Temp* blendet in der Funktionsleiste über jeder E-Mail einen Button ein, mit dem man temporär die HTML-Ansicht aktivieren kann. Die Ansicht wird automatisch wieder auf die Standardansicht zurückgeschaltet, wenn man zur nächsten E-Mail wechselt.

  Man kann auch eine Tastenkombination für die Aktivierung der HTML-Ansicht definieren.
- Außerdem können folgende Features in den *Erweiterten Einstellungen* deaktiviert werden, die jedoch nur für die Darstellung von HTML-E-Mails in der Ansicht *Orginal HTML* relevant sind, oder für andere Komponenten, die den HTML-Viewer nutzen:

```
network.cookie.cookieBehavior          =  2
beacon.enabled                         =  false
layout.css.visited_links_enabled       =  false
media.hardware-video-decoding.enabled  =  false
media.navigator.enabled                =  false
gfx.downloadable_fonts.enabled         =  false
network.IDN_show_punycode              =  true
network.http.sendRefererHeader         =  0
security.family_safety.mode            =  0
```

9.4.5 Sichere Konfiguration als E-Mail-Client

Einige Hinweise für die sichere Nutzung des Mediums E-Mail mit Mozilla Thunderbird:

- Die Passwörter für die E-Mail-Accounts speichert Thunderbird in einer lokalen Datenbank (DB). Um missbräuchlichen Zugriff auf diese Daten zu vermeiden, kann man ein Masterpasswort konfigurieren. Die Passwort-DB von Thunderbird wird dann mit dem Masterpasswort verschlüsselt. Das Masterpasswort (bzw. Hauptpasswort) aktiviert man in den Einstellungen in der Sektion *Datenschutz & Sicherheit* (bevor man einen E-Mail-Account einrichtet).

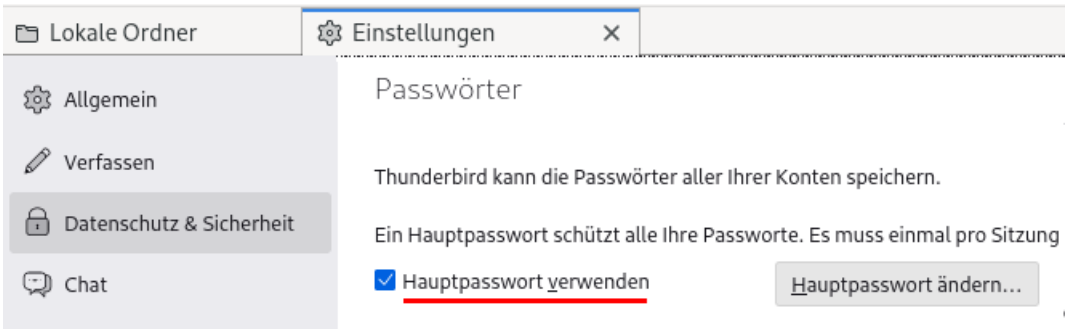


Abbildung 9.6: Masterpasswort in Thunderbird aktivieren

Zukünftig wird Thunderbird beim jedem Start nach dem Masterpasswort fragen, um damit die Passwörter für die E-Mail-Server und OpenPGP-Schlüssel zu entschlüsseln.

Um Verwirrungen durch Überkomplexität zu vermeiden, könnte man das gleiche Master- bzw. Hauptpasswort für alle lokale Passwort-DBs verwenden (Firefox-Passwort-DB, Keepass-DB usw.), da der Angriffsvektor ähnlich ist. Ein Angreifer hat Zugriff auf alle lokalen Passwort-Datenbanken oder (hoffentlich) auf keine. Das gilt aber nur für lokal gespeicherte Daten. Für Online-Accounts sind immer unterschiedliche Passwörter zu verwenden!

- Im Kopf einer E-Mail kann man zusätzliche Informationen anzeigen lassen:

  1. Ein E-Mail-Absender besteht aus einem Namen und der E-Mail-Adresse. Standardmäßig zeigt Thunderbird nur den Namen an. Informativer und sicherer ist es, die vollständige E-Mail-Adresse mit anzuzeigen. Das aktiviert man in den *Erweiterten Einstellungen* mit folgender Option:

     ```
     mail.showCondensedAddresses = false
     ```

  2. Eine E-Mail kann den Absender im FROM-Header und/oder im Header SENDER enthalten. Wenn beide angegeben sind, zeigt Thunderbird nur den FROM-Header an. Ein Angreifer könnte das nutzen, um eine E-Mail mit gefakten S/MIME-Zertifikaten als signiert erscheinen zu lassen. Um diesen Angriff zu erkennen, kann man sich beide Absenderinformationen anzeigen lassen (wenn vorhanden) und sollte stutzig werden, wenn sie unterschiedlich sind:

     ```
     mailnews.headers.showSender = true
     ```

  3. Die Anzeige des E-Mail-Programms, das der Absender verwendet, ist immer mal wieder interessant. Diese Anzeige kann man mit folgender Option in den *Erweiterten Einstellungen* aktivieren:

     ```
     mailnews.headers.showUserAgent = true
     ```

  4. Thunderbird 115+ bietet die Möglichkeit, das Senden der User-Agent Kennung im Kopf jeder E-Mail abzuschalten und potentiellen Angreifern damit keine Informationen über die zum Lesen von E-Mails verwendete Software + Version zu liefern:

```
mailnews.headers.sendUserAgent = false
```

- Alle Bilder in HTML-Mails, die von einem externen Server geladen werden, können direkt mit der E-Mail-Adresse des Empfängers verknüpft sein. Anhand der Logdaten kann der Absender erkennen, wann und wo die E-Mail gelesen wurde. Einige Newsletter verwenden auch HTML-Wanzen. Im Newsletter von Paysafecard findet man beispielsweise ganz unten eine kleine 1x1-Pixel Wanze, die offenbar mit einer individuellen, nutzerspezifischen URL von einem Trackingservice geladen wird:

  ```
  <IMG src="http://links.mkt3907.com/open/log/43.../1/0">
  ```

  Easyjet.com (ein Billigflieger) kann offenbar die Aufrufe seiner Newsletter selbst zählen und auswerten. In den E-Mails mit Informationen zu gebuchten Flügen findet man folgende kleine Wanze am Ende der Mail:

  ```
  <IMG src="http://mail.easyjet.com/log/bEAS001/mH9..." height=0 width=0
  ↪ border=0>
  ```

  Um Tracking mit Bildern und HTML-Wanzen zu verhindern, kann man in den *Erweiterten Einstellungen* das Laden externer Bilder blockieren:

  ```
  permissions.default.image  =  2
  ```

  Auch andere Medienformate können von einem externen Server geladen und als Wanzen genutzt werden. Einen derartigen Einsatz von Audio- oder Videodateien habe ich bisher nicht gefunden, aber technisch wäre es möglich. Man kann das Laden von Videos und Audiodateien mit folgenden Parametern unterbinden:

  ```
  media.webm.enabled  =  false
  media.wave.enabled  =  false
  media.ogg.enabled   =  false
  ```

- Die Links in HTML-Mails führen oft nicht direkt zum Ziel, sondern werden ebenfalls über einen Trackingservice geleitet, der jeden Aufruf des Links individuell für jede Empfängeradresse protokollieren kann. Als Beispiel soll ein Link aus dem Paysafecard-Newsletter dienen, der zu einem Gewinnspiel bei Paysafecard führen soll:

  ```
  <a href="http://links.mkt3907.com/ctt?kn=28&ms=3N...">Gewinne Preise
  ↪ im Wert von 10.000 Euro</a>
  ```

  Diesem Tracking kann man nur entgehen, wenn man diese Links in HTML-Mails nicht aufruft! Der Trackingservice hat die Möglichkeit, Logdaten von verschiedenen E-Mails zu verknüpfen und evtl. auch das Surfverhalten einzubeziehen. Wichtige Informationen findet man auch auf der Webseite des Absenders.

- JavaScript wird in E-Mails und in der RSS-Feed-Ansicht generell nicht ausgeführt. Nur wenn man die Webseiten-Ansicht bei RSS-Feeds aktiviert oder Webseiten in Thunderbird aufruft (was eigentlich fast nie vorkommt), wird JavaScript-Code ausgeführt.

  Außerdem wird JavaScript für die OAuth-2.0-Authentifizierung (Zwei-Faktor-fähig) bei einigen E-Mail-Providern wie Google Mail oder Office365 benötigt. Deshalb ist JavaScript nicht generell deaktiviert, sondern nur einige Optionen zur Verbesserung der Sicherheit:

```
javascript.options.baselinejit       = false
javascript.options.ion               = false
javascript.options.native_regexp     = false
```

- Im SMTP-Dialog mit dem Mailserver beim Versenden einer E-Mail sendet Thunderbird im EHLO-Kommando standardmäßig die lokale IP-Adresse:

  ```
  SSL/TLS Handshake zwischen Client und Server
  Client: EHLO 192.168.23.44
  ```

  Viele Mailserver vermerken diese lokale IP-Adresse aus dem EHLO-Kommando im ersten Received-Header der E-Mail zusammen mit der externen IP-Adresse, die der Mailserver sieht, und teilen sie damit auch Dritten mit:

  ```
  Received: from cefige3264.dynamic.kabel-deutschland.de
  ↪  ([188.192.92.109] helo=[192.168.23.44]) by smtp.server.tld
  ```

  Um zu vermeiden, dass diese Information veröffentlicht wird, kann man in den *Erweiterten Einstellungen* eine neue String-Variable anlegen und einen Fake definieren:

  ```
  mail.smtpserver.default.hello_argument = [127.0.0.1]
  ```

  Datenschutzfreundliche E-Mail-Provider entfernen den ersten Received-Header vollständig, da er nicht nur die lokale IP-Adresse aus dem internen Netzwerk enthält, sondern auch die externe IP-Adresse, die Hinweise auf den Aufenthaltsort des Absenders liefert und von Datensammlern mit dem Surfprofil verknüpft werden kann.

- In dem Adressbuch *Gesammelte Adressen* werden die E-Mail-Adressen der Empfänger aus den versendeten E-Mails gesammelt. Diese E-Mail-Adressen stehen dann für die Autocomplete-Funktion zur Verfügung, wenn man beim Schreiben einer E-Mail die Empfängeradressen eingibt.

  Wenn man die E-Mail-Adressen der Empfänger nicht automatisiert speichern möchte, kann man das Feature in den Einstellungen in der Sektion *Verfassen* abschalten.

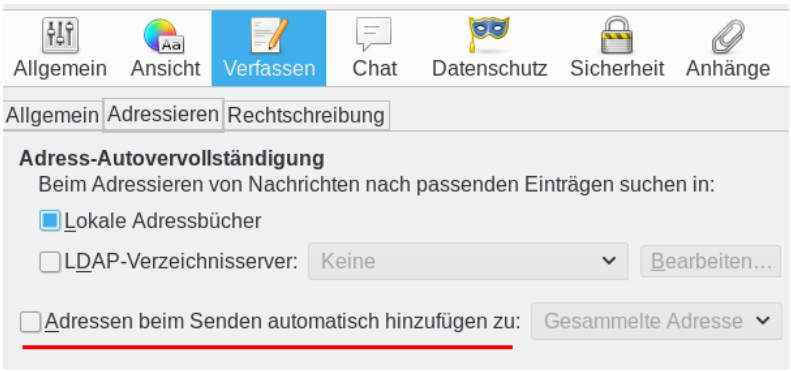


Abbildung 9.7: Sammeln von E-Mail-Adressen abschalten

In den *Erweiterten Einstellungen* kann man folgenden Wert setzen:

```
mail.collect_email_address_outgoing = false
```

Dann muss man sich aber selbst um die Pflege des Adressbuches kümmern.

- Die *extension blocklist* kann Mozilla nutzen, um einzelne Add-ons in Thunderbird zu deaktivieren. Es ist praktisch ein Kill-Switch für Add-ons. Beim Aktualisieren der Blockliste werden außerdem detaillierte Informationen an Mozilla übertragen.

  Ich mag es nicht, wenn jemand irgendetwas remote auf meinem Rechner deaktiviert oder deaktivieren könnte. In den *Erweiterten Einstellungen* kann man es abschalten:

  ```
  extensions.blocklist.enabled = false
  ```

- Thunderbird kontaktiert täglich den AMO-Server von Mozilla und sendet eine genaue Liste der installierten Add-ons. Als Antwort sendet der Server Statusupdates für die installierten Add-ons. Diese Funktion ist unabhängig vom Update Check für Add-ons, es ist nur eine zusätzliche Datensammlung von Mozilla. In den *erweiterten Einstellungen* kann man dieses Feature abschalten:

  ```
  extensions.getAddons.cache.enabled = false
  ```

- Alle Übertragungen von Telemetriedaten, Healthreport usw. an Mozilla unterbindet man ab Thunderbird 45 mit folgendem globalen Kill-Switch:

  ```
  datareporting.policy.dataSubmissionEnabled  = false
  datareporting.healthreport.uploadEnabled    = false
  ```

  Außerdem können einige Funktionen zusätzlich (redundant) deaktiviert werden:

  ```
  toolkit.telemetry.archive.enabled     = false
  toolkit.telemetry.bhrPing.enabled     = false
  toolkit.telemetry.updatePing.enabled  = false
  toolkit.telemetry.unified             = false
  ```

- Die Nutzung der Safebrowsing-Funktion deaktiviert man in Thunderbird genau wie in Firefox ESR. Gegen Phishing-Angriffe schützen technische Maßnahmen nicht vollständig, sondern in erster Linie das eigene Verhalten. Gegen Malware schützen ein achtsamer Umgang mit seltsamen Anhängen sowie regelmäßige Updates des Systems besser als Virenscanner oder Block-Listen.

  ```
  browser.safebrowsing.phishing.enabled                                = false
  browser.safebrowsing.malware.enabled                                 = false
  browser.safebrowsing.blockedURIs.enabled                             = false
  browser.safebrowsing.downloads.enable                                = false
  browser.safebrowsing.downloads.remote.enabled                        = false
  browser.safebrowsing.downloads.remote.block_dangerous                = false
  browser.safebrowsing.downloads.remote.block_dangerous_host           = false
  browser.safebrowsing.downloads.remote.block_uncommon                 = false
  browser.safebrowsing.downloads.remote.block_potentially_unwanted = false
  browser.safebrowsing.downloads.remote.url =
  ↪  https://s.%.c.invalid/download
  ```

  Es gibt allerdings auch die Ansicht, dass der Vorteil der Blockierung von Phishing-Webseiten die Nachteile überwiegt, vor allem bei Menschen mit geringer IT-Affinität.

- Bei jedem Start kontaktiert Thunderbird den Remote-Settings-Server von Mozilla, um die Hijack-Blacklist usw. zu aktualisieren. Das ist überflüssig, da diese Daten regelmäßig bei einem Update von Thunderbird aktualisiert werden. Man kann die ständigen Verbindungen zum Remote-Settings-Server unterbinden, indem man die Adresse des Servers auf eine ungültige URL setzt:

  ```
  services.settings.server = https://s.%.c.invalid/v1
  ```

9.4.6 Sichere Optionen für TLS-Verschlüsselung

Die Transportverschlüsselung (TLS) sichert die Verbindung zwischen einem E-Mail-Client und dem Mailserver des Providers gegen unerwünschte Lauscher. Seit der Einführung des Internets wird diese Verschlüsselung ständig weiterentwickelt und an neue, moderne Erkenntnisse der Kryptografie angepasst. Gleichzeitig werden jedoch aus Kompatibilitätsgründen alte, unsichere Versionen mitgeschleppt statt abgeschaltet.

1. In der aktuellen zivilen Kryptoanalyse gilt nur TLS 1.3 als uneingeschränkt sicher.

   Um den Handshake zur Aushandlung einer TLS-Verschlüsselung einige Millisekunden zu beschleunigen, wurde ein Zero-Round-Trip-Handshake in TLS 1.3 eingeführt. Viele Sicherheitsexperten sehen dieses Feature kritisch und als zukünftigen Angriffspunkt. In Thunderbird wurde bereits eine Option implementiert, um es abzuschalten.

2. Bei TLS 1.2 gibt es Einschränkungen bezüglich Sicherheit, da nicht alle in diesem Standard definierten Cipher-Suiten als uneingeschränkt sicher eingestuft werden. Gemäß IETF RFC 7525 und BSI TR-03116-4 gelten nur folgende Cipher-Suiten als sicher:

   ```
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
   ```

   Die neueren Cipher-Suiten mit CHACHA20-POLY1305 von D. J. Bernstein können ebenfalls als sicher eingestuft werden. Bei DHE-Cipher-Suiten ist zu beachten, dass diese Cipher nur sicher sind, wenn hinreichend große Diffie-Hellman-Parameter verwendet werden (was nicht immer gegeben ist). Es tritt immer wieder der Fehler auf, dass nur 1024-Bit-DH-Parameter verwendet werden, was die NSA seit 2010 on-the-fly knacken kann. Deshalb ist die Deaktivierung der DHE-Cipher empfehlenswert.

3. TLS 1.0/1.1 gelten als unsicher und werden von Thunderbird nicht mehr verwendet.

TLS-1.3-only-Konfiguration für Thunderbird

Am einfachsten aktiviert man eine sichere TLS-Verschlüsselung, wenn man nur TLS 1.3 verwendet. Dafür aktiviert man in den erweiterten Einstellungen folgende Option:

```
security.tls.version.min = 4
```

Außerdem kann man den Zero-Round-Trip-Handshake von TLS 1.3 deaktivieren:

```
security.tls.enable_0rtt_data = false
```

Diese Einstellung funktioniert mit E-Mail-Providern wie mailbox.org oder Posteo.de, die Wert auf Sicherheit legen. Bei vielen anderen E-Mail-Providern gibt es damit Probleme.

Der Server *download.mozilla.com* hat eine grottenschlechte TLS-Konfiguration und unterstützt kein TLS 1.3. Wenn Thunderbird darauf angewiesen ist, Updates von diesem Server zu beziehen (z. B. die MacOS-Version oder Portable Thunderbird), dann wird es beim Update-Prozess Probleme geben. Man könnte die jeweils aktuelle Version im Browser herunterladen und installieren oder man verwendet die TLS-1.2-secured-Konfiguration für Thunderbird.

Außerdem kann es Probleme beim Abrufen von einigen RSS-Feeds geben, wenn der Webserver, der den Feed bereitstellt, kein TLS 1.3 unterstützt.

TLS-1.2-secured-Konfiguration für Thunderbird

Standardmäßig erlaubt Thunderbird 78.x die Nutzung von TLS 1.2 und TLS 1.3. Wenn man noch TLS 1.2 nutzen muss, weil der E-Mail-Provider TLS 1.3 nicht flächendeckend auf allen Servern einsetzt, dann sollte man die schwachen Cipher-Suiten des TLS-1.2-Standards deaktivieren. Folgende Einstellungen sind in diesem Fall empfehlenswert:

```
security.tls.version.min = 3 (default ab Thunderbird 78.x)

security.ssl3.ecdhe_ecdsa_aes_128_sha = false
security.ssl3.ecdhe_ecdsa_aes_256_sha = false
security.ssl3.ecdhe_rsa_aes_128_sha   = false
security.ssl3.ecdhe_rsa_aes_256_sha   = false
security.ssl3.rsa_aes_128_sha         = false
security.ssl3.rsa_aes_256_sha         = false
security.ssl3.rsa_des_ede3_sha        = false
```

Weitere Einstellungen für die TLS-Verschlüsselung

- Insecure Renegotiation zu verbieten wird seit 2009 als Sicherheitsproblem eingestuft. Ein Angreifer kann die Login-Credentials (Username und Passwort) abschnorcheln, ohne die Verschlüsselung knacken zu müssen. Tools zum Ausnutzen der Insecure Renegotiation für einen Angriff gibt es auch als OpenSource (z. B. dsniff). Deshalb:

  ```
  security.ssl.require_safe_negotiation           = true
  security.ssl.treat_unsafe_negotiation_as_broken = true
  ```

- Strenges Certifikate Pinning erzwingen (z. B. für Add-on-Updates):

  ```
  security.cert_pinning.enforcement_level = 2
  ```

- Für RSS-Feeds und die Webseiten-Ansicht in Feeds kann man den HTTPS-only-Mode aktivieren und das Laden von unverschlüsseltem Content verbieten:

  ```
  security.mixed_content.upgrade_display_content = true
  dom.security.https_only_mode                   = true
  ```

Verbindungsprobleme mit sicheren TLS-Einstellungen

Wenn man die in Abb. 9.8 gezeigte, schwer verständliche Fehlermeldung beim Abrufen oder Senden von E-Mails erhält, gibt es Probleme beim Aufbau einer sicheren Verbindung und man wechselt am besten den Mail-Provider.

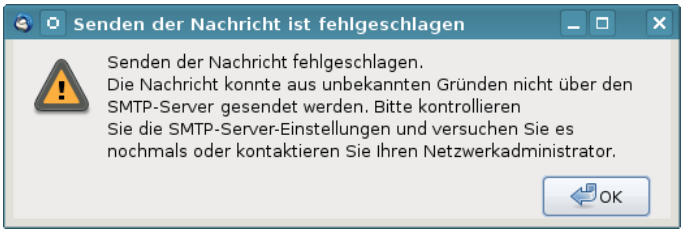


Abbildung 9.8: Fehlermeldung bei unsicherer Verbindung

9.4.7 Datenverluste vermeiden

Die folgenden Hinweise wurden von den Mozilla-Entwicklern erarbeitet, um den Nutzer bestmöglich vor Datenverlusten zu schützen:

- Das Antiviren-Programm ist so einzustellen, dass es den Profilordner von Thunderbird NICHT(!) scannt. Die automatische Beseitigung von Viren kann zu Datenverlusten führen.
- Der Ordner *Posteingang* sollte so leer wie möglich gehalten werden. Gelesene E-Mails sollten auf themenspezifische Unterordner verteilt werden.
- Die Ordner sollten regelmäßig komprimiert werden, um gelöschte E-Mails endgültig aus der MBOX zu entfernen und den Speicherplatz freizugeben.
  - In den Einstellungen in der Sektion *Erweitert* kann man eine automatische Komprimierung konfigurieren, sobald x MB Speicherplatz dadurch frei werden. Bei jedem Start prüft Thunderbird, ob die Ordner komprimiert werden können.
  - Alternativ kann man mit der rechten Maustaste auf einen Ordner klicken und den Punkt *Komprimieren* wählen. Während des Komprimierens sollten keine anderen Aktionen in Thunderbird ausgeführt werden.
- Regelmäßig sollten Backups des gesamten Profils von Thunderbird angelegt werden. Unter Linux ist *$HOME/.thunderbird* zu sichern, Unter WINDOWS sichert man *C:/Dokumente und Einstellungen/<NAME>/Anwendungsdaten/Thunderbird*.

9.4.8 Wörterbücher installieren

Für die automatische Rechtschreibkontrolle beim Schreiben einer E-Mail muss man die nötigen Wörterbücher für die bevorzugten Sprachen installieren. Man kann neben dem immer vorhandenen Englisch die Wörterbücher für weitere Sprachen hinzufügen.

- Unter Linux nutzen Thunderbird und Firefox die Hunspell-Wörterbücher für die Rechtschreibkontrolle. Mit dem bevorzugten Paketmanager kann man die Wörterbücher für verschiedene Sprachen installieren. Für Debian/Ubuntu könnte man *apt* verwenden. Neben *hunspell-de-de* für deutsches Deutsch gibt es auch Pakete für Österreicher (*hunspell-de-at*) oder Schweizer (*hunspell-de-ch*):

```
> sudo apt install hunspell-de-de
```

Fedora und QubesOS fassen alle deutschen Sprachen in einem Paket zusammen:

```
> sudo dnf install hunspell-de
```

- Für andere Betriebssysteme kann man fehlende Wörterbücher von der Webseite für Language-Tools[24] herunterladen und in Thunderbird als Add-on installieren oder man klickt einfach auf den Link im Konfigurationsdialog, um weitere Wörterbücher zu installieren.

  In den Einstellungen in der Sektion *Verfassen* kann man die bevorzugte Sprache als Standard konfigurieren. Die Auswahl der Sprache kann man beim Schreiben einer Mail jederzeit ändern.

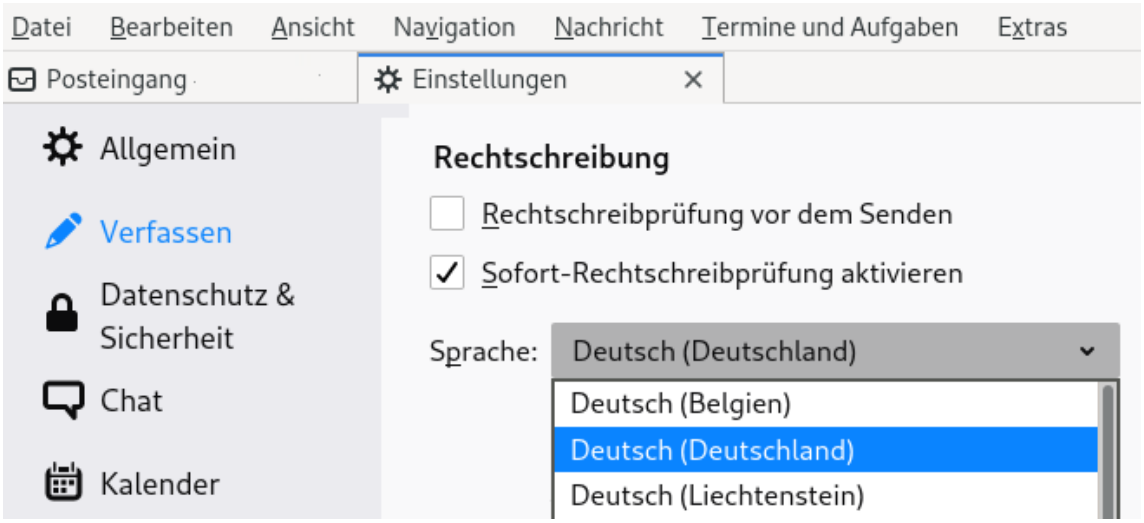


Abbildung 9.9: Bevorzugte Sprache für Rechtsschreibprüfung auswählen

9.4.9 RSS-Feeds

RSS-Feeds bieten die Möglichkeiten, sich schnell über Neuigkeiten in häufig gelesenen Blogs zu informieren ohne die Webseiten einzeln abklappern zu müssen. Thunderbird enthält einen RSS-Reader, den man dafür nutzen kann.

Um mehrere interessante RSS-Feeds zu sammeln, erstellt man in der *Konten-Verwaltung* ein neues Konto und wählt den Typ *Anderes Konto hinzufügen...*.

[24] https://addons.mozilla.org/de/thunderbird/language-tools/

Im zweiten Schritt wählt man den Typ *Blogs und RSS-Feeds* und danach eine beliebige Kontenbezeichnung.

In den Einstellungen für das RSS-Feed-Konto kann man festlegen, in welchem Intervall die Feeds abgerufen werden und ob sie beim Start von Thunderbird aktualisiert werden sollen. Danach kann man die *Abonnements verwalten* und die Adressen der RSS-Feeds hinzufügen. Man kopiert die URL des RSS-Feeds von der Webseite des Blogs in das Feld für die Feed-URL und klickt auf den Button *Hinzufügen* wie in Abb. 9.10 dargestellt.

Abbildung 9.10: RSS-Feed hinzufügen

Die Neuigkeiten aus den Blogs kann man zukünftig wie E-Mails lesen. Dabei kann man eine simple Textanzeige wählen oder die Ansicht als Webseite. Wer die Ansicht als Webseite bevorzugt, sollte JavaScript, Cookies und andere Tracking-Elemente deaktivieren. Zum Kommentieren muss man allerdings die Webseite des Blogs im Browser aufrufen.

Aus Sicherheitsgründen ist es empfehlenswert, den RSS-Feed als Plain Text zu lesen und nicht als Webseite zu laden. Das sieht nicht so hübsch aus, aber man verringert die Angriffsmöglichkeiten durch bösartigen Schadcode oder Media-Elemente, wenn die Webbrowser-Komponente von Thunderbird kritische Lücken enthält (z. B. CVE-2016-9899 und CVE-2016-9893).

```
rss.display.prefer_plaintext        =  true
rss.display.disallow_mime_handlers  =  3
rss.display.html_as                 =  1
rss.show.content-base               =  1
```

Bei jedem Start kontaktiert Thunderbird standardmäßig die Webserver, auf denen die RSS-Feeds liegen, und sucht nach den Favicons der Webseite für die Darstellung in der Liste der Feeds. Dieses Verhalten kann man Thunderbird abgewöhnen, indem man folgenden Parameter in den Einstellungen setzt:

```
browser.chrome.site_icons  =  false
```

9.4.10 Große Dateien verschicken

Dateien bis zu 10-20 MB kann man in der Regel als E-Mail-Anhang versenden (bei manchen Mail-Providern etwas mehr, bei einigen etwas weniger). Größere Dateien bis zu einige GB kann man im Webbrowser bei Cloud Prividerb hochladen, wo sie für begrenzte Zeit zum Download bereitstehen. Nach dem Upload bekommt man einen Link für den Download, den man dann zusammen mit einem optionalen Passwort per E-Mail verschicken kann.

- Auf diesen **1-Klick-Hostern** kann man große Dateien zum Download bereitstellen:
  - https://send.adminforge.de/ (bis zu 8 GB, Dateien sind Ende-zu-Ende-verschlüsselt, Schlüssel in Download-URL enthalten, Passwortschutz möglich, Uploads können bis zu 7 Tage verfügbar sein);
  - https://upload.adminforge.de/ (bis zu 2 GB, Dateien sind Ende-zu-Ende-verschlüsselt, Schlüssel in Download-URL enthalten, Passwortschutz möglich, Uploads können bis zu 30 Tage verfügbar sein);
  - https://upload.disroot.org/ (bis zu 2 GB, Dateien sind Ende-zu-Ende-verschlüsselt, Schlüssel in Download-URL enthalten, Passwortschutz möglich, Uploads können bis zu 30 Tage verfügbar sein);
  - https://send.tresorit.com/ (bis zu 5 GB, Dateien sind Ende-zu-Ende-verschlüsselt, Passwortschutz für Downloads möglich, benötigt eine E-Mail-Adresse, aber Wegwerf-Adressen wie AnonBox.net funktionieren, Uploads werden nach 7 Tagen oder nach 10 Downloads gelöscht);
  - https://nowtransfer.de/ (von adminForge.de, Uploads bis zu 8 Wochen verfügbar);
  - https://1fichier.com/ (bis zu 300 GB, Passwortschutz für Downloads möglich, bis zu 15 Tagen verfügbar).

  Hinweis: Wenn man einen Downloadlink ohne Passwortschutz via E-Mail versendet, verursacht der Virenscanner des E-Mail Providers möglicherweise den ersten Download und beim Versand via Messenger wird möglicherweise ein Link Preview erstellt, der ebenfalls als Download gezählt wird. Man sollte ohne Passwortschutz mindestens zwei Downloads vor dem Löschen zulassen.

- Mit **Filelink Add-ons** kann man den Upload in Thunderbird integrieren und große Anhänge beim Schreiben einer E-Mail hochladen (wenn man häufig große Dateien versendet).
  1. Als erstes muss man dafür ein passendes Filelink Add-on installieren. Empfehlenswert ist **Send** in Kombination mit einem vertrauenswürdigen Provider wie z.B. *send.adminForge.de*. Die Uploads werden bei diesem Filelink Add-on Ende-zu-Ende verschlüsselt auf dem Cloud Server gespeichert.
  2. In den *Einstellungen* in der Sektion *Verfassen* (ganz unten) ist der Filelink Provider zu aktivieren und zu konfigurieren. Für Send ist die URL des Provider anzugeben sowie die Defaultwerte für Anzahl der Downloads und max. Dauer der Speicherung.
  3. Wenn man beim Schreiben einer E-Mail eine große Datei anhängt, wird ein Hinweis eingeblendet. Man kann auf den Button *Filelink verwenden* klicken und nach Anpassung von Passwort, max. Downloads und Speicherdauer die Datei hochladen.

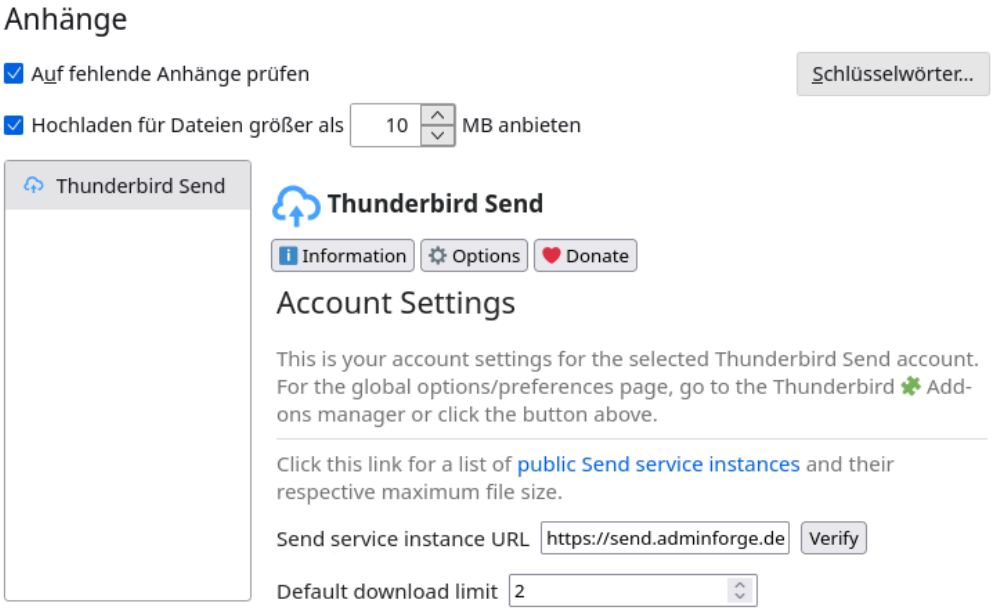
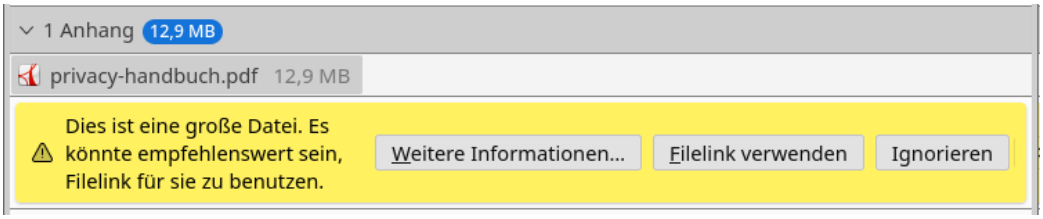


Abbildung 9.11: Filelink Add-on Send in den Einstellungen konfigurieren



Wenn man nur einen Download erlauben möchte, sollte man ein (simples) Passwort setzen, damit die Virescanner bei einigen E-Mail Providern keinen Download auslösen.

4. Nach dem Upload wird der Download Link automatisch in die E-Mail eingefügt.

- Einige E-Mail-Provider wie mailbox.org oder ProtonMail bieten einen eigenen Cloudspeicher, auf dem man größere Dateien (in Abhängigkeit von der Größe des Speichers) ablegen und einen Freigabelink erstellen kann, den man per E-Mail versendet.

  Bei mailbox.org kann man diese Funktion direkt beim Schreiben einer E-Mail nutzen, indem man die Option DriveMail für Anhänge aktiviert. Die Anhänge werden dann in den Cloudspeicher hochgeladen und in die E-Mail wird nur ein Link zum Download eingefügt.

  Mit den Optionen kann ein Passwort für den Zugriff vergeben und die Zeitdauer konfiguriert werden, für welche die Dateien zum Download verfügbar sein sollen, bevor sie automatisch gelöscht werden. Die Anhänge im Cloudspeicher DriveMail werden nicht(!) verschlüsselt.

9.4.11 Thunderbird Add-ons

Mit Add-ons kann man Thunderbird um kleine Funktionalitäten ergänzen, die praktisch sind. Um ein Add-on zu installieren, öffent man die Add-on Verwaltung und gibt den Namen des Add-ons im Suchfeld ein. <ENTER> öffnet einen neuen Tab zum Installieren des Add-ons.

allow-html-temp1.png

Ungender ersetzt ideologisch motivierte Sprachverhunzungen wie *Politiker*innen* oder *Panzerfahrer_Innen*, die man nicht aussprechen oder in andere Sprachen übersetzen kann, die

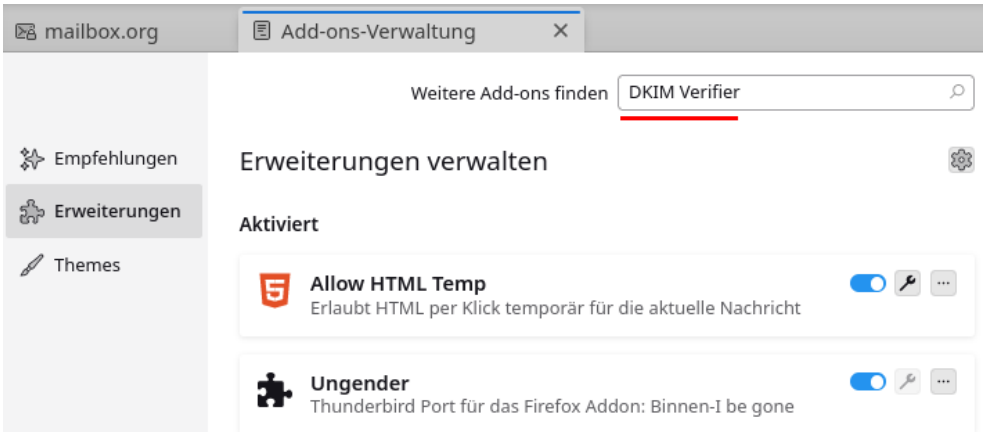


Abbildung 9.12: Add-on Verwaltung in Thunderbird

laut Duden kein korrektes Deutsch sind und auch vom Rat für Deutsche Rechtschreibung nicht empfohlen werden, durch das grammatikalische Generikum.

In privaten E-Mails ist es (in meinem Umfeld) unüblich zu gendern. In Mails von Firmen oder Banken kommt es gelegentlich vor, dass man als *Kunden:Innen* o.ä. genervt wird.

Allow-HTML-Temp blendet in der Funktionsleiste über jeder E-Mail einen Button ein, mit dem man temporär die HTML-Ansicht aktivieren kann. Die Ansicht wird automatisch wieder auf die Standardansicht zurückgeschaltet, wenn man zur nächsten E-Mail wechselt.

Man kann auch eine Tastenkombination für die Aktivierung der HTML-Ansicht definieren.

Nach der Installation kann man die Konfiguration des Add-on anpassen und wählen, zwischen welchen Ansichten man hin-und-her schalten möchte und ob in der temporären HTML Ansicht auch ext. Bilder angezeigt werden sollen oder Anhänge eingebunden dargestellt werden sollen (auf keinen Fall). Meistens reicht die restriktive Konfiguration zum besseren Lesen von E-Mails aus (Abb. 9.13).

Anhänge sollte man grundsätzlich nicht eingebunden darstellen, da das die Infektion mit Viren deutlich vereinfacht. Wenn externe Inhalte in der org. HTML Ansicht erlaubt werden, ergeben sich für die Absenden Trackingmöglichkeiten, wie der E-Mail Privacy Test zeigt.

DKIM Verifier eigt im Kopf der E-Mail das Ergebnis der Verifizierung der DKIM Signaturen an, die von dem versendenden E-Mail Server erstellt werden. Damit ist schnell prüfbar, ob die E-Mail wirklich von dem angegebenen Server versendet wurde (wenn eine DKIM Signatur vorhanden ist) und gefälschte Absender lassen sich leichter erkennen.

Das Add-on in den Einstellungen flexibel konfigurierbar. Die Anzeige der Absenderadresse kann man beispielsweise bunt einfärben usw. Für die Prüfung der DKIM Signaturen holt dass Add-on den öffentlichen DKIM Schlüssel des sendenden Mailservers aus dem DNS. Das kleine Schloss hinter dem Ergebnis der Signaturprüfung zeigt an, dass die DNS Information ebenfalls vertrauenswürdig und DNSSEC signiert ist. Das kann das Add-on aber nur prüfen, wenn *libunbound* als DNS Resolver verwendet wird, die man für Windows und MacOS extra installieren muss.

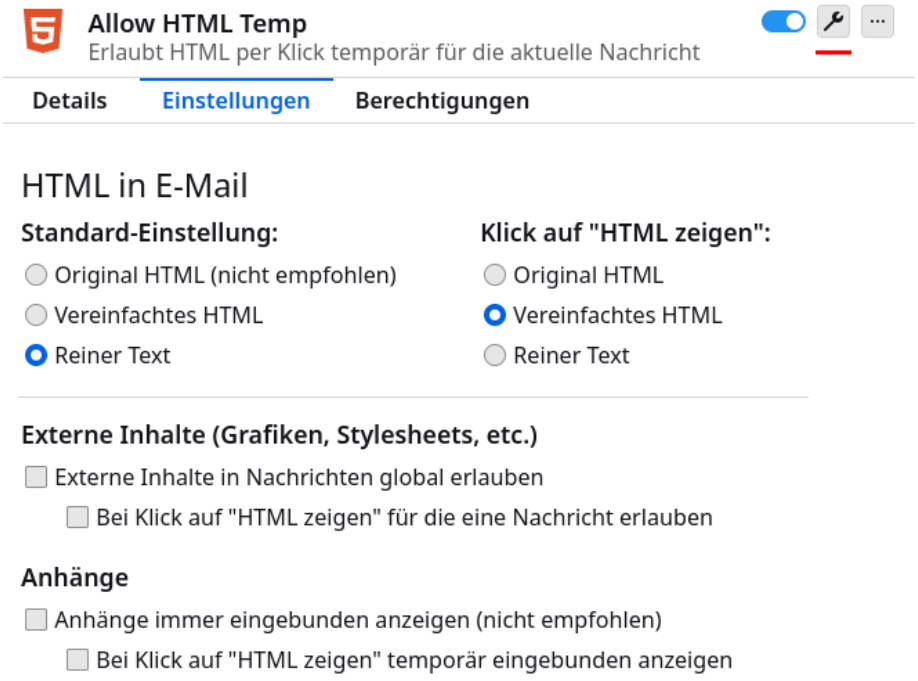


Abbildung 9.13: Restriktive Konfiguration für das Add-on Allow-HTML-Temp

9.5 Private Note

E-Mails werden auf dem Weg durch das Netz an vielen Stellen mitgelesen und ausgewertet. Ein Postgeheimnis existiert praktisch nicht. Kommerzielle Datensammler wie Google und Yahoo scannen alle Mails, die sie in die Finger bekommen. Geheimdienste wie NSA, SSSI, FRA oder BND haben Monitoring-Programme für den E-Mail-Verkehr.

Gelegentlich möchte man aber nicht, dass eine vertrauliche Nachricht von Dritten gelesen wird. Verschlüsselung wäre eine naheliegende Lösung. Das ist aber nur möglich, wenn Absender und Empfänger über die nötige Kompetenz verfügen.

Als Alternative kann man *PrivNote*[25] der Firma*insophia* nutzen. Man schreibt die Nachricht auf der Webseite des Anbieters. JavaScript muss dafür freigegeben werden. In den Optionen kann man festlegen, wann die Nachricht gelöscht werden soll, man kann zusätzlich ein Passwort für das Lesen setzen und eine E-Mail bekommen, wenn die Nachricht gelöscht wird.

Das zusätzliche Passwort ist nur sinnvoll, wenn es über einen unabhängigen Kanal zum Empfänger übertragen wird. Man könnte z. B. bei einem Treffen ein Passwort vereinbaren und es nutzen, bis man ein neues Passwort austauscht. Man könnte es mit jeder Nachricht ändern, so dass die aktuelle Nachricht immer das Passwort für die nächste Nachricht enthält. Man kann es beliebig kompliziert gestalten, solange beide Seiten den Überblick behalten. Es ist aber nicht sinnvoll, ein Passwort zusammen mit dem Link zum Lesen der Nachricht in der gleichen E-Mail zu schicken.

Wenn man auf den Button *Create note* klickt, wird ein Link generiert, unter dem man die Nachricht EINMALIG abrufen kann. Die Nachricht wird im Browser verschlüsselt auf dem Server gespeichert und nur der Link enthält den Key, um die Daten zu entschlüsseln.

Den Link kann man per E-Mail dem Empfänger der Nachricht senden. Er kann die Nachricht im Browser abrufen. Nach dem Abruf der Nachricht wird sie auf dem Server gelöscht, sie ist also

[25] https://privnote.com/

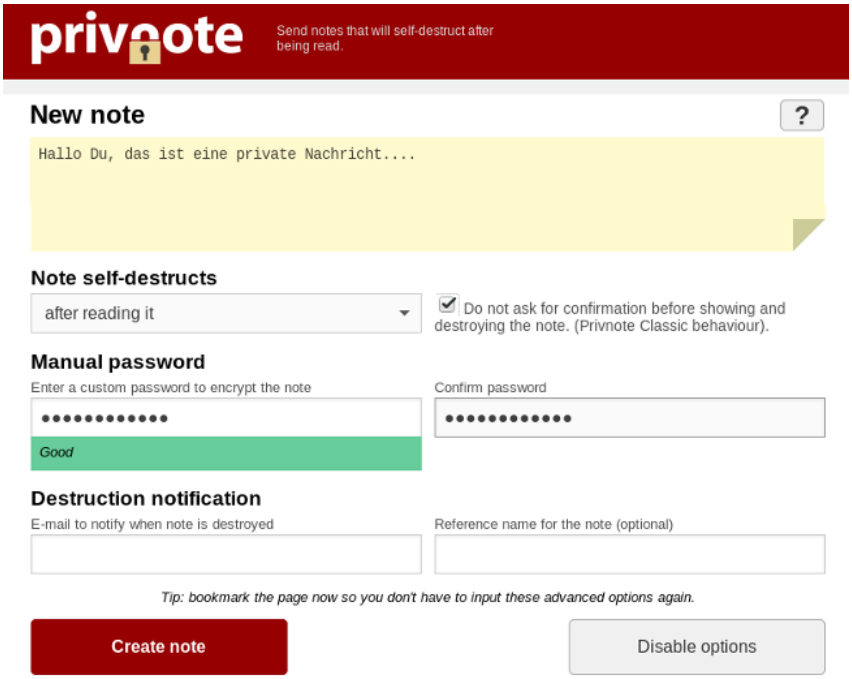


Abbildung 9.14: Eine Private Note schreiben

nur EINMALIG lesbar. Darauf sollte man den Empfänger hinweisen. Wenn der Empfänger die Nachricht nicht abruft, wird sie nach 30 Tagen gelöscht.

Man sollte den Link NICHT über Kanäle in Social Networks (z. B. Facebook) versenden. Wenn man nämlich dort auf den Link klickt, läuft im Hintergrund ein Crawl der Seite, bevor man weitergeleitet wird. Facebook holt sich die Nachricht und der Empfänger kommt zu spät.

PrivNote ist nicht kryptografisch abhörsicher wie die E-Mail-Verschlüsselung mit OpenPGP. Wenn ein Angreifer unbedingt den Inhalt der Nachricht lesen will, kann er die Nachricht vor dem Empfänger abrufen und über den Inhalt Kenntnis erlangen. Der eigentliche Empfänger kann nur den Angriff erkennen, da die Nachricht auf dem Server gelöscht wurde. Damit sind die Angebote für private Nachrichten geeignet, aber nicht für geheime oder streng vertrauliche Informationen.

Kapitel 10

E-Mails verschlüsseln

Weltweit wird der unverschlüsselte E-Mail-Verkehr systematisch gescannt. Mit *Echelon*, das auch zur Industriespionage und zum Abhören von NGOs verwendet wird, sind die NSA zusammen mit Abhörschnittstellen bei allen großen amerikanischen ISPs führend. Frankreich betreibt ein ähnliches System unter dem Namen *French ECHELON*.

Das russische Pendant zur NSA ist der SSSI (früher FAPSI). Der schwedische Geheimdienst FRA und das Schweizer Onyx Projekt nutzen Supercomputer zur Verarbeitung der abgeschnorchelten Datenmengen. Für Saudi-Arabien, Syrien, Iran, Tunesien und Ägypten wurden ebenfalls entsprechende Aktivitäten nachgewiesen und auch die *Great Firewall* von China verfügt über die nötigen Features.

In Deutschland wird der E-Mail-Verkehr im Rahmen der *Strategischen Fernmeldeaufklärung* von den Geheimdiensten gescannt. Eine von der G-10-Kommission genehmigte Stichwortliste mit 16.400 Begriffen (Stand 2010) wird für die automatisierte Vorauswahl verwendet, um nach Waffenhandel, Proliferation und Terroristen zu suchen. Im Jahr 2010 meldeten die Scanner 37 Mio. E-Mails als verdächtig. 2011 hat der BND es geschafft, die automatisierten Scanner mit einem Spamfilter zu kombinieren, so dass „nur noch“ 2,1 Mio. E-Mails als verdächtig gemeldet und kopiert wurden.

OpenPGP und S/MIME

OpenPGP und S/MIME (*Secure MIME Protokoll*) sind fast 20 Jahre alte Standards für E-Mail-Kryptografie. Sie können folgende Aufgaben erfüllen:

1. Mit dem **Verschlüsseln** von E-Mails wird die Vertraulichkeit des Inhalts der E-Mail gewährleistet. Eine Nachricht kann nur vom Empfänger mit dem passenden Schlüssel geöffnet und gelesen werden.
2. Mit dem **Signieren** von E-Mails wird die Authentizität der Nachricht gewährleistet. Anhand der Signatur kann der Empfänger prüfen, ob eine Mail wirklich von dem angegebenen Absender kommt und unterwegs nicht modifiziert wurde.
3. Die Metadaten im Header der E-Mail (Absender, Empfänger, verwendete Software, evtl. die IP-Adresse des Absenders usw.) werden durch diese beiden Verfahren nicht(!) verschleiert und können für die Kommunikationsanalyse verwendet werden.

OpenPGP und S/MIME nutzen **Asymmetrische Kryptografie**. Das heißt, es wird ein Schlüsselpaar mit unterschiedlichen Schlüsseln zum Verschlüsseln und zum Entschlüsseln verwendet. Das Grundprinzip ist einfach erklärt:

- Jeder Anwender generiert ein Schlüsselpaar bestehend aus einem geheimen und einem öffentlichen Schlüssel. Während der geheime Schlüssel sorgfältig geschützt nur dem Anwender zur Verfügung stehen sollte, ist der öffentliche Schlüssel an alle Kommunikationspartner zu verteilen.
- Wenn Beatrice eine verschlüsselte Nachricht an Anton senden will, nutzt sie den öffentlichen Schlüssel von Anton, um die Nachricht zu chiffrieren. Nur Anton kann den Inhalt der E-Mail mit seinem geheimen Schlüssel dechiffrieren und lesen.
- Wenn der Anton eine signierte E-Mail an Beatrice senden will, erstellt er eine Signatur (digitale Unterschrift) mit seinem geheimen Schlüssel. Beatrice kann mit dem öffentlichen Schlüssel von Anton die Unterschrift und damit die Echtheit der Nachricht verifizieren, da nur Anton Zugriff auf seinen geheimen Schlüssel haben sollte.

Verschlüsselung und Signatur können kombiniert werden. Dabei wird der Inhalt der Nachricht zuerst signiert und dann alles zusammen (Nachricht + Signatur) verschlüsselt.

PGP, GnuPG und S/MIME haben es in den letzten 20 Jahren nicht geschafft, eine massentaugliche Usability zu entwickeln. Wenn man erst einmal 20 Seiten Anleitung lesen muss, um die E-Mail-Verschlüsselung zu verstehen, die Software selbst konfigurieren, sich selbst die notwendigen Schlüssel erstellen oder beglaubigen lassen muss, sich um die Verteilung der Schlüssel selbst kümmern und es danach noch jedem Partner einzeln erklären muss, dann ist diese Krypto einfach nicht massentauglich.

Pretty Easy Privacy (PEP) und Autocrypt

PEP und Autocrypt hatten das Ziel, die Usability von OpenPGP zu verbessern und damit eine breitere Anwendung von E-Mail-Verschlüsselung zu ermöglichen. Bei Sicherheit und Flexibilität wurden teilweise erhebliche Einschränkungen in Kauf genommen, ohne dass jedoch das Ziel einer nennenswert größeren Verbreitung von OpenPGP erreicht wurde.

Bei **Pretty Easy Privacy** (PEP) sind die Einschränkungen moderat:

- Bei der Einrichtung eines Accounts erstellt PEP im Hintergrund automatisch ein Schlüsselpaar (RSA, 2048 Bit). Der private Key wird standardmäßig nicht mit einem Passwort gesichert, da die PEP-Entwickler es als überflüssiges und störendes Feature ansehen. Es wird eine Verschlüsselung der Festplatte empfohlen.

  (Optional kann man einen Passwortschutz für private Schlüssel aktivieren und muss dann alle Schlüssel neu erstellen.)
- PEP tauscht die öffentlichen Schlüssel automatisch als E-Mail-Attachment aus. Nach einer ersten, unverschlüsselten Mail (aktiver Modus) oder spätestens nach der zweiten ausgetauschten E-Mail (passiver Modus) werden alle weiteren E-Mails verschlüsselt. Den Erstkontakt zu verschlüsseln, ist nicht vorgesehen.

  Hinweis: E-Mails mit BCC Adressen werden nicht(!) verschlüsselt.
- Der Betreff und weitere Header werden standardmäßig verschlüsselt (Memoryhole).
- Auf der Gegenseite akzeptiert PEP den ersten Key von einem Kommunikationspartner und verwendet ihn zukünftig automatisch (trust in first use). Alle weiteren Keys werden verworfen, um Sicherheitsprobleme wie bei Autocrypt zu vermeiden. (Dem erfahrenen Anwender wird der Klick auf *OpenPGP-Schlüssel importieren* erspart.)

- Verifizierung von Schlüsseln ist anhand von Trustwords möglich, die über einen unabhängigen, sicheren Kanal oder bei einem Treffen verglichen werden müssen.
- PEP-Sync kann die Schlüssel zwischen mehreren Geräten synchronisieren.
- PEP verwendet statt GnuPG die eigene Implementierung *Sequoia PGP* als Backend.

Mit **Autocrypt**[1] wurde die Sicherheit von OpenPGP drastisch geschwächt, um den Austausch der Schlüssel zu vereinfachen. OpenPGP mit Autocrypt bietet keine sichere Verschlüsselung, sondern nur noch **some protection most of the time**. Außerdem wurden die Mail-Provider per Definition als vertrauenswürdig deklariert, damit wurde das wesentliche Ziel einer Ende-zu-Ende-Verschlüsselung über Bord geworfen. Der Schutz gegen den Mail-Provider war und ist jedoch das wesentliche Ziel jeder Ende-zu-Ende-Verschlüsselung.

Eine Ende-zu-Ende-Verschlüsselung, die nicht mehr gegen die Provider schützt, ist einfach überflüssig. Bedauerlicherweise ist Autocrypt in vielen Tools zur E-Mail-Verschlüsselung standardmäßig aktiviert, was OpenPGP für sicherheitskritische Anwendungen (beispielsweise Whistleblower) nutzlos gemacht hat.

In der Entwickler-Community sind die Ansichten gespalten. Bei dem Browser-Add-on Mailvelope wurde Autocrypt implementiert und standardmäßig aktiviert. Die Thunderbird-Entwickler haben diesen Schlüsseltausch nicht implementiert.

Mit **countermitm**[2] gibt es eine Erweiterung für den Autocrypt-Schlüsseltausch, die eine Verifizierung von Schlüsseln und ein *Network of Trust* einführt, um bei Autocrypt mögliche Man-in-the-Middle-Angriffe für verifizierte Schlüssel zu verhindern. *contermitm* gehört nicht zum Autocrypt-Standard und wird unabhängig davon entwickelt.

10.1 E-Mails verschlüsseln mit Thunderbird

Thunderbird stellt alle Features für die Verschlüsselung mit OpenPGP und S/MIME bereit:

Sichere Konfiguration: Der Efail-Angriff hat demonstriert, dass eine sichere Konfiguration des E-Mail-Clients eine notwendige Voraussetzung für sichere Verschlüsselung ist (E-Mails als Plain Text anzeigen, keine eingebundene Anzeige von Anhängen usw.).

Masterpasswort aktivieren: Thunderbird sichert die privaten Keys mit einer zufälligen Passphrase, die in der Passwortdatenbank gespeichert wird. Es ist daher wichtig, die Passwortdatenbank mit einem Masterpasswort zu sichern.

Schlüssel erstellen: Um die Verschlüsselung von E-Mails zu aktivieren, muss man in den Kontoeinstellungen in der Sektion *Ende-zu-Ende-Verschlüsselung* ein PGP-Schlüsselpaar generieren oder importieren oder ein S/MIME-Zertifikat importieren.

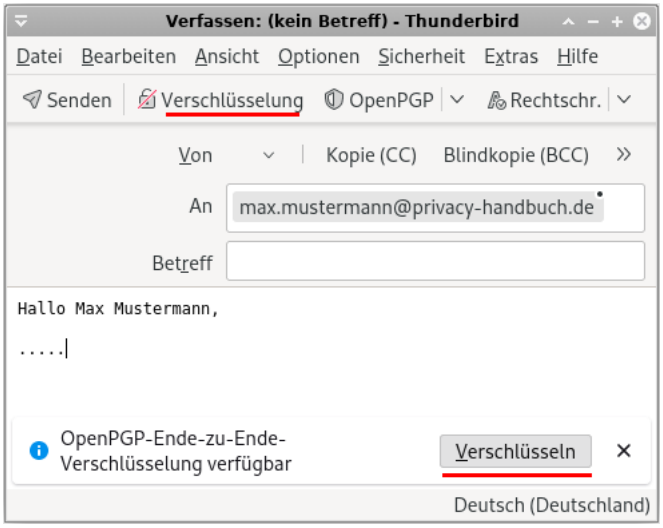
Schlüssel verteilen: Um verschlüsselt mit Kommunikationspartnern via E-Mail kommunizieren zu können, muss man die öffentlichen Schlüssel (public keys) austauschen. Bei modernen Krypto-Messengern wird das im Hintergrund automatisch erledigt. Bei der E-Mail-Verschlüsselung muss man sich noch selbst darum kümmern.

1. Damit die Partner verschlüsselt schreiben oder Signaturen prüfen können, muss man ihnen den eigenen Schlüssel zusenden oder zum Download anbieten.

[1] https://autocrypt.org/
[2] https://countermitm.readthedocs.io/en/latest/index.html

2. Damit man selbst verschlüsselt schreiben kann, muss man die Schlüssel der Kommunikationspartner in Thunderbird importieren.
3. Die frisch importierten Schlüssel der Partner müssen akzeptiert bzw. verifiziert werden, bevor man sie zum Verschlüsseln von E-Mails verwenden kann.

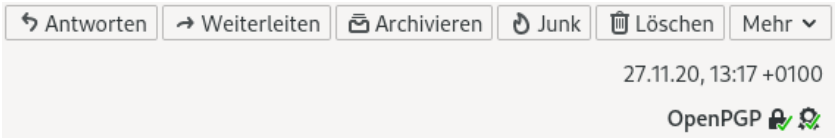
E-Mails schreiben: Wenn man die Hürden beim Austausch der Schlüssel überwunden hat, kann man beim Schreiben die Verschlüsselung mit einem Klick aktivieren:



(Wenn man auf verschlüsselte E-Mails antwortet, wird es automatisch aktiviert.)

Standardmäßig werden verschlüsselte E-Mails signiert und die Betreffzeile versteckt. Wenn man das OpenPGP-Menü aufklappt, kann man die Optionen anpassen.

E-Mails lesen: Verschlüsselte E-Mails werden von Thunderbird automatisch entschlüsselt und angezeigt, wenn man sie öffnet. Man sieht oben rechts im Kopf der E-Mail ein oder zwei kleine Symbole bei verschlüsselten und/oder signierten E-Mails:



Verschlüsselte E-Mails werden nicht in den globalen Index aufgenommen und können nicht bei einer Suche nach Begriffen aus dem Inhalt der Mail gefunden werden.

10.1.1 Eigenen OpenPGP-Schlüssel erstellen oder importieren

Um OpenPGP zu aktivieren, muss man in der Verwaltung des E-Mail-Accounts unter *Ende-zu-Ende-Verschlüsselung* ein Schlüsselpaar für OpenPGP erzeugen oder importieren.

Wenn man ein neues Schlüsselpaar erstellt, gibt es nicht viele Fragen (Abb. 10.1).

Wenn man bereits OpenPGP verwendet, kann man seinen bereits in GnuPG vorhandenen privaten Schlüssel in eine Datei exportieren und diese in Thunderbird importieren. Auf der Kommandozeile erledigt man den Export aus GnuPG in die Datei mit:

```
> gpg --export-secret-keys --armor user@server.tld > mein-key.asc
```

Die Datei mit dem Schlüssel kann man als eigenen Schlüssel importieren.

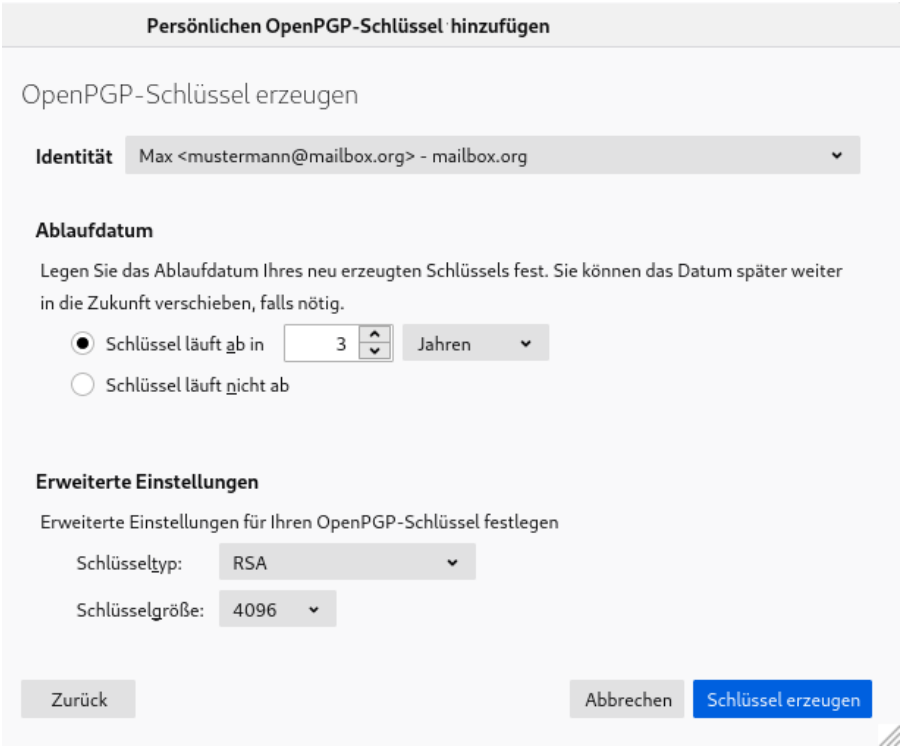


Abbildung 10.1: Neues OpenPGP-Schlüsselpaar in Thunderbird erstellen

10.1.2 Eigenen OpenPGP-Schlüssel mit GnuPG verwenden

Die Verwaltung der privaten Schlüssel mit der OpenPGP.js-Implementierung von Thunderbird ist zwar einfach, aber aus Sicht der kryptografischen Sicherheit nur suboptimal. GnuPG schützt den privaten Schlüssel besser und für hohe Sicherheitsanforderungen sind Smartcards empfehlenswert.

Wer eine OpenPGP-Smartcard verwendet oder den privaten Schlüssel nicht an Thunderbird übergeben, sondern für hohe Sicherheitsanforderungen weiterhin die bereits vorhandene GnuPG-Installation zur Verwaltung des privaten Schlüssel verwenden möchte, kann folgende Variable in den erweiterten Einstellungen von Thunderbird aktivieren:

```
mail.openpgp.allow_external_gnupg = true
```

Dann wird für die Einrichtung des eigenen Schlüssels eine dritte Option angeboten. Im folgenden Schritt kann man die ID des eigenen Schlüssels angeben, der im GnuPG-Keyring liegt (Abb. 10.2). Der Zugriffsschutz für den privaten Key wird dann von GnuPG geregelt. Die Krypto-Operationen mit dem privaten Key werden dann ebenfalls von GnuPG ausgeführt statt mit OpenPGP.js in Thunderbird, was die kryptografische Sicherheit verbessert.

Den Public-Key und die Schlüssel der Kommunikationspartner muss man immer in Thunderbird importieren. Sie können nicht von einem externen GnuPG verwaltet werden.

10.1.3 Den eigenen öffentlichen Schlüssel verteilen

Damit Kommunikationspartner mir verschlüsselt schreiben oder die Signatur meiner E-Mail verifizieren können, muss ich ihnen den eigenen öffentlichen Schlüssel zusenden oder zum Download anbieten. Dafür gibt es mehrere Möglichkeiten:

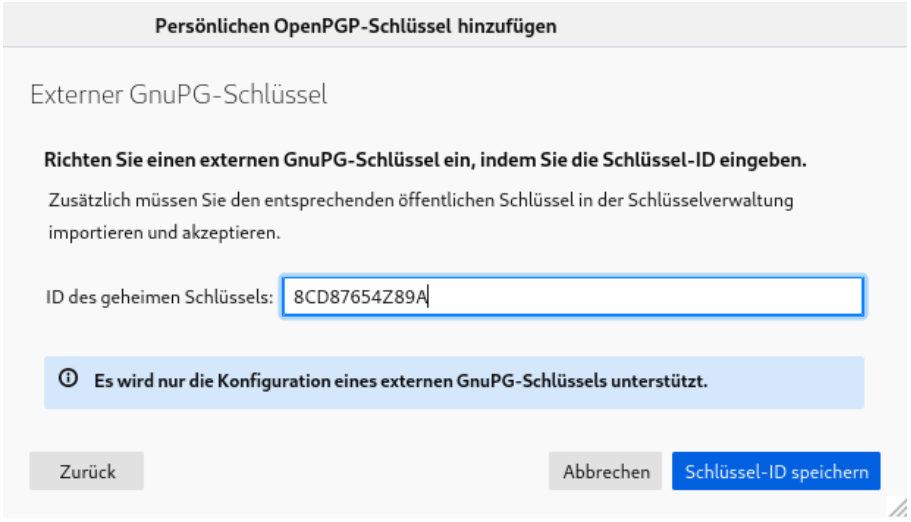


Abbildung 10.2: Privaten OpenPGP-Schlüssel mit GnuPG verwalten

1. Man kann den eigenen öffentlichen Schlüssel auf einem Webserver zum Download bereitstellen oder in einer Cloud hochladen und den Download-Link für alle freigeben. In der Signatur jeder E-Mail weist man auf den Download hin und gibt damit dezent zu verstehen, dass man nach Möglichkeit verschlüsselte E-Mails bevorzugt.

   Echte Profis stellen den Schlüssel auch für Web Key Discovery (WKD) bereit.

2. Man kann den öffentlichen Schlüssel in den OpenPGP Keyserver Pool hochladen.[3]

   Auf der Webseite kann man seinen eigenen Schlüssel hochladen. Es werden E-Mails mit der Aufforderung zur Bestätigung an alle Adressen gesendet, die im Schlüssel genannt sind. Die E-Mails enthalten einen Link, den man im Browser öffnen muss, um den Erhalt der E-Mail zu bestätigen. Danach wird der Schlüssel freigeschaltet.

   Die OpenPGP-Keyserver bieten einen Link zum Download, den man in der E-Mail-Signatur verwenden kann, um auf die Möglichkeit zum Download hinzuweisen.

3. Man kann die Möglichkeiten nutzen, die E-Mail-Provider zur Unterstützung der Schlüsselverteilung anbieten. Näheres findet man in den FAQ seines Providers.

4. Man kann es auch ganz klassisch machen und den Schlüssel als Attachment an eine signierte E-Mail anhängen. (Thunderbird fügt dabei auch einen Autocrypt-Header ein, um anderen E-Mail-Clients den Import zu erleichtern.)

10.1.4 Fremde Schlüssel importieren

Für den Import der Schlüssel der Kommunikationspartner gibt es mehrere Möglichkeiten:

1. Wenn man einen OpenPGP-Schlüssel als Anhang per E-Mail erhalten hat, kann man ihn mit zwei Mausklicks importieren.

[3] https://keys.openpgp.org/

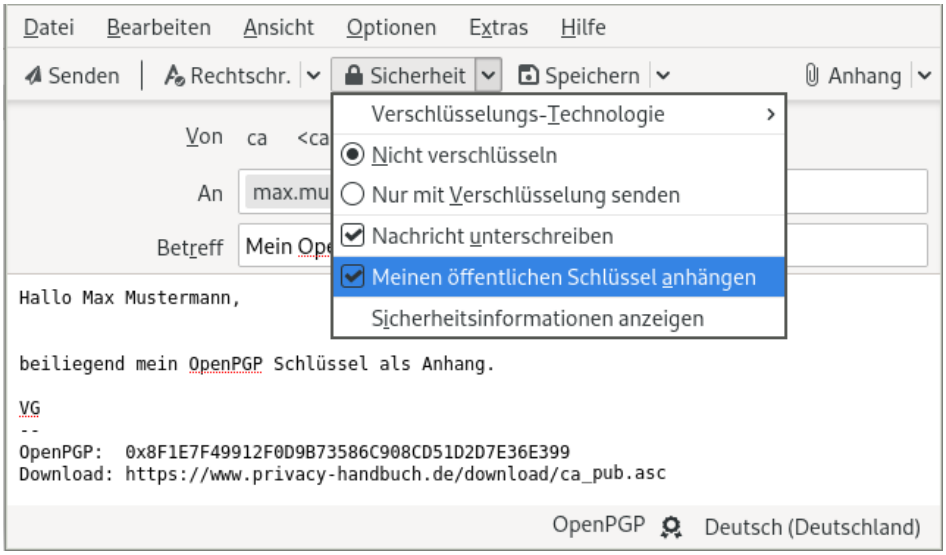
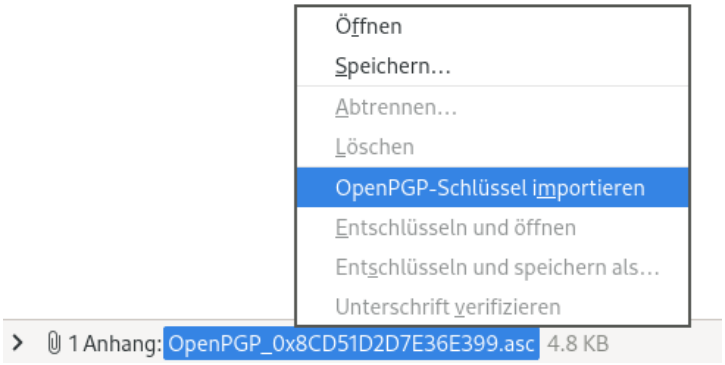
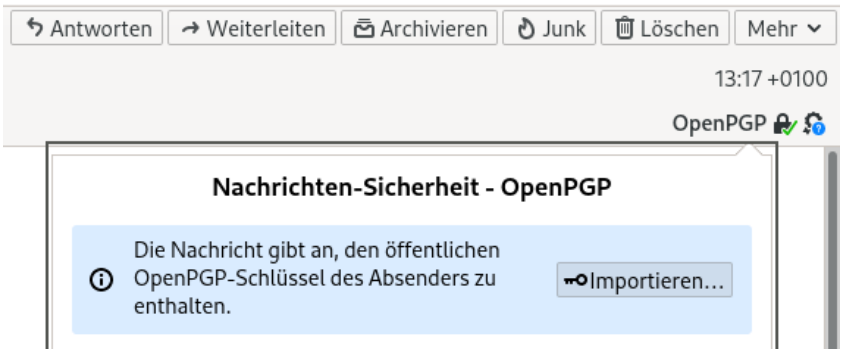


Abbildung 10.3: Öffentlichen OpenPGP-Schlüssel per E-Mail verteilen



2. Wenn eine E-Mail einen Autocrypt-Header mit dem OpenPGP-Schlüssel des Absenders enthält, kann man ihn ebenfalls mit zwei Mausklicks importieren.



3. In der OpenPGP-Schlüsselverwaltung, die man unter *Extras* → *OpenPGP-Schlüssel verwalten* findet, gibt es weitere Optionen zum Importieren von Schlüsseln:

   - Man kann einen oder mehrere Schlüssel aus einer Datei importieren.
   - Man kann einen Schlüssel aus der Zwischenablage importieren.

- Man kann den Schlüssel von einer Download-URL abrufen, die man auf einer Webseite oder in der Signatur einer E-Mail findet.
- Man kann den Schlüssel anhand der E-Mail-Adresse via Web Key Discovery (WKD) und auf OpenPGP-Keyservern suchen und importieren.

10.1.5 Fremde Schlüssel akzeptieren bzw. verifizieren

Es reicht nicht aus, die Schlüssel der Kommunikationspartner in Thunderbird zu importieren, um sie anschließend verwenden zu können. Man muss die importierten Schlüssel noch akzeptieren oder anhand des Fingerabdrucks den Schlüssels verifizieren, um ausdrücklich zu bestätigen, dass man diese Schlüssel in Zukunft verwenden will.

Um Schlüssel zu akzeptieren bzw. zu verifizieren, öffnet man die Schlüsselverwaltung, wählt den frisch importierten Schlüssel aus und öffnet den Dialog *Schlüsseleigenschaften*.

Auf dem Reiter *Ihre Akzeptanz* kann man angeben, dass man vermutlich den richtigen Schlüssel erhalten hat (akzeptieren) oder dass man den Fingerabdruck des Schlüssels über einen sicheren Kanal oder bei einem persönlichen Treffen mit dem Inhaber des Schlüssels verifiziert hat und sicher ist, den richtigen Schlüssel zu verwenden (Abb. 10.4).

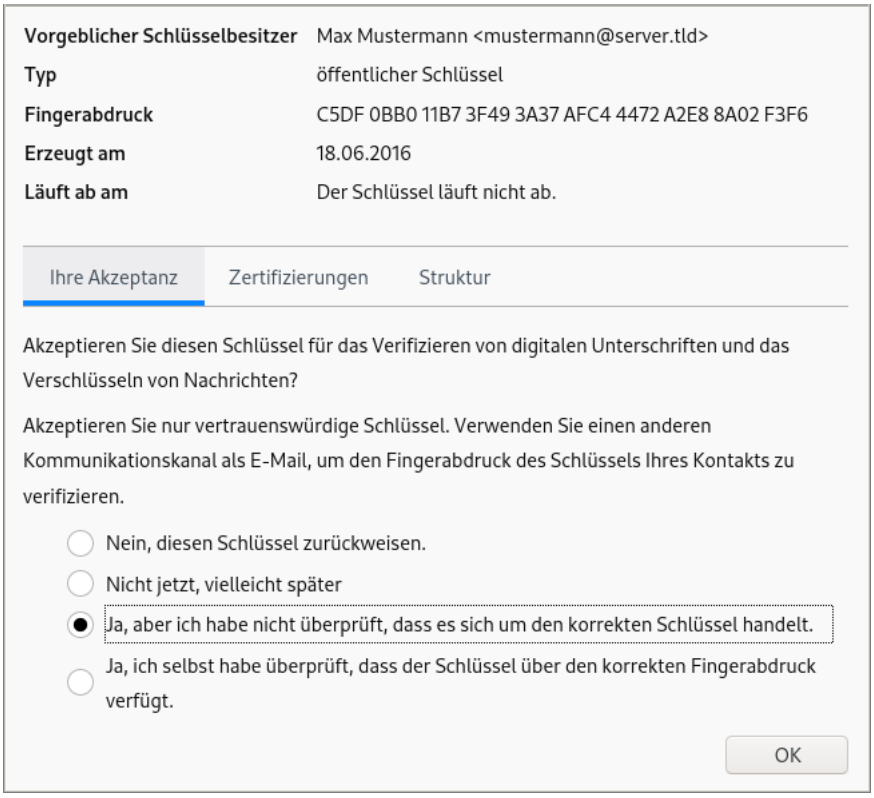


Abbildung 10.4: Importierten OpenPGP-Schlüssel akzeptieren oder verifizieren

10.2 Gedanken zum Browser-Add-on Mailvelope

Mailvelope ist ein Add-on für die Browser Mozilla Firefox und Google Chrome, das OpenPGP-Verschlüsselung im Webinterface ermöglicht. Es kann die interne OpenPGP.js-Implementierung

oder eine externe GnuPG-Installation nutzen. OpenPGP.js hat konzeptuell bedingt einige Schwächen und ist nicht für hohe Sicherheitsanforderungen geeignet. Es handelt sich um folgende konzeptuelle Schwächen:

- **Unsichere Speicherung der Schlüssel:** Die Speicherung der Schlüssel im lokalen Storage des Browsers ist konzeptuell unsicher. Es wurden bei verschiedenen Audits immer wieder Angriffsmöglichkeiten via XSS (2015) oder mittels Clickjacking (2019) aufgedeckt, die ein Auslesen der privaten Schlüssel ermöglichten.

- **JavaScript ist nicht für starke Krypto geeignet:** JavaScript wurde nicht als Programmiersprache für Krypto-Anwendungen entworfen. Best-Practices für die Implementierung von Krypto sind mit JavaScript nicht umsetzbar.

  JavaScript bietet keine Möglichkeiten, bei der Programmierung identische Ausführungszeiten für Code-Verzweigungen zu erzwingen. Durch Seitenkanalangriffe ist es damit möglich, die Reihenfolge der Nullen und Einsen im privaten Schlüssel durch Beobachtung bei der Codeausführung zu rekonstruieren. In modernen Krypto-Bibliotheken ist das ein Security-Bug (z. B. CVE-2016-7056 ECDSA P-256 timing attack key recovery, OpenSSL).

  Seitenkanalangriffe auf Browser sind einfach, da der Rechner nicht kompromittiert werden muss. Das Script für den Angriff kann von einer beliebigen Webseite geladen werden, wie Forscher in dem Paper *The Spy in the Sandbox – Practical Cache Attacks in JavaScript*[4] gezeigt haben.

  Mit JavaScript is es nicht möglich, einen geheimen Schlüssel nach der Benutzung aus dem Hauptspeicher zu löschen (Overwriting memory – why?). Das normale Verhalten von Mailvelope wurde bei Tor Onion Router als Security-Bug eingestuft.[5]

  Was in anderen Krypto-Implementierungen als schwerer Bug gilt, wird bei Mailvelope einfach als JavaScript-Limitierung hingenommen.

  In den FAQ von Mailvelope wird darauf hingewiesen, dass die geheimen Schlüssel durch das Senden eines Speicherabbildes in Absturzberichten an die Entwickler bei Mozilla oder Google kompromittiert werden könnten. Deshalb sollte man diese Funktion im Browser unbedingt deaktivieren.

10.2.1 Mailvelope mit GnuPG nutzen

Mailvelope bietet die Möglichkeit, statt der traditionellen Variante mit der OpenPGP.js-Implementierung eine lokale Installation von GnuPG zu verwenden. Damit vermeidet man die oben genannten Schwächen von OpenPGP.js. Auch das Mailvelope-Team empfiehlt in den FAQ[6] die Verwendung von GnuPG zur Verbesserung der Sicherheit. Die Verwendung von OpenPGP-Smartcards ist nur in Kombination mit GnuPG möglich und nicht mit OpenPGP.js.

Die Verwendung von GnuPG mit Mailvelope wird nicht funktionieren, wenn man unter Linux den Firefox-Prozess unter Kontrolle von apparmor oder SELinux laufen lässt.

10.2.2 Mailvelope und Autocrypt

Standardmäßig verwendet Mailvelope den Autocrypt-Schlüsseltausch. Da Autocrypt die Sicherheit von OpenPGP massiv schwächt, sodass die Verschlüsselung nur noch *some protection most of the*

[4] https://www.cs.columbia.edu/~simha/spyjs.ccs15.pdf
[5] https://heise.de/-1746523
[6] https://www.mailvelope.com/de/faq#gnupg

time und keinen Schutz mehr gegen einen bösartigen E-Mail-Provider bietet, ist die Deaktivierung von Autocrypt im Dashboard dringend zu empfehlen.

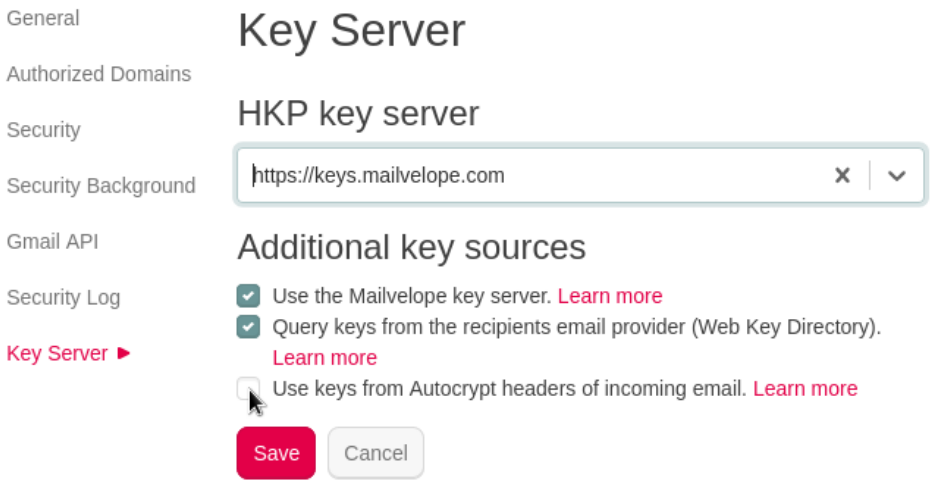


Abbildung 10.5: Autocrypt in Mailvelope deaktivieren

10.3 Einige Ergänzungen zum Thema GnuPG

GnuPG ist eine frei nutzbare Implementierung des OpenPGP-Standards zur Verschlüsselung und Signierung von Daten. Es wird vom GNU-Projekt ständig weiterentwickelt. Das Thunderbird Add-on Enigmail verwendet standardmäßig GnuPG 2.x.

Windows: Das Projekt gpg4win[7] stellt ein Paket für Windows mit GnuPG, dem GNU-Privacy-Assistenten für die Schlüsselverwaltung und einer Erweiterung für MS Outlook bereit.

Linux, BSD: Die Distributionen installieren GnuPG 2.x nicht immer vollständig. Manchmal muss man etwas nachinstallieren. Für Debian/Ubuntu funktioniert:

```
> sudo apt install gnupg2 gpg-agent pinentry-gtk2 scdaemon
```

Bei einigen Linux-Distributionen ist *gpg-agent* im Paket *gpgsm* enthalten. Der *gpg-agent* wird für die Eingabe der Passphrase benötigt und sollte beim Login automatisch gestartet werden. Dafür fügt man in der Konfiguration *$HOME/.gnupg/gpg.conf* folgende Zeile am Ende ein:

```
use-agent
```

In der Datei *$HOME/.gnupg/gpg-agent.conf* kann man konfigurieren, wie lange der Agent die Passphrase für einen Key speichert. Standardmäßig wird eine Passphrase 10 Minuten (600 s) gespeichert. GPA ändert den Wert aus Sicherheitsgründen auf 300 s.

```
default-cache-ttl 300
max-cache-ttl 360
```

Verbesserte Konfiguration von GnuPG

In der Konfigurationsdatei *gpg.conf* kann man nach der Installation ein paar kleine Verbesserungen vornehmen. Die Konfigurationsdatei findet man unter Windows in *%APPDATA%/GnuPG* und unter Linux/BSD im Verzeichnis *$HOME/.gnupg*.

Die Datei kann man mit einem Texteditor bearbeiten und folgende Optionen ergänzen bzw. durch Entfernen des Kommentarzeichens # aktivieren:

```
# keine Informationen über Version und Betriebssystem einfügen
no-emit-version
no-comments

display-charset utf-8

# 16-stellige Key-IDs verwenden statt 8-stelliger (schwerer zu faken)
keyid-format 0xlong

# Keyserver-URLs in Keys ignorieren (Tracking möglich)
```

[7] http://www.gpg4win.org/

```
keyserver-options no-honor-keyserver-url, no-auto-key-retrieve,
↪  no-include-revoked

# Empfohlene Preferenzen für Krypto-Algorithmen
personal-digest-preferences SHA512 SHA384 SHA256
personal-cipher-preferences AES256 AES192 AES TWOFISH
personal-compress-preferences Uncompressed ZIP ZLIB BZIP2
default-preference-list SHA512 SHA384 SHA256 AES256 AES192 AES Uncompressed

# Signaturalgorithmus für Beglaubigungen
cert-digest-algo SHA512

# Einstellungen für symmetrische Verschlüsselung
s2k-cipher-algo AES256
s2k-digest-algo SHA384

# Cipher mit 64 Bit Blockgröße deaktivieren, weil sie
# schwach sind und ohne MDC verwendet werden (siehe: #Efail)
disable-cipher-algo 3DES
disable-cipher-algo IDEA

# SHA1 als schwachen Algorithmus markieren (wie MD5)
weak-digest SHA1

# sonstiges
fixed-list-mode
verify-options show-uid-validity
list-options show-uid-validity
```

Bei der Erstellung eines OpenPGP-Schlüssels werden die Einstellungen in der aktuell konfigurierten *Default Preference List* für Krypto-Algorithmen in den Schlüssel übernommen. GnuPG verwendet die für den Schlüssel gültigen Präferenzen immer dann, wenn keine Präferenzen in der Konfiguration angegeben wurden, wenn der Kommunikationspartner also keine persönlichen Präferenzen in seiner Config definiert hat.

Wenn man seinen Schlüssel vor einigen Jahren erstellt hat, dann wird in diesem Fall bspw. das angeknackste SHA-1 als Digest-Algorithmus bevorzugt verwendet. Man muss die persönlichen Präferenzen auch in die eigenen Schlüssel übernehmen und die Schlüssel danach neu verteilen. Das geht nur auf der Kommandozeile. Man muss das GnuPG-Kommandozeilen-Tool gpg2 mit der Option *–edit-key* und der Key-ID aufrufen. Danach kann man sich mit dem Kommando *showpref* die Präferenzen für diesen Schlüssel anzeigen lassen und mit dem Kommando *setpref* die Defaults übernehmen:

```
> gpg2 --edit-key mustermann@server.tld
gpg (GnuPG) 2.1.x; Copyright (C) 2016 Free Software Foundation, Inc.
...
gpg> showpref
[ unbekannt ] (1). Max Mustermann <mustermann@server.tld>
   Verschlü.: AES256, AES192, AES, CAST5, 3DES
   Digest: SHA1, SHA256, RIPEMD160
   Komprimierung: nicht komprimiert, ZLIB, BZIP2, ZIP
```

```
    Eigenschaften: MDC, Keyserver no-modify

gpg> setpref
Setze die Liste der Voreinstellungen auf:
   Verschlü.: AES256, AES192, AES, 3DES
   Digest: SHA512 SHA384 SHA256, SHA1
   Komprimierung: nicht komprimiert
   Eigenschaften: MDC, Keyserver no-modify
Die Voreinstellungen wirklich ändern? (j/N) j
...
Sie benötigen die Passphrase, um den geheimen Schlüssel zu entsperren.
Benutzer: "Max Mustermann <mustermann@server.tld>"
...
gpg> quit
Änderungen speichern? (j/N) j
```

10.3.1 Gedanken zur Auswahl und Stärke von Schlüsseln

Aktuelle GnuPGP-Versionen unterstützen neben RSA- und DSA-Schlüsseln mit bis zu 4096 Bit Länge auch Schlüssel auf der Basis elliptischer Kurven. Alle Optionen hat man zur Auswahl, wenn man ein Schlüsselpaar auf der Kommandozeile im Experten-Modus erstellt:

```
> gpg2 --expert --full-gen-key
```

Welche Schlüssel sollte man nutzen? Ein paar Gedanken zur Auswahl:

1. RSA Schlüssel werden von allen PGP Implementierungen problemlos akzeptiert. Bei ausreichender Schlüssellänge mit mind. 3072 Bit gelten diese Schlüssel als sicher.
2. Schlüssel auf der Basis elliptischer Kurven werden nur in aktuellen PGP-Implementierungen unterstützt, die sich aber noch nicht überall durchgesetzt haben. Für den Einsatz elliptischer Kurven in PGP gibt es folgende Standards:
   - Der RFC 6637 der IETF empfiehlt nur die NIST-Kurven P-256, P-384 und P-512 für OpenPGP.
   - Die Java-Bibliothek BountyCastle sowie PGP-Implementierungen für C# und VB.net können außerdem mit den Brainpool-Kurven nach RFC 5639 umgehen.
   - Das GnuPGP-Team hat mit RFC 4880bis Draft eine Erweiterung vorgeschlagen, auch die Unterstützung für die Kurven Ed25519 und Curve25519 zu integrieren. Dieser Draft wurde in GnuPG 2.1+ umgesetzt und wird auch von Thunderbird unterstützt.

10.3.2 GnuPG-Smartcards nutzen

Die Sicherheit asymmetrischer Verschlüsselung hängt von der sicheren Aufbewahrung des privaten Schlüssels ab. Es gibt mehrere Möglichkeiten, wie private Keys kompromittiert werden könnten:

- Wenn man GnuPG auf mehreren Computern nutzt, auf denen andere Nutzer Administrator- bzw. Root-Privilegien haben, könnten die privaten Keys von Administratoren eingesammelt werden.

- Böswillige Buben können mit einem Trojaner versuchen, den privaten Key zu kopieren und die Passphrase mit Keyloggern oder mit Tools wie *Elcomsoft Distributed Password Recovery* ermitteln.
- Die unbedachte Entsorgung einer Festplatte oder eines Computers ist ein weiteres Risiko, wenn die privaten Daten nicht sicher gelöscht wurden.

Smartcards ermöglichen eine sichere Nutzung von GnuPG unter diesen Bedingungen. Der Private-Key ist nicht auf dem Rechner, sondern ausschließlich auf der Smartcard gespeichert. Er verlässt diese sichere Umgebung nicht und alle Krypto-Operationen, die den privaten Schlüssel nutzen, werden auf der Smartcard ausgeführt. Die Nutzung von Smartcards hätte wahrscheinlich die Kompromittierung der Schlüssel von Cryptome.org[8] verhindern können.

Ein paar Angebote für OpenPGP-Smartcards:

- Die **GnuPG-Smartcard** gibt es von kernelconcepts.de[9]. Die Bestellung erfolgt per E-Mail und man braucht zusätzlich einen Smartcard-Reader oder den ebenfalls dort erhältlichen Gemalto USB Adapter.
- Der **NitroKey**[10] ist ein Open-Source-Hardware-Projekt und der Nachfolger des Cryptostick. Der NitroKey Pro enthält zusätzlich einen OTP-Generator und einen Passwortspeicher. (Für diese Zusatzfunktion ist die NitroKey-App[11] zu installieren.)
- Der **Yubikey** ist ein One-Time-Passwortgenerator (OTP), den man für Logins bei Webdiensten nutzen kann. Er enthält zusätzlich eine OpenPGP-Smartcard.[12]

Erster Test

Die GnuPG Software Collection kann Smartcards *out-of-the-box* nutzen. Zuerst sollte man prüfen, ob alles funktioniert und die Smartcard erkannt wird. Smartcard anschließen und auf der Konsole bzw. in der DOS-Box folgendes Kommando eingeben:

```
> gpg2 --card-status
Application ID ...: D27600xxxxxxxxxxxxxx
Version ..........: 2.0
Manufacturer .....: unknown
...
```

Wenn keine Smartcard gefunden wird, kann man zuerst prüfen, ob die GnuPG Software Collection vollständig installiert wurde (*gpg2 + gpg-agent + scdaemon*) und ob der gpg-agent läuft. Bekannte Probleme gibt es auch mit dem GNOME Keyring Manager (siehe unten).

[8] http://heise.de/-2817797
[9] https://www.floss-shop.de/de/search?sSearch=OpenPGP
[10] https://www.nitrokey.com/de
[11] https://www.nitrokey.com/de/download
[12] https://www.yubico.com/products/yubikey-hardware/

Verwaltung der Smartcard mit GNU Privacy Assistant (GPA)

Der GNU Privacy Assistant (GPA) ist Bestandteil des gpg4win-Paketes und kann in allen Linux-Distributionen aus den Repositorys installiert werden. Mit diesem GUI können auch OpenPGP-Smartcards verwaltet werden. Dafür wählt man das Fenster *Kartenverwaltung*. Dort kann man neue Schlüssel auf der Smartcard generieren lassen, die Daten anpassen und eine neue PIN/PUK setzen.

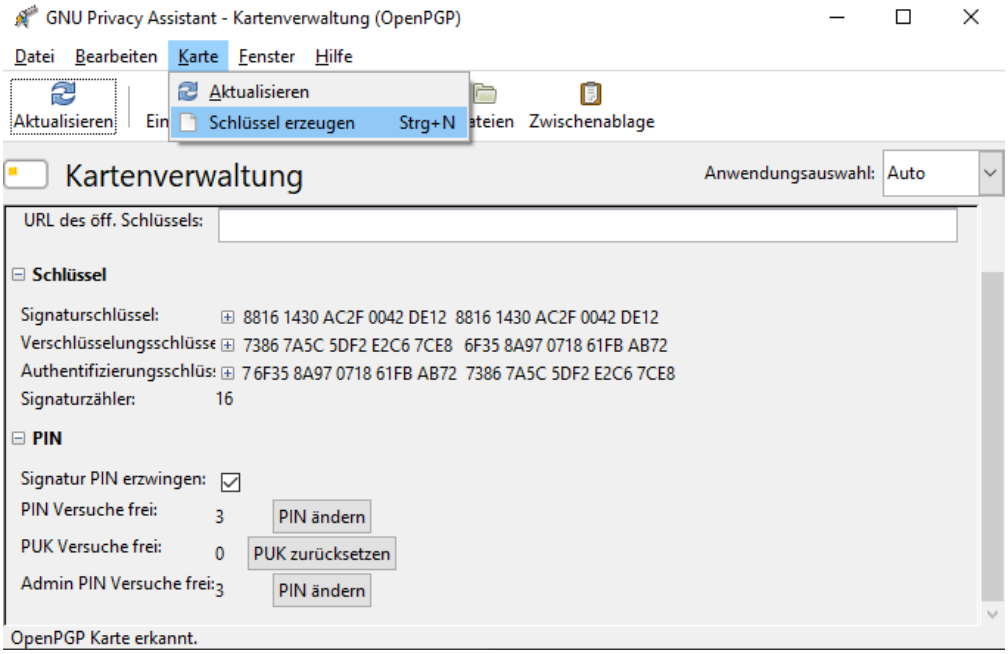


Abbildung 10.6: Smartcards mit dem GNU Privacy Assistant (GPA) verwalten

Die PIN benötigt man, wenn man die Smartcard zum Entschlüsseln oder Signieren von Daten verwenden möchte. Die PUK (auch Admin-PIN genannt) wird benötigt, wenn man Daten auf der Smartcard ändern oder neue Schlüssel erzeugen möchte.

Verwaltung der Smartcard auf der Kommandozeile

Die Nutzung von gpg2 auf der Kommandozeile stellt einige Möglichkeiten mehr als das GUI von GPA zur Verfügung. Einen Überblick über alle Smartcard-Funktionen gibt die Hilfe mit dem Kommando *help*. Als Erstes muss man den Admin-Mode aktivieren, dann hat man vollen Zugriff auf alle Funktionen:

```
> gpg2 --card-edit
...
gpg/card> admin
Admin-Befehle sind erlaubt

gpg/card> help
...
gpg/card> quit
```

Neue Schlüssel generiert man auf der Smartcard mit *generate*, die PIN und Admin-PIN kann man mit *passwd* ändern. Mit *unblock* kann man den Zähler für Fehlversuche zurücksetzen und *factory-reset* löscht alle Schlüssel auf der Smartcard.

Neuer oder fremder Rechner – was nun?

Ein nettes Feature von OpenPGP-Smartcards ist es, an einem neuen oder fremden Rechner den Public-Key von einer Download-Adresse holen zu können. Der Private-Key ist auf der Card in einer sicheren Umgebung, somit kann man auch unterwegs auf einem halbwegs vertrauenswürdigen fremden Rechner eines Bekannten mit vollständiger GnuPG-Installation die PGP-Verschlüsselung nutzen, ohne den privaten Schlüssel zu kompromittieren.

Der Download des Public-Key steht nur auf der Kommandozeile zur Verfügung. Nach dem Abrufen des Public-Key von der Download-URL muss man noch einmal den Card-Status aufrufen, damit der private Schlüssel an den Public-Key gebunden wird:

```
> gpg2 --card-edit
...
gpg/card> fetch        (Abrufen des Public-Key von der Download-URL)
gpg/card> quit
...
> gpg2 --card-status   (Re-bind von Private- und Public-Key)
...
```

Vorhandenen Schlüssel mit Smartcard weiterverwenden

Wenn man bereits PGP für die Verschlüsselung nutzt und einen vorhandenen Schlüssel weiterverwenden möchte, dann kann man die Private-Keys dieses Schlüssels auch auf eine OpenPGP-Smartcard übertragen. Damit erspart man sich die Verteilung eines neuen Schlüssels und kann die Beglaubigungen des Web-of-Trust behalten.

GnuPG erstellt standardmäßig Schlüsselpaare mit einem Hauptschlüssel zum Signieren und Beglaubigen sowie einen Unterschlüssel zum Verschlüsseln. Die OpenPGP-Smartcard kennt drei Schlüssel: einen zum Signieren, einen zum Verschlüsseln und einen zum Authentifizieren. Man muss die von GnuPG erstellten Haupt- und Unterschlüssel einzeln auf die korrespondierenden Plätze auf der Smartcard schieben.

Als erstes ruft man *gnupg2* mit der Funktion *edit-key* für den Schlüssel auf, den man auf die Smartcard verschieben will. Mit *toggle* schaltet man auf die Verwaltung der privaten Keys. Dann schiebt man mit *keytocard* zuerst den Hauptschlüssel als Signatur-Key auf die Smartcard, wählt den Subkey mit *key 1* aus und schiebt den Encryption-Subkey auf den passenden Platz auf der Smartcard.

```
> gpg2 --edit-key mustermann@server.tld
Geheimer Schlüssel ist vorhanden.
...
gpg> toggle

sec  rsa2048/8A02F3F6
     erzeugt: 2016-06-18  verfällt: niemals   Aufruf: SC
ssb  rsa2048/08D68793
```

```
      erzeugt: 2016-06-18  verfällt: niemals   Aufruf: E

gpg> keytocard
Den Hauptschlüssel wirklich verschieben? (j/N) j
Wählen Sie den Speicherort für den Schlüssel:
    (1) Signatur-Schlüssel
    (3) Authentisierungs-Schlüssel
Ihre Auswahl? 1

gpg> key 1

sec  rsa2048/8A02F3F6
     erzeugt: 2016-06-18  verfällt: niemals   Aufruf: SC
ssb*  rsa2048/08D68793
     erzeugt: 2016-06-18  verfällt: niemals   Aufruf: E

gpg> keytocard
Wählen Sie den Speicherort für den Schlüssel:
   (2) Verschlüsselungs-Schlüssel
Ihre Auswahl? 2

gpg> quit
Änderungen speichern? (j/N) j
```

Danach kann man den Status der Smartcard prüfen und sich davon überzeugen, dass die beiden Schlüssel jetzt als *Signature key* und *Encryption key* auf der Smartcard liegen:

```
> gpg2 --card-status

Reader ...........: 20A0:4108:000036C40000000000000000:0
Application ID ...: D2760001240102010005000036C40000
Version ..........: 2.1
...
PIN retry counter : 3 0 3
Signature counter : 0
Signature key ....: C5DF 0BB0 11B7 3F49 3A37  AFC4 4472 A2E8 8A02 F3F6
      created ....: 2016-06-18 15:32:07
Encryption key....: 94E1 D64A 51C0 8C78 CE60  6472 0059 00DC 08D6 8793
      created ....: 2016-06-18 15:32:07
Authentication key: [none]
General key info..: pub  rsa2048/8A02F3F6 <mustermann@server.tld>
sec   rsa2048/8A02F3F6  erzeugt: 2016-06-18  verfällt: niemals
ssb   rsa2048/08D68793  erzeugt: 2016-06-18  verfällt: niemals
```

10.3.3 Autocrypt

Das Verfahren Autocrypt will den Nutzern den manuellen PGP-Schlüsselaustausch abnehmen und ihn dadurch nutzerfreundlich machen. Der PGP-Schlüssel soll im Header jeder E-Mail mitgesendet werden, damit der Empfänger sofort automatisch verschlüsselt antworten kann, ohne sich um den Schlüsseltausch (und die Validierung?) kümmern zu müssen.

Für die theoretische Begründung der Sicherheit greift Autocrypt auf das Konzept Opportunistic Security (RFC 7435) zurück. Das bedeutet, dass die Verschlüsselung nur noch gegen passive Angreifer schützt soll, aber nicht mehr gegen aktive Angreifer, die sich als Man-in-the-Middle in die Kommunikation einschleichen können.

Wenn jemand **Opportunistic Security** verspricht, dann funktioniert die Verschlüsselung ganz gut, solange sich niemand ernsthaft für die Kommunikation interessiert. Gegen einen ernsthaften, aktiven Angriff bietet dieses Konzept keinen Schutz und man muss im Zweifel davon ausgehen, dass die Verschlüsselung genau dann kompromittiert wird, wenn man sie gebraucht hätte. Opportunistic Security bietet ausdrücklich nur **Some Protection Most of the Time**.

Wie könnte ein E-Mail-Provider die Verschlüsselung kompromittieren?

1. Die E-Mail-Header werden von den Mailprovidern ständig routiniert manipuliert. Es werden neue Header eingefügt, einige Header werden gelöscht usw. In gleicher Weise könnten die Autocrypt-Header von den versendenden oder empfangenden E-Mail-Providern manipuliert und ein falscher Schlüssel könnte eingefügt werden.

2. Es ist keine kryptografische Validierung der OpenPGP-Schlüssel vorgesehen, die im Autocrypt-Header gesendet werden. Der E-Mail-Client soll den jeweils neuesten Schlüssel ohne Überprüfung akzeptieren. Wenn ein E-Mail-Provider den PGP-Schlüssel im Autocrypt-Header gegen einen falschen Key austauscht, dann wird der Empfänger der Mail diesen falschen Schlüssel mit hoher Wahrscheinlichkeit verwenden.

3. Wenn eine Antwort geschrieben wird, kann der E-Mail-Provider natürlich erkennen, dass eine Mail mit dem Fake-Schlüssel verschlüsselt wurde. Er entschlüsselt die Mail, nimmt den Inhalt zur Kenntnis und verschlüsselt sie dann mit dem richtigen Schlüssel, bevor er sie zustellt. Das Opfer bemerkt nicht, dass der PGP-Schlüssel ausgetauscht wurde.

Das ist kein Bug sondern ein Feature des zugrundeliegenden Konzeptes.

Dass ein solches Szenario nicht nur theoretisch sondern auch in der Praxis relevant sein kann, hat der E-Mail-Provider Hushmail demonstriert. 2007 wurde Hushmail von der US-amerikanischen DEA gezwungen, die PGP-Verschlüsselung für einige Kunden mit gefälschten Schlüsseln zu kompromittieren. Und die Spezialisten der Behörde ZITiS klatschen bestimmt vor Freude in die Hände, wenn Autocrypt großflächig eingesetzt wird.

Ende-zu-Ende-Verschlüsselung soll den Inhalt von E-Mails gegen Beobachtung durch die E-Mail-Provider schützen. Der **E-Mail-Provider** ist der potentielle **Angreifer**, gegen den uns Ende-zu-Ende-Verschlüsselung schützen soll! Eine E2E-Verschlüsselung, die nur unter der Voraussetzung funktioniert, dass der E-Mail-Provider vertrauenswürdig ist, wird zu Bullshit. Wenn auch noch erwartet wird, dass der Provider den Schlüsseltausch durch DKIM-Signaturen der Header absichern muss, dann steht die Welt auf dem Kopf.

Der Autocrypt-Schlüsseltausch erfordert, dass man dem E-Mail-Provider vertraut, und führt damit Ende-zu-Ende-Verschlüsslung mit OpenPGP ad absurdum. Es kompromittiert die Sicherheit zugunsten (zweifelhafter) Vereinfachungen der Usability.

10.3.4 Verschlüsselung in Webformularen

Auch bei der Nutzung eines Webmail-Accounts oder von Webforms für die Versendung anonymer E-Mails muss man auf Verschlüsselung nicht verzichten.

Einige grafische Tools für die Schlüsselverwaltung wie GPA[13] (*GNU Privacy Assistent*) enthalten einen Editor. Man kann den Text in diesem Editor schreiben, mit einem Klick auf den entsprechenden Button signieren oder verschlüsseln und das Ergebnis über die Zwischenablage in die Textbox der Website einfügen. Das Entschlüsseln funktioniert in umgekehrter Reihenfolge.

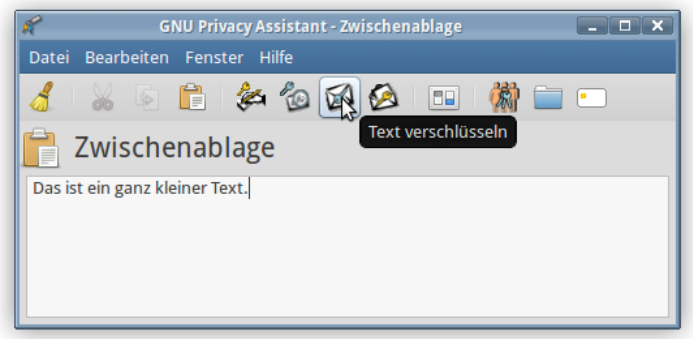


Abbildung 10.7: Text mit GPA verschlüsseln

Andere grafische Tools wie *Kleopatra* vom KDE-Projekt bieten die Ver- und Entschlüsselung des Textes in der Zwischenablage an. Um eine verschlüsselte Nachricht zu versenden, schreibt man den Text mit einem beliebigen Editor (Notepad, gedit, mousepad, kwrite usw.), kopiert danach den gesamten Text in die Zwischenablage (mit den Tasten STRG-A und STRG-C) und wählt dann die Option zum Verschlüsseln der Zwischenablage im Menü (Abb. 10.8). Nach der Auswahl der Empfänger wird der Text aus der Zwischenablage verschlüsselt und das verschlüsselte Ergebnis wieder in der Zwischenablage gespeichert. Diesen unlesbaren Zeichensalat kann man im Textfeld im Webformular einfügen (Taste: STRG-V). Entschlüsseln funktioniert wieder in umgekehrter Reihenfolge.

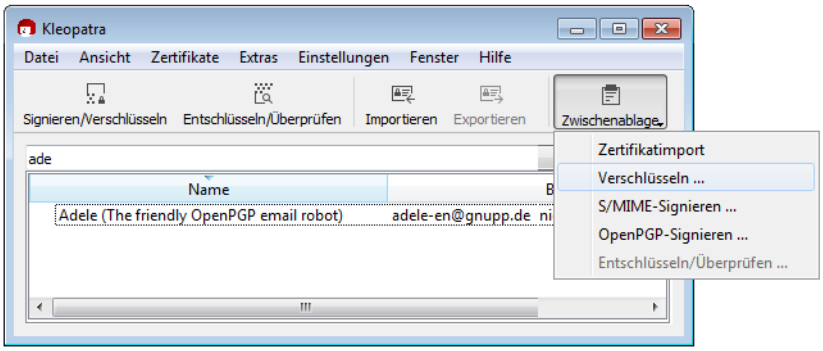


Abbildung 10.8: Kleopatra GnuPG GUI: Assistent zur Verschlüsselung von Dateien

10.3.5 OpenPGP-Verschlüsselung für Kontaktformulare

Dass Metadaten (z. B. Absender und Empfänger einer E-Mail) für die Überwachung eine große Rolle spielen, ist seit den Veröffentlichungen von Snowden/Greenwald allgemein bekannt. Leser des Privacy-Handbuches haben es evtl. vorher gewusst (siehe: Kommunikationsanalyse).

Kontaktformulare bieten eine Möglichkeit, diese Metadaten zu verschleiern. Wer ein Blog oder eine Webseite betreibt, kann recht einfach ein Kontaktformular zur Verfügung stellen. Es gibt

[13] http://www.gnupg.org/related_software/gpa/index.de.html

Wordpress-Plug-ins für Kontaktformulare, einfache PHP-Scripte oder fertige Perl-CGI Scripte. Man kann eine individuell passende Lösung wählen.

Dabei sollte man auf Folgendes achten:

1. Das Kontaktformular sollte den Absender nicht zur Eingabe seiner E-Mail-Adresse zwingen. Als Work-around kann man im HTML-Code des Formulars das Feld für die Absender-E-Mail-Adresse als *hidden* deklarieren und einen Standardwert setzen.
2. Das Script sollte die IP-Adresse des Absenders nicht in den Header der E-Mail einfügen. Einige Scripte für Kontaktformulare wollen damit den Spam-Schutz verbessern. Einfach ausprobieren.
3. Das Kontaktformular sollte immer via HTTPS (SSL-verschlüsselt) aufgerufen werden. Wenn die Webseite auch via plain HTTP erreichbar ist, sollten alle Links auf der Webseite zum Kontaktformular mit der vollständigen URL angegeben werden:

   ```
   <a href="https://www.server.tld/kontakt.html">Kontakt</a>
   ```

   Jeder gute Webhoster bietet inzwischen für einen kleinen Aufpreis SSL-Verschlüsselung für alle Kunden, Wordpress.com hat es standardmäßig aktiviert.

Im Folgenden möchte ich einige Möglichkeiten vorstellen, wie man ein Kontaktformular mit OpenPGP-Verschlüsselung aufmotzen könnte.

Hinweis: Bei allen Varianten handelt es sich um *server based crypto*, die nicht die gleiche Sicherheit wie richtige Ende-zu-Ende-Verschlüsselung gewährleisten kann. Diese Verschlüsselung schützt gegen passive Lauscher am Draht, kann aber durch potente aktive Angreifer kompromittiert werden.

Ganz einfach ohne Programmierung

Man kann einen guten E-Mail-Provider nutzen, der TLS-Verschlüsselung für eingehende E-Mails erzwingen kann und ein verschlüsseltes Postfach bietet, z. B. mailbox.org.

- Nachdem man einen E-Mail-Account bei mailbox.org erstellt und bezahlt hat, ist der Alias für TLS-verschlüsselten Versand/Empfang sowie das OpenPGP-verschlüsselte Postfach zu aktivieren und der eigene Public-Key hochzuladen.
- Im Script des Kontaktformulars konfiguriert man als Empfänger die E-Mail-Adresse: *<name>@secure.mailbox.org* bzw. *<name>@tls.mailbox.org*.

Vom Browser des Absenders wird die Nachricht SSL-verschlüsselt zum Webserver übertragen. Von dort wird sie über eine TLS-verschlüsselte Verbindung an Mailbox.org gesendet und auf dem Mailserver mit dem OpenPGP-Key verschlüsselt.

Diese Variante schützt den Inhalt der Nachrichten gegen den allgemeinen Überwachungswahn und bei Beschlagnahme von Daten. Sie schützt nicht gegen eine TKÜ nach §100 a/b StPO beim Hoster des Kontaktformulars oder beim E-Mail-Provider, da der Inhalt als Plain-Text an diesen Stellen mitgelesen werden kann.

Mit JavaScript im Browser des Absenders

Diese Variante erfordert HTML-Kenntnisse, um einige Anpassungen im HTML-Code des Kontaktformulars vorzunehmen und die Bibliothek *OpenPGPjs* einzubinden.

Hinweis: Verschlüsselung mit JavaScript im Browser bietet keine hohe, sondern lediglich hinreichende Sicherheit. Die Gründe wurden bereits mehrfach erwähnt. Für den Erstkontakt ist es aber besser als eine unverschlüsselte E-Mail.

1. Die Javascript-Bibliothek *openpgp.min.js* aus dem Projekt OpenPGPjs[14] ist bei Github auszuchecken und aus dem Verzeichnis *dist* auf den eigenen Webserver zu kopieren.

2. Das JavaScript-Schnipselchen *encrypt_message.js* von der Webseite des Privacy-Handbuchs[15] herunterladen und auf den Webserver kopieren. Dieses JavaScript-Schnipselchen verschlüsselt das Textarea-Feld mit der ID *message* mit dem OpenPGP-Schlüssel, der in dem DIV-Container *pubkey* steht. Wenn das Textarea-Feld oder der DIV-Container im Formular eine andere ID haben, sind die Zeilen 5 und 6 anzupassen:

```
function encrypt_message() {
  if (!(window.crypto && window.crypto.getRandomValues)) {
    window.alert("Fehler: der Browser ist veraltet und wird nicht
    ↪ supported!");
  } else {

    var message = document.getElementById("message");
    var pgpkey = document.getElementById("pubkey");

    if(message.value == "") {
        window.alert("Kein Text gefunden, das Textfeld ist leer!");
    } else {
        # Verschlüsseln des Textes im Textarea
        var options = { data: message.value,
             publicKeys: openpgp.key.readArmored(pgpkey.innerHTML).keys
           };
        openpgp.encrypt(options).then(function(ciphertext) {
             message.value = ciphertext.data; });
        # Button für Verschlüsseln deaktivieren
        document.getElementById("encrypt").disabled = true;
        document.getElementById("send").disabled = false;
    }
  }
}
```

3. Im HTML-Header der Webseite des Formulars sind die Scripte zu laden:

```
...
<script src="openpgp.min.js" async></script>
<script src="encrypt_message.js" async></script>
...
```

[14] https://github.com/openpgpjs/openpgpjs
[15] https://www.privacy-handbuch.de/handbuch_32v.htm

4. Der HTML-Code des Formulars enthält das Textfeld mit der ID *message* und zwei Buttons (*Verschlüsseln* und *Senden*). Der Button zum Absenden des Formulars ist beim Laden der Seite deaktiviert. Der Absender muss zuerst den Text verschlüsseln. Dabei wird der erste Button inaktiv und der Button zum Versenden wird aktiviert.

```
<FORM name="contact" method="post" action="https://server.tld/....">

<textarea id="message" ...></textarea>

<input type="button" onclick="encrypt_message();"
   value="Verschlüsseln" id="encrypt" />

<button type="submit" disabled="true" id="send">Senden</button>

</FORM>
```

5. Außerdem ist der eigene OpenPGP-Public-Key als versteckter DIV-Container mit der ID *pubkey* irgendwo im HTML-Code einzubauen.

```
<div id="pubkey" hidden="true">
-----BEGIN PGP PUBLIC KEY BLOCK-----
....
-----END PGP PUBLIC KEY BLOCK-----
</div>
```

6. Für Surfer, die JavaScript standardmäßig deaktivieren, kann man einen Hinweis einfügen, dass JavaScript für die Funktion des Formulars nötig ist:

```
<NOSCRIPT>
Bitte aktivieren Sie JavaScript für die Verschlüsselung der Nachricht!
</NOSCRIPT>
```

Hinweise: Einige ältere Browser können keine Krypto-tauglichen Zufallszahlen mit JavaScript erzeugen. Das kann die Verschlüsselung deutlich schwächen. Deshalb ist es mit diesen Browsern nicht möglich, das Formular zu nutzen. Außerdem kann die Verschlüsselung auf dem Server durch unbemerkte Modifikationen am JavaScript-Code angegriffen werden. Trotzdem ist es besser, als keine Verschlüsselung zu verwenden.

10.3.6 OpenPGP Keyserver

Die OpenPGP-Keyserver bilden eine Infrastruktur im Web, um öffentliche Schlüssel auch Unbekannten zum Download anzubieten. Die verschiedenen Server synchronisieren ihren Datenbestand. Man kann die Keyserver nach einem passenden Schlüssel durchsuchen.

- Auf der Kommandozeile bzw. der DOS-Box kann man nach OpenPGP-Schlüsseln anhand der E-Mail-Adresse suchen und einen der gefundenen Schlüssel importieren:

```
> gpg2 --search max.mustermann@privacy-handbuch.de
```

Wenn man die Key-ID oder den Fingerprint des Schlüssels kennt und weiß, dass der Schlüssel auf einem Keyserver zu finden ist, kann man ihn auch direkt importieren:

```
> gpg2 --recv 0xD51D2D79912F0D9B73586C908CD51D2D7E36E399
```

- In Enigmail findet man die Suchfunktion in der Schlüsselverwaltung unter dem Menüpunkt *Schlüssel-Server → Schlüssel suchen.*

Keyserver-Pool von OpenPGP (mit E-Mail-Verifikation)

Der Keyserver-Pool https://keys.openpgp.org stellt einen modernen Keyserver für OpenPGP-Schlüssel zur Verfügung, der einige Probleme der alten Keyserver wie die des SKS-Keyserver-Pools vermeidet. Insbesondere werden die E-Mails in den Schlüsseln verifiziert, um das Problem mit Fake-Keys (siehe unten) zu lösen. Der Pool ist außerdem auch als Tor-Onion-Service-v3-Adresse erreichbar.

Auf der Webseite kann man seinen eigenen Schlüssel hochladen. Es werden E-Mails mit einer Aufforderung zur Bestätigung an alle Adressen gesendet, die im Schlüssel genannt werden. Die E-Mails enthalten einen Link, den man im Browser öffnen muss, um den Erhalt der E-Mail zu bestätigen. Danach werden die Schlüssel freigeschaltet.

Thunderbird verwendet standardmäßig nur diesen Keyserver, eine Anpassung der Konfiguration ist nicht nötig. Um den Keyserver auch mit dem Programm *gpg2* auf der Kommandozeile zu nutzen, kann man den Keyserver in der Konfigurationsdatei *$HOME/.gnupg/dirmngr.conf* (Linux) bzw. *%APPDATA%/GnuPG/dirmngr.conf* (Windows) konfigurieren und folgende Optionen einfügen:

```
keyserver hkps://keys.openpgp.org
keyserver
 ↪  hkp://zkaan2xfbuxia2wpf7ofnkbz6r5zdbbvxbunvp5g2iebopbfc4iqmbad.onion
```

Wenn genau zwei Keyserver konfiguriert werden und einer davon ein Tor-Onion-Service ist, dann verwendet GnuPG automatisch den Onion-Service, wenn Tor Onion Router läuft.

Nach der Änderung der Konfiguration muss *Dirmngr* evtl. beendet werden:

```
> gpgconf --kill dirmngr
```

(Zukünftige Versionen von GnuPG werden diesen Keyserver standardmäßig nutzen.)

Hinweis: dieser Keyserver entfernt aus Sicherheitsgründen alle Signaturen von Dritten aus den hochgeladenen Schlüsseln. Die Verifikation von Schlüsseln anhand der Signaturen (*Web of Trust*) ist also nicht möglich.

Vorsicht bei der Nutzung von veralteten SKS-Keyservern!

Man kann auf den Keyservern des SKS-Pool und ähnlichen veralteten Servern anhand von E-Mail-Adressen, 8-stelligen oder 16-stelligen Key-IDs oder bekannten Fingerprints nach Schlüsseln suchen.

1. Wenn man nach der E-Mail-Adresse sucht, dann werden unter Umständen mehrere Schlüssel zum Importieren angeboten. Es gibt immer wieder Witzbolde, die Schlüssel für fremde E-Mail-Adressen auf den Keyservern hochladen (um zu stänkern?).

   Wenn man zum Beispiel den Schlüssel von Felix v. Leitner (Fefe) sucht, dann findet man fünf Schlüssel. Aber nur der Schlüssel von Oktober 2013 ist korrekt (nicht der neueste Schlüssel!), wie Fefe in seinem Blog schreibt.[16]

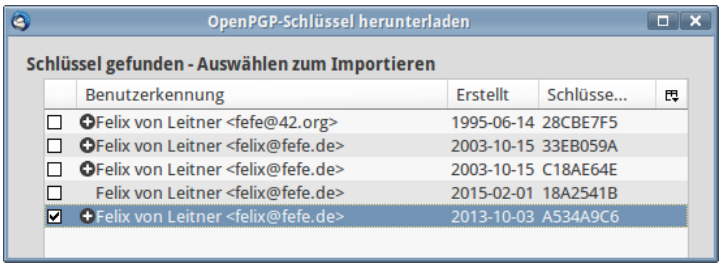


Abbildung 10.9: Fünf OpenPGP-Schlüssel für eine E-Mail-Adresse

   J. Schmidt von Heise.de beklagt, dass ein Scherzkeks OpenPGP-Schlüssel für seine E-Mail-Adresse auf die Keyserver hochgeladen hat und dass er die damit verschlüsselten E-Mails nicht lesen kann (Editorial c't 6/2015).

   Erinn Clark signierte die Downloads des TorBrowserBundle. Für ihre E-Mail-Adresse wurden Fake-Schlüssel auf den Keyservern publiziert.[17]

   Gavin Andresen signierte die Bitcoin-Binaries, für seine E-Mail-Adresse wurden ebenfalls Fake-Schlüssel auf den Keyservern publiziert.[18]

2. Statt nach E-Mail-Adressen kann man auch nach der 8-stelligen Key-ID suchen (z. B. 0xA534A9C6). Diese Methode liefert bessere Ergebnisse, allerdings muss man die richtige Key-ID kennen. Auch diese Methode ist nicht sicher, da man diese Key-IDs ebenfalls faken kann, wie ein Forscherteam demonstrierte.[19]

3. Die 16-stellige Key-ID (z. B. 0xFC32CEECA534A9C6) ist schwieriger zu faken, aber auch nicht als kryptografisch sichere ID entworfen.

4. Am besten ist es, wenn man den gesuchten Schlüssel anhand des Fingerprints sucht (z. B. 0x68995C53D2CEE11B0E4182F62146D0CD2B3CAA3E). Diese Suche liefert als einzige Variante vertrauenswürdige Ergebnisse.

10.3.7 Web des Vertrauens (WoT)

Im Prinzip kann jeder Anwender einen Schlüssel mit beliebigen E-Mail-Adressen generieren. Um Vertrauen zu schaffen, gibt es das **Web of Trust**.

Hat Beatrice die Echtheit des Schlüssels von Conrad überprüft, kann sie diesen mit ihrem geheimen Schlüssel signieren und der Community zur Verfügung stellen oder direkt an Anton schicken. Anton, der den Schlüssel von Beatrice bereits überprüft hat und(!) Beatrice als *vertrauenswürdige Person* definiert, kann damit aufgrund der Signatur auch dem Schlüssel von Conrad vertrauen.

[16] https://blog.fefe.de/?ts=aa27d652
[17] https://lists.torproject.org/pipermail/tor-talk/2014-March/032308.html
[18] http://gavintech.blogspot.ch/2014/03/it-aint-me-ive-got-pgp-imposter.html
[19] http://heise.de/-2473281

Es bildet sich ein kleines Netz von Vertrauensbeziehungen. Die Grafik 10.10 zeigt eine mögliche Variante für den Key von Anton (A).

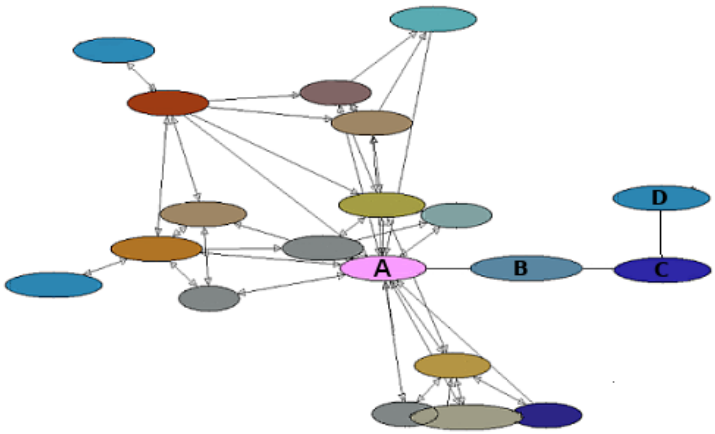


Abbildung 10.10: Beispiel für ein Web of Trust

- Anton (A) vertraut dem Schlüssel von Conrad (C), weil er von Beatrice (B) unterschrieben wurde und Beatrice für Anton eine vertrauenswürdige Person ist.
- Anton (A) vertraut dem Schlüssel von Doris (D) nicht, obwohl er von Conrad unterschrieben wurde und der Schlüssel von Conrad durch die Signatur von Beatrice als vertrauenswürdig gilt.

Warum vertraut Anton (A) dem Schlüssel von Doris (D) nicht automatisch? Weil er Conrad (C) nicht kennt und ihn daher nicht als *vertrauenswürdige Person* definiert hat!

Es bildet sich also kein weltweites Vertrauensnetz automatisch, indem man irgendwelche Schlüssel irgendwie unterschreibt und dann verteilt! Das Web of Trust funktioniert nur in einer kleinen Umgebung, weil zwei(!) Bedingungen erfüllt sein müssen. Neben einer digitalen Signaturkette muss auch jeder unterschreibender Nutzer in der Kette als *vertrauenswürdige Person* gekennzeichnet sein. Das geht nur, wenn man die Personen kennt.

Hinweis: Aktuelle GnuPG-Versionen importieren keine Signaturen von Dritten, wenn man sich einen PGP-Schlüssel von einem Keyserver holt, und moderne Keyserver wie der Pool von OpenPGP.org stellen auch keine Signaturen von Dritten mehr bereit. Thunderbird unterstützt das Signieren von Schlüsseln ebenfalls nicht mehr. **Das WoT ist praktisch tot.**

Das Web of Trust funktioniert nur in Ausnahmefällen, wenn man die Schlüssel direkt untereinander austauscht oder auf einer Webseite zum Download bereitstellt.

Certification Authorities

Diese Infrastruktur kann auch von vertrauenswürdigen Institutionen (Certification Authorities, CAs) genutzt werden. Die Nutzer wenden sich an die CA und lassen gegen Vorlage von Ausweisdokumenten den eigenen OpenPGP-Key signieren. Alle Partner benötigen lediglich den öffentlichen Schlüssel der CA, um die Echtheit der Schlüssel zu überprüfen.

In einer Gruppe kann eine vertrauenswürdige Person diese Rolle übernehmen. Alle Mitglieder eines Vereins oder einer Arbeitsgruppe oder die Mitarbeiter einer Firma senden ihre OpenPGP-Schlüssel an diese Person, die Schlüssel werden überprüft und signiert und an zentraler Stelle zum Download bereitgestellt. Die Mitglieder der Gruppe müssen nur den Schlüssel der Vertrauensperson überprüfen, signieren und die Vertrauenswürdigkeit des Inhaber setzen. Dann kann die Gruppe mit verifizierten Schlüsseln kommunizieren.

Weitere Beispiele für Certification Authorities sind:

- CAcert.org signiert auch OpenPGP-Schlüssel;
- Krypto-Kampagne der Zeitschrift c't;
- PCA des Deutschen Forschungsnetzes (DFN-PCA).

10.4 Verschlüsselte Dokumente per E-Mail senden

Manchmal möchte man eine vertrauliche E-Mail an einen Kommunikationspartner schreiben, der keine Ahnung von E-Mail-Verschlüsselung hat. Oder man möchte nicht, dass Schnüffelprogramme von Google, Yahoo! oder Microsoft die Mail lesen.

Als Alternative zur E-Mail-Verschlüsselung könnte man den Inhalt der Mail in ein verschlüsseltes Dokument packen und dieses Dokument als Anhang mit der Mail versenden. **LibreOffice**-Dokumente werden mit AES256 verschlüsselt, wenn man beim Speichern des Dokumentes die Option *Mit Kennwort speichern* aktiviert. Außerdem kann LibreOffice Dokumente mit OpenPGP verschlüsselt speichern (Abb. 16.1).

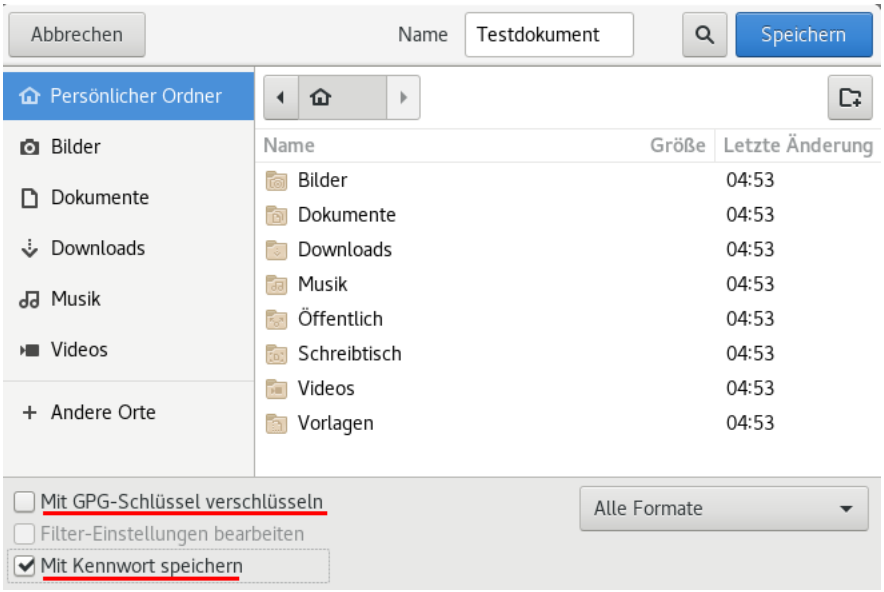


Abbildung 10.11: Verschlüsselte Speicherung in LibreOffice aktivieren

Wenn man keine OpenPGP-Schlüssel, sondern ein Kennwort verwendet, dann muss man dem Empfänger das Kennwort zum Öffnen der Datei über einen sicheren 2. Kanal mitteilen oder man schreibt im Text der E-Mail eine Andeutung, die nur der Empfänger interpretieren kann:

Das Passwort ist der Name der Bar, in der wir neulich ein Bier getrunken haben.

Man muss nicht für jede Nachricht ein neues Passwort definieren, sondern kann ein einmal sicher ausgetauschtes Passwort auch über einen längeren Zeitraum verwenden. Das ist sicherer, als immer wieder unsichere Methoden für den Passworttausch zu nutzen.

Kapitel 11

Instant Messaging und Telefonie

Instant Messaging und verschlüsselte Audio- und Videotelefonie wachsen immer mehr zusammen. Typische Messenger kann man auch für verschlüsselte Telefonie nutzen und Telefonie-Anwendungen können auch kurze Nachrichten und Dateien austauschen.

1. Messenger-Apps bieten neben 1:1-Chats und Dateitransfer auch Gruppenchats, Abstimmungstools und andere Social Features für textbasierte Kommunikation. Audio- und Videotelefonie ist inzwischen häufig enthalten, Videokonferenzen gibt es öfters.

   Die sogenannten Kanäle oder Channels bieten eine Top-Down-Kommunikation (der Boss spricht und Abonnenten dürfen lauschen). Außerdem unterscheiden sie sich von Gruppenchats darin, dass die Anzahl der Mitglieder unbegrenzt ist und dass ein Mitglied/Abonnent andere Mitglieder nicht sehen kann (Privatsphäre).

2. Telefonie-Apps wurden in erster Linie für verschlüsselte Audio- und Videotelefonie entwickelt. Als Zusatzfeature gibt es auch die Versendung von Nachrichten und Dateien, aber i. d. R. keine Gruppenchats und keine Kommunikation in Gruppen.

3. Videokonferenz-Systeme können i. d. R. einfach mit einem Webbrowser genutzt werden, für Smartphones sind Apps verfügbar. In den Videokonferenzen kann man die Kamera abschalten und nur via Audio-Talk teilnehmen. Es gibt eine Screen-Sharing-Funktion und man kann einzelnen Teilnehmern Nachrichten schicken.

Messenger mit verschlüsselter Audio- und Videotelefonie

Messenger werden primär auf dem Smartphone genutzt, denn ständige mobile Erreichbarkeit ist eine wesentliche Voraussetzung für *Instant* Messaging. Desktop-Clients sind i. d. R. auch vorhanden, aber manchmal nur als Zusatzoption zur Smartphone-App.

Einen idealen Messenger, der alle Bedingungen erfüllt, gibt es nicht. Man muss abwägen, welche Schwerpunkte man bei seinen Anforderungen setzt. Um viele Kontakte zu erreichen, könnte man mehrere Messenger parallel verwenden.

Threema ist einer der sichersten Messenger und hat eine 7-stellige Nutzerbasis. Es wird eine zufällige Buchstabenkombination als Kennung für den Account generiert, der optional mit einer Telefonnummer verknüpft werden kann. Neben Messaging-Funktionen gibt es verschlüsselte Audio- und Videotelefonie und Konferenzen sind mit bis zu 16 Teilnehmern möglich. (ausführlich: 11.1.1).

Als Hauptgerät zum Erstellen eines Accounts benötigt man ein Smartphone oder ein anderes Gerät (Tablet o. Ä.) mit Android OS bzw. iOS und Internetverbindung. Eine SIM-Karte ist nicht nötig.

Die Clients sind Open-Source und die gesamte Software wurde mehrfach auditiert.

Es gibt außerdem eine kommerzielle Version für Unternehmen und mit Threema OnPrem eine Version für hohe Sicherheitsanforderungen, die komplett beim Kunden gehostet wird.

Signal App ist kostenlos nutzbar, weil das Projekt durch großzügige Spenden von reichen Mäzenen finanziert wird. Der Messenger ist intuitiv bedienbar, hat inzwischen eine 9-stellige Nutzerbasis und ist führend bei Sicherheit und Privatsphäre. Signal App verwendet die Telefonnummer als Kennung für den Account und man benötigt ein Smartphone. Die Software ist Open Source, aber die Infrastruktur ist zentralisiert (ausführlich: 11.1.2).

Signal App ist ideal für die private Kommunikation mit Bekannten und Freunden, die nicht IT-affin sind und denen man bedenkenlos die eigene Telefonnummer geben kann. Neben Chats und Gruppenchats gibt es verschlüsselte Audio- und Videotelefonie sowie Audio- und Videokonferenzen mit bis zu 40 Teilnehmern.

Telegram bietet viele Social Features und ist als zensurresistente Twitter-Alternative mit Black Market Features populär geworden (z. B. bei Protesten in Hongkong und Belarus 2020), aber als Messenger für vertrauliche Kommunikation weniger geeignet (ausführlich: 11.1.3).

Telegram benötigt zwingend ein Smartphone als Hauptgerät und verwendet die Telefonnummer als Account-Kennung. Die Landesvorwahl dient dabei auch als Filterkriterium für die Umsetzung staatlicher Zensurvorgaben in den Twitter-ähnlichen Kanälen, die ein besonders Feature von Telegram sind.

Wire kann ohne Telefonnummer auf bis zu 8 Geräten genutzt werden. Neben Chats und Gruppenchats gibt es verschlüsselte Audio- und Videotelefonie, Audiokonferenzen mit bis zu 25 und Videokonferenzen mit bis zu 12 Teilnehmern.

Um die Synchronisation der Geräte zu gewährleisten, wird eine unverschlüsselte Datenbank mit den Metadaten auf den Servern geführt. Das ist praktisch eine Vorratsdatenspeicherung, die wir bei E-Mail seit 20 Jahren verhindern wollen. (Für Unternehmen mit Compliance-Anforderungen und eigenen Servern ist das nicht relevant.)

Wire Enterprise (Bund) ist der bevorzugte Messenger der Bundesregierung und vom BSI für VS-NfD zugelassen (BSI-VSA-10519). Wire ist eine gute Kollaborationsplattform für Unternehmen. Das öffentliche Wire hinkt in der Sicherheit hinterher und ist wegen der VDS weniger geeignet.

Jabber/XMPP, matrix sind ebenfalls kostenlos und Open Source. Im Gegensatz zu Threema, Signal App oder Telegram wird die föderale Infrastruktur von Enthusiasten betrieben. Jeder, der sich dazu in der Lage fühlt, kann eigene Server betreiben. Die Kennung für einen Account ist unabhängig von einer Telefonnummer frei wählbar und man kann einen oder mehrere Accounts in beliebigen Kombinationen auf mehreren PCs oder Smartphones nutzen. [matrix] bietet neben Chats und flexibel konfigurierbaren Gruppenchats auch verschlüsselte Audio- und Videotelefonie.

Ein Hauptziel von [matrix] und Jabber/XMPP ist es, eine föderale Infrastruktur ähnlich wie bei E-Mail zu schaffen, die mit beliebigen Clients genutzt werden kann. Während [matrix] expandiert, verliert Jabber/XMPP kontinuierlich an Bedeutung.

Community-basierte Entwicklung und föderale Infrastruktur erschweren die Einführung

und Umsetzung von Sicherheitsfeatures. M. Marlinspike hat diese Phänomene als systemimmanent für diese Open-Source-Projekte beschrieben.[1]

Der **bwmessenger** ist ein Fork für den Einsatz von [matrix] in der Bundeswehr. Für die Nutzung des *bwmessenger* gelten in der Bundeswehr die gleichen Regeln[2] wie für unverschlüsselte E-Mail und Telefonie:

- Auf Standardgeräten (Smartphones, Laptops, PCs) darf der bwmessenger in der Bundeswehr nur für offen eingestufte Kommunikation verwendet werden.
- Auf dienstlichen SMK-Geräten, die für **S**ichere **M**obile **K**ommunikation geeignet sind (SINA-Laptops, SecuSUITE-Smartphones), darf der bwmessenger genau wie unverschlüsselte E-Mails auch für VS-NfD-Kommunikation genutzt werden, da die SMK-Plattform die kryptografische Sicherheit gewährleistet.

Exoten mit besonderen Privacyfeatures

Session Messenger verwendet keine Telefonnummern als Account-Kennungen sondern eine lange, unhandliche Session-ID, die man am besten durch Scannen des QR-Codes bei einem persönlichen Treffen austauscht. Der Datenverkehr wird durch das OXEN-Onion-Netzwerk anonymisiert, um die Analyse von Metadaten zu verhindern.

Die Nachrichten sind Ende-zu-Ende-verschlüsselt (ohne Forward Secrecy) und Gruppenchats mit bis zu 100 Mitgliedern sind möglich. Dateien können mit einer Größe von max. 10MB verschickt werden. Für größere Dateien könnte man 1-Click-Hoster via TorBrowser nutzen.

Audio- und Videotelefonie ist ebenfalls möglich. Es wird dabei WebRTC als Verschlüsselungsstandard genutzt, aber keine Anonymisierung via OXEN-Onion-Netzwerk, da die Latenz des Onion-Routings für Audio- und Videotelefonie zu hoch ist.

Session Messenger kann auf mehreren Geräten und ohne Smartphone genutzt werden.

Alle Daten werden nur lokal auf dem Endgerät dauerhaft gespeichert. Es gibt aber kein Backup. Wenn man sein Smartphone verliert oder wechseln möchte, muss man den Account mindestens auf einem Zweitgerät eingerichtet haben. Anderenfalls verliert man alle Kontakte und Nachrichten, die älter als die Time-to-Life im OXEN Netzwerk sind (TTL: 3 Tage).

SimpleX (für Android und iPhones) ist ein relativ junger Messenger mit einem interessanten Konzept zur Vermeidung von Metadaten: Es gibt keine Account-IDs. Stattdessen werden beim Aufbau eines Chats Ende-zu-Ende-verschlüsselte Sessions zwischen zwei SimpleX-Clients eingerichtet. Die Server schieben nur die Datenpakete von A nach B durch das Netz oder puffern sie, wenn B nicht erreichbar ist.

Verschlüsselte Gruppenchats sowie Audio- und Videotelefonie sind ebenfalls möglich. Wenn man auf Audio- und Videotelefonie verzichtet, kann man SimpleX mit Tor Onion Router kombinieren, um die Anonymität bei der Nutzung zu verbessern.

Ohne Account-IDs gibt es auch keine Verifikation von Kommunikationspartnern. Um sicherzustellen, dass man wirklich mit dem gewünschten Gesprächspartner verbunden ist, kann der Aufbau einer Chat-Verbindung durch Scannen eines One-Time-QR-Codes bei einem persönlichen Treffen oder durch Versendung einer Einladung über einen sicheren, verifizierten Kanal erfolgen. (Die Frage, warum man SimpleX nutzen sollte, wenn es bereits einen verifizierten und sicheren Kommunikationskanal gibt, kann man ganz allgemein nicht beantworten.)

[1] https://www.signal.org/blog/the-ecosystem-is-moving/
[2] https://www.presseportal.de/pm/76712/4764023

SimpleX eignet sich insbesondere, wenn man geheimhalten möchte, dass man mit Person XY in Kontakt steht. Man sollte XY dann auf keine Fall in das Adressbuch eintragen, da diverse Apps das Adressbuch auslesen. Für den Alltag ist die Verbreitung zu gering.

Tox ist ein offenes Protokoll für verschlüsselte Telefonie und Chats, das für hohe Sicherheitsansprüche entwickelt wurde. Die Kommunikation läuft direkt von Client zu Client. Es gibt keine zentralen Server und keinen Provider, der Kommunikationsprofile erstellen könnte.

Briar gibt es für Android und in einer Beta Version für Desktop PCs/Laptops. Es ist ein Messenger für hohe Sicherheitsanforderungen. Die Kommunikation und Speicherung ist vollständig verschlüsselt. Es werden keine zentralen Server genutzt sondern Peer-2-Peer-Kommunikation via Tor Onion Router oder direkt via WLAN/Bluetooth, wenn kein Internet verfügbar ist.

Kontakte können nur bei einem persönlichen Treffen (Face-2-Face) hinzugefügt werden, indem man gegenseitig die QR-Codes scannt. Nur so ist nach Meinung der Entwickler sichergestellt, dass man wirklich mit der gewünschten Person kommuniziert.

Apps für verschlüsselte Audio- und Videotelefonie

Anwendungen für verschlüsselte Telefonie konnten sich in den letzten 10 Jahren im privaten Bereich nicht großflächig etablieren, obwohl die technischen Voraussetzungen mit der Standardisierung des SRTP/ZRTP Protokolls seit 2011 vorhanden gewesen wären. Aktuell bieten Messenger eine einfache Möglichkeit für verschlüsselte Audio- und Videotelefonie und machen zusätzliche SIP-Clients mit ZRTP-Verschlüsselung im privaten Bereich eigentlich überflüssig.

Jami ist eine Open-Source-App für verschlüsselte Telefonie, die weitestgehend ohne zentrale Server auskommt. Es wird eine Distributed Hash Table (DHT) zum Aufbau der Verbindung zwischen Clients verwendet Die Kommunikation läuft direkt zwischen den Clients. In einigen speziellen Fällen kommen zentrale Server zum Einsatz.

Wie andere Anwendungen, die Daten über eine DHT verteilen, sollte Jami aus dem Internet erreichbar sein. Anderenfalls kommt es zu zeitverzögerten, unregelmäßigen Zustellung von Nachrichten und verpassten Anrufen. Die Entwickler empfehlen, UPnP auf dem Router zu aktivieren und die Firewall abzuschalten, damit Jami das Port-Forwarding auf dem Router automatisch konfigurieren kann und erreichbar ist.

Hinweis: Das BSI, das FBI oder die US Homeland Security empfehlen ausdrücklich die Deaktivierung von UPnP zur Vermeidung von Sicherheitsrisiken! Wenn man diesen Empfehlungen folgt, wird man mit Jami im P2P Modus nicht glücklich.[3] [4] [5]

Linphone ist ein Open-Source-VoIP-Client für Smartphones und PCs. Wie bei VoIP üblich werden die Accounts auf föderal organisierten SIP-Servern verwaltet. Die Kommunikation erfolgt direkt zwischen den Clients oder über einen TURN-Server, wenn keine direkte Verbindung möglich ist. Als Besonderheit bietet Linphone verschlüsselte Audio-Konferenzen. Die Verschlüsselung der Audio- und Videokommunikation erfolgt mit SRTP/ZRTP.

Hinweis: VoIP Clients, die das SIP-Protokoll nutzen, müssen ebenfalls aus dem Internet erreichbar sein, damit der SIP-Server den Client bei Anrufen kontaktieren und die Verbindung vermitteln kann. Die Konfiguration von Router und Firewall ist machbar, für

[3] https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/basisschutz_fuer_den_router.html
[4] https://www.howtogeek.com/122487/htg-explains-is-upnp-a-security-risk/
[5] https://www.zdnet.com/article/homeland-security-disable-upnp-as-tens-of-millions-at-risk/

Nicht-ITler aber nicht ganz trivial. Deshalb konnte sich verschlüsselte VoIP-Telefonie in den letzten 20 Jahren im privaten Bereich nicht in der Breite durchsetzen.

Simlar.org ist ein deutsches Open-Source-Projekt für verschlüsselte VoIP-Telefonie. Der Source-Code für Clients und Server ist bei Github zu finden. Die Verschlüsselung der Kommunikation erfolgt mit SRTP/ZRTP. Die SIP-Server stehen in Deutschland.

Es gibt Apps für Android und iPhone. Im F-Droid-Store gibt es eine Google-freie Version. Diese Version muss ständig laufen und sollte nicht beendet werden, wenn man Anrufe annehmen will, da die Google Push Services nicht verwendet werden.

Lösungen für Videokonferenzen

Kommerzielle Lösungen für Videokonferenzen wie Microsoft Teams, Zoom oder Slack sind nicht DSGVO-konform. Es gibt aber Alternativen, die man auch selbst betreiben kann:

Jitsi Meet ist eine Open-Source-Software für den eigenen Konferenzserver.

Nextcloud Talk ist eine weitere Open-Source-Lösung für Videokonferenzen.

Eine durchgehende Ende-zu-Ende-Verschlüsselung gibt es bei Videokonferenzen nicht. In der Regel können die Server-Betreiber die Konferenzen beobachten. Man könnte deshalb den Server selbst aufsetzen oder einen vertrauenswürdigen Betreiber wählen.

Kommerzielle Angebote für Unternehmen

GSMK Cryptophones bieten ein ganzheitliches Sicherheitskonzept und High-End-Security. Sie sind aber auch mit 2.000+ Euro entsprechend teuer.

Silent Circle bietet mobile, verschlüsselte Kommunikation für Unternehmen, NGOs und Regierungen mit Enterprise-Features wie Verwaltung der Nutzer und Geräte.

SecuSUITE for Samsung Knox ist derzeit die bevorzugte Lösung für sichere mobile Kommunikation in deutschen Bundesbehörden und ist vom BSI für VS-NfD zugelassen.

Mobile Encryption App der Telekom adressiert Unternehmen und Behörden, die sich etwas preiswerter gegen Spionage durch starke (ausländische) Angreifer schützen wollen. Die App verschlüsselt Telefonie nach dem GSMK-Protokoll.

Die App verwendet ein eigenes verschlüsseltes Adressbuch und bietet einen sicheren Speicher für Notizen. Sie kann auch ohne SIM-Karte genutzt werden, da die Teilnehmer über individuelle +800-Telefonnummern adressiert werden. Die Infrastruktur wird von der Deutschen Telekom in deutschen Rechenzentren betrieben. Im September 2019 wurde die iOS-Version vom BSI für VS-NfD zugelassen. Die Freigabe der Android-Version für VS-NfD ist für 2020 geplant. Mit Kosten von 10-20 Euro pro Person ist die Mobile Encryption App für Unternehmen mit hohen Sicherheitsanforderungen eine preiswerte Alternative zu GSMK Kryptophones.

11.1 Instant Messaging

Die Übernahme von WhatsApp durch Facebook zeigt, dass es einfach Sch... ist, sich das gesamte Adressbuch mit allen Kontakten klauen zu lassen. Irgendwann landet es in den großen Datensammlungen von Google, Microsoft, Facebook oder Yahoo!, die alle als PRISM-Partner der NSA gelistet sind.[6]

In korrektem Juristen-Deutsch könnte man es DSGVO-konform z. B. so formulieren:[7]

> *Wer den Messenger-Dienst WhatsApp nutzt, übermittelt nach den technischen Vorgaben des Dienstes fortlaufend Daten in Klardaten-Form von allen in dem eigenen Smartphone-Adressbuch eingetragenen Kontaktpersonen an das hinter dem Dienst stehende Unternehmen (Facebook).*
>
> *Wer durch seine Nutzung von WhatsApp diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden.*

Wenn man als WhatsApp-Nutzer die Telefonnummern mit Bekannten austauscht, dann müsste man also eigentlich um die Zustimmung bitten, Name, Telefonnummer und Freundschaftsstatus an Facebook zu schicken. Das Gespräch könnte etwa wie folgt ablaufen:

- Anton: *Du hast doch nichts dagegen, wenn ich deinen Namen und dass wir Freunde sind mit deiner Telefonnummer an Facebook schicke – oder?*
- Beatrice: *Eyhh Mann, alles ok – mache ich doch auch.*

Anforderungen an einen guten Messenger

Unter Berücksichtigung des Crypto War 3.0 und der massiven Überwachung von Instant Messaging, welche durch E. Snowden bekannt gemacht wurde, ergeben sich folgende Anforderungen an einen guten Messenger-Dienst:

1. Sichere Ende-zu-Ende-Verschlüsselung nach dem aktuellen Stand der Technik, die durch unabhängige Experten evaluiert werden kann. Die Auswertung von 160.000 Überwachungsberichten aus dem Snowden-Fundus[8] zeigt, dass Geheimdienste die Messenger-Kommunikation massiv überwachen.
2. Sichere Transportverschlüsselung (SSL/TLS) für die notwendige Kommunikation der Apps mit den Servern und zwischen den Servern. Dabei sollten alle Best-Practice-Empfehlungen umgesetzt werden, inklusive Certificate Pinning u. Ä.
3. Der Account sollte frei wählbar und nicht an eine Telefonnummer gebunden sein. Telefonnummern sind im Gegensatz zu E-Mail-Adressen ein eindeutiges Identifizierungsmerkmal und nicht so einfach austauschbar wie (Wegwerf-)E-Mail-Adressen. Das ermöglicht die Verknüpfung verschiedener Accounts bei unterschiedlichen Messaging-Diensten und die Zuordnung zu einer Person. Außerdem schützt die Weitergabe eines Pseudonyms statt Telefonnummer gegen Stalking.

[6] https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/whatsapp-will-infos-mit-facebook-teilen-12995
[7] https://www.lareda.hessenrecht.hessen.de/bshe/document/LARE190000030
[8] http://apps.washingtonpost.com/g/page/world/communication-breakdown/1153/

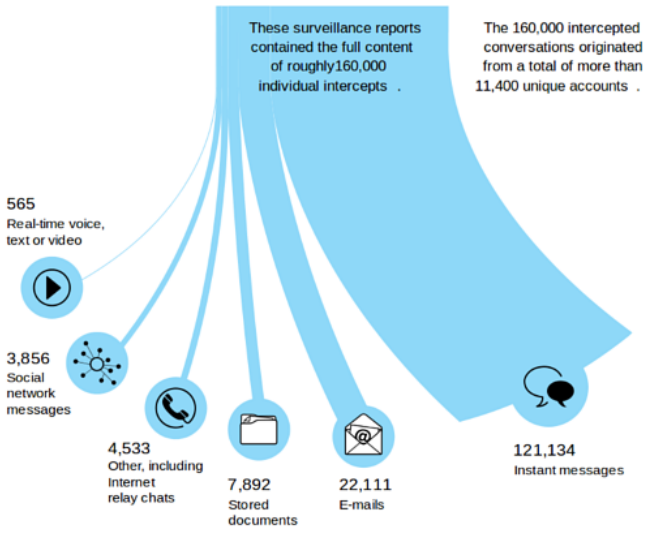


Abbildung 11.1: Auswertung von 160.000 Überwachungsberichten

4. Es sollte keine unerwünschten Uploads (Datenklau) ohne ausdrückliche Zustimmung durch den Nutzer geben. Der Dienst sollte auch komplett ohne Datenklau nutzbar sein und nur optional Daten wie das Adressbuch abgreifen.

5. Eine Google-freie Installation (beispielsweise via F-Droid) sollte möglich sein.

6. Die Nutzung auf dem Desktop-PC sollte möglich sein. Oft lässt es sich auf dem PC oder Laptop mit Tastatur/Bildschirm besser arbeiten als mit einem Smartphone.

7. Die Infrastruktur sollte dezentral verteilt sein und nicht von einem einzelnen Betreiber kontrolliert werden. Dezentrale Infrastrukturen sind nur schwer von Regierungen durch Gesetze kompromittierbar, um Geheimdiensten die Überwachung zu ermöglichen, wie z. B. mit BlackBerry in Indien oder in Kanada, mit Skype weltweit oder die Gesetze zu Backdoors für alle Messenger in Russland oder Australien.

   Im Gegensatz zu einigen Open-Source-Dogmatikern bin ich nicht der Meinung, dass die dezentrale Infrastruktur freier Messenger gegen die Installation von Backdoors auf den Servern schützt. Während bei Threema oder Signal App immer wieder angezweifelt wird, ob dort wirklich die auditierte bzw. veröffentlichte Software auf den Servern läuft, werden die Open-Source-Admins von Jabber- oder [matrix]-Servern per Definition zu Heiligen erklärt, die niemals nie etwas anderes installieren würden als die offizielle Serversoftware und niemals neugierig Metadaten beschnüffeln würden.

   Für diese Glorifizierung der Open-Source-Admins gibt es keinen Grund. Als wir vor einigen Jahren noch Jabber/XMPP mit OTR-Verschlüsselung verwendeten, hofften wir, dass die Admins der Server nicht mit dem Modul *mod_otr*[9] – *Man in the Middle Module for Off-the-Record* spielen oder es zumindest nicht gegen uns anwenden. Man musste vertrauen, so wie man Threema oder Signal App vertrauen muss.

   Die Gründe für Vertrauen sind sehr individuell. Manch einer sagt sich, *Ich vertraue dem Admin, weil es ein Bekannter ist.* Ein anderer denkt, *Ich vertraue dem Admin nicht, weil es ein Bekannter ist und die Neugier und Verführung zu einer kleinen Schnüffelei, die niemand bemerken würde, unter Bekannten größer ist.* (Stichwort Love-INT o. Ä.)

[9] https://www.ejabberd.im/mod_otr

8. Es wäre schön, wenn die Bedienung so einfach wäre, dass auch meine Tante und ihre Kaffeekranz-Freundinnen ohne lange Erklärungen damit umgehen könnten.

Einen idealen Messenger, der alle Bedingungen erfüllt, gibt es nicht. Man muss abwägen, was wichtig ist und welche Schwerpunkte man bei den Anforderungen setzt.

Multi-Device-Support und Ende-zu-Ende-Verschlüsselung

Multi-Device-Support ist heutzutage ein häufig gewünschtes Feature für Messenger. Man möchte via PC und Laptop online sein, um eine vernünftige Tastatur und einen großen Bildschirm zu nutzen, und man möchte via Smartphone unterwegs erreichbar sein. Dieses Feature erschwert es aber, eine sichere Ende-zu-Ende-Verschlüsselung zu realisieren.

Ein potenter Angreifer kann den Multi-Device-Support der Messenger-Protokolle nutzen, um ein weiteres Gerät im Namen des Opfers zu registrieren. Damit können alle Unterhaltungen mitgelesen werden und auch E2E verschlüsselte Chats sind betroffen.

- Das BKA hat diesen Angriff mehrmals erfolgreich gegen Telegram-Nutzer eingesetzt. Das Team von Prof. Fedderath demonstrierte, wie es geht:[10] Die Behörden gaben die Telefonnummer der Zielperson in der Telegram-Web-App ein und die SMS zur Autorisierung des Zugriffs wurde abgefangen. Dann konnten die unverschlüsselten Gruppenchats unbeobachtet mitgelesen werden. Die geheimen Chats von Telegram konnten damit nicht geknackt werden, da die Verschlüsselung MTProto nicht Multi-Device-fähig ist.

- Außerdem konnte das BKA durch Registrierung eines zusätzlichen Gerätes für den WhatsApp-Account von Magomed Ali-C. (ein Terrorverdächtiger aus dem Umkreis von Anis Amri) die Ende-zu-Ende-verschlüsselten Chats mitlesen. Dafür brauchte das BKA allerdings kurzzeitig einen unbeobachteten Zugriff auf das entsperrte Handy von Magomed Ali-C., um das zusätzliche Gerät zu aktivieren.

- Im Iran wurden seit 2014 wesentlich elegantere Angriffe staatlicher Hacker auf Telegram und WhatsApp eingesetzt. Mit der Zusendung eines bösartigen Dokumentes wurden die Smartphones der Opfer kompromittiert und dann die Account-Credentials von WhatsApp oder Telegram ausgelesen. Damit konnten die Angreifer ein weiteres Gerät im Namen des Opfers registrieren und den Multi-Device-Support exploiten.

- Im August 2022 wurde der SMS-Dienstleister Twilio, der auch von Signal App zur Versendung von SMS genutzt wird, mit einer Phishing-Attacke angegriffen. Die Angreifer verschafften sich damit Zugang zur Infrastruktur und versuchten, für drei Signal-Nutzer ein neues Gerät zu registrieren und die SMS zur Verifikation abzufangen. Bei einem Nutzer waren sie erfolgreich und hatten mehrere Stunden Zugang zur aktuellen Kommunikation. Ein Zugriff auf Kontakte oder alte Nachrichten war aufgrund der sicheren Konzeption von Signal App nicht möglich.

- Das Audit der OMEMO-Verschlüsselung[11] für Jabber/XMPP beschreibt einen möglichen Man-in-the Middle-Angriff auf die Verschlüsselung, der ebenfalls die Multi-Device-Fähigkeiten des Protokolls ausnutzt. Ein Angreifer (Eve) veranlasst Alice, ein neues Gerät mit einem eigenen Key für Bob in die Liste aufzunehmen. Alice sendet in Zukunft alle Nachrichten verschlüsselt mit den Schlüsseln für Bob+Eve. Eve kann die Nachrichten mitlesen, ohne die Krypto brechen zu müssen. Um unentdeckt zu bleiben, entfernt Eve ihre

[10] https://www.youtube.com/watch?v=wBaj0LxcnY8
[11] https://conversations.im/omemo/audit.pdf

Geräte-ID, bevor sie die Nachricht an Bob weiterleitet (Abb. 11.2). Diese Manipulation ist bei OMEMO möglich, weil die Nachrichten nicht kryptografisch authentifiziert werden. (Hat man das einfach vergessen?)

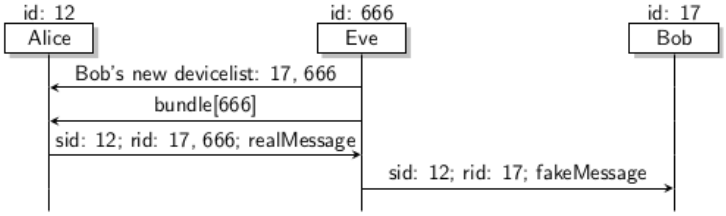


Abbildung 11.2: Man-in-the-Middle-Angriff auf OMEMO Verschlüsselung

- Das Paper *Practically-exploitable Cryptographic Vulnerabilities in Matrix*[12] beschreibt mehrere Angriffe auf die Verschlüsselung bei [matrix]. Ein bösartiger Homeserver kann zusätzliche Nutzer in E2E-verschlüsselte Räume einfügen oder neue Geräte für einen User registrieren und damit alle E2E-verschlüsselten Chats dieses Nutzers mitlesen, solange der Nutzer das zusätzliche Gerät oder den neuen Teilnehmer im Raum (Gruppenchat) nicht bemerkt. Außerdem könnte ein bösartiger Homeserver Sessions kompromittieren und sich selbst als Man-in-the-Middle in ausgewählten Räumen platzieren oder sich als vertrauenswürdiges Gerät eines Nutzers ausgeben und ein Backup anfordern, das Zugriff auf alle Daten bietet.

Schutz gegen Angriffe, die ein zusätzliches Gerät für einen Account registrieren wollen:

1. Bei Multi-Device-fähigen Messengern wie Signal App oder Telegram kann man eine zweistufige Bestätigung bzw. Registrierungssperre für das Hinzufügen neuer Geräte aktivieren. Damit ist für die Anmeldung eines neuen Gerätes eine zusätzliche Passphrase bzw. PIN erforderlich, die sich vom Account-Passwort unterscheiden sollte. Die oben genannten Angriffe sind dann nicht mehr möglich.

2. Als Schutz gegen Angriffe bei (kurzzeitigem) physischem Zugriff auf ein entsperrtes Smartphone bieten hochwertige Messenger eine zusätzliche PIN-Sperre für die App, die man bei hohem Schutzbedarf aktivieren kann. Damit wird verhindert, dass ein Angreifer die App auf dem Smartphone starten kann und damit die Rechte erlangt, um ein zusätzliches Gerät anzumelden.

Anmerkung: Die Krypto-Protokolle OTR (Jabber/XMPP) und MTProto (Telegram) sind nicht Multi-Device.fähig und daher von diesem Angriff nicht betroffen.

Multi-Device-Support als Mini-Cloud

Der moderne Mensch nutzt heutzutage oft mehrere Geräte (neben dem Smartphone noch einen Desktop-PC zuhause und/oder einen Laptop für die Reise). Damit steht man vor dem Problem, das man Daten (Fotos, Urlaubsdokumente, Passwörter usw.) auf mehreren Geräten braucht. Man könnte ein E-Mail an sich selbst schicken – könnte man machen . . . ist aber suboptimal.

Man kann auch den Multi-Device-Support moderner Messenger dafür nutzen. Dabei profitiert man von der Ende-zu-Ende-Verschlüsselung der Daten. Bei wirklich guten Messenger wie Signal App

[12] https://nebuchadnezzar-megolm.github.io/

oder Threema werden die Daten ausschließlich verschlüsselt auf den eigenen Geräten gespeichert und liegen nicht unverschlüsselt auf Servern von Dritten rum. Außerdem ist man flexibler, da neben beliebigen Dateien und Notizen auch Sprachmemos unkompliziert genutzt werden können.

Für die Messenger-Mini-Cloud richtet man sich einen oder mehrere private (verschlüsselte) Gruppenchats ein, zu denen Dritte keinen Zugang haben und die man für Selbstgespräche nutzt. Alle Dateien, Notizen oder Sprachmemos, die man hier ablegt, stehen auf allen Geräten zur Verfügung, auf denen ein Client für den Messenger installiert ist. (Funktioniert mit allen Messengern.)

In den Desktop-Clients von Signal App oder Telegram ist ein Chat für die Selbstgespräche schon vorbereitet. Man kann sie in den Desktop-Clients aktivieren.

- Beim Signal-App-Desktop-Client startet man den Chat *Note to Self* (Abb. 11.3).

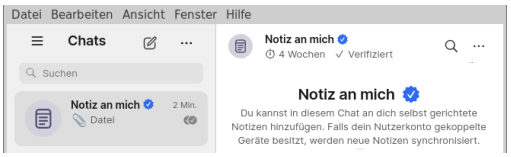


Abbildung 11.3: Signal Desktop: *Note-to-Self*-Chat aktivieren

- Beim Telegram-Desktop-Client startet man den Chat *Gespeichertes*, den man im Menü findet, das man mit einem Klick auf das Burgersymbol oben rechts öffnet.

  Hinweis: Bei Telegram werden die Daten zwar verschlüsselt auf den Servern abgelegt aber Telegram hat auch die Schlüssel, ist also fast so wie E-Mails an die eigene Adresse, die unverschlüsselt beim E-Mail-Provider rumliegen.

Harte und weiche Verifikation

Auch wenn die Krypto nicht gebrochen werden kann, sind verschiedene Angriffe möglich:

Social Attacks greifen nicht die Krypto an. Stattdessen versucht ein Angreifer (Mallory), sich das Vertrauen zu erschleichen, indem er sich als eine bekannte Person ausgibt:

- Mallory: *Hi Anton, ich bin Beatrice und wollte über das geheime Ding ...*
- Anton: *Hallo Beatrice – schön dass Du Dich meldest – also ...*

... und gleichzeitig in die andere Richtung:

- Mallory: *Hi Beatrice, ich bin Anton. Also zu diesem geheimen Ding ...*
- Beatrice: *Ohhh – Anton, schön dass Du Dich meldest. Tja also ...*

Und damit wäre Mallory ein MitM, solange Anton und Beatrice sich nicht gegenseitig verifizieren. Dieser Angriff ist bei Messengern einfacher, die anonyme Accounts ermöglichen, die nicht an eine Telefonnummer gebunden sind. Bei Signal App o. Ä. wäre zusätzlich noch ein SIM-Swap nötig.

Angriffe auf die Schlüssel attackieren den Schlüsseltausch. Um eine einfache Kontaktaufnahme zu ermöglichen, wenn der Gegenüber offline ist, stellen viele einfache Messenger die Public-Keys der Nutzer auf den Servern zur Verfügung. Ein bösartiger Betreiber könnte

prinzipiell die Keys austauschen und den Datenverkehr umleiten, sodass Mallory wieder in der Mitte sitzt und als Reflektor agieren kann, der die Nachrichten umschlüsselt und mitliest.

Gegen diese Angriffe schützt eine Verifikation der Kommunikationspartner:

Weiche Verifikation schützt gegen Social Attacks. Man könnte den Gegenüber via Audio- oder Videocall anrufen (Messenger unterstützen es) und wenn man den Gegenüber erkennt und die Verschlüsselung prüft, chattet man mit der richtigen Person.

Wenn der Account des Gegenüber mit einer Telefonnummer verknüpft ist, dann ist eine Verifikation via Adressbuch möglich. Einige Messenger können die Telefonnummer mit dem Adressbuch abgleichen und schützen damit gegen Social Attacks.

- Bei Signal App ist das standardmäßig der Fall, so dass diese Social Attacks unter Bekannten, die die Telefonnummern ausgetauscht haben, schwer möglich sind.
- Bei Threema kann man einen Account optional mit einer Telefonnummer verknüpfen (und damit die Anonymität teilweise aufgeben). Threema speichert Hashwerte der verknüpften Telefonnummer oder E-Mail-Adresse auf dem Server und zeigt eine schwache (weiche) Verifikation an, wenn der Client die verknüpfte Telefonnummer im Adressbuch findet.
- Bei Telegram wird die Telefonnummer aus dem Adressbuch unter dem Account angezeigt, die man vergleichen könnte. Aufgrund der Implikationen für die Privatsphäre ist es aber nicht empfehlenswert, Telegram den Zugriff auf das Adressbuch zu erlauben.

(Es ist also nicht grundsätzlich verwerflich, wenn Messenger-Accounts mit Telefonnummern verknüpft werden. Es kommt darauf an, ob man den Messenger vor allem für vertrauliche, private Kommunikation mit Bekannten verwenden möchte oder ob man in erster Linie anonym irgendwo rumtrollen will.)

Harte Verifikation überprüft die verwendeten Schlüssel. Ein universelles Verfahren zur Überprüfung der Schlüssel ist ein Vergleich der Fingerabdrücke der Schlüssel bei einem Face-2-Face Treffen oder out-of-band über einen unabhängigen, sicheren Kanal.

Der Fingerabdruck muss nicht unbedingt anhand kryptischer Zeichenfolgen verglichen werden, sondern könnte auch mit bunten Bildchen erfolgen, was intuitiver ist.

- Bei Face-2-Face Treffen scannt man gegenseitig einen angezeigten QR-Code.
- Bei einem unabhängigen Kanal muss man sicher sein, dass am anderen Ende des Kanals wirklich die gewünschte Person sitzt. Der Kanal muss verifiziert sein.

Die Notwendigkeit der Verifikation hängt wesentlich vom Verfahren des Schlüsseltausches beim Aufbau der Kommunikation und von den Sicherheitsanforderungen ab.

- Messenger für hohe Sicherheitsanforderungen wie Briar oder Tox haben einen sicheren Schlüsseltausch implementiert, der eine harte Verifikation einschließt.
- Signal App setzt nicht nur bei Verschlüsselung der Daten Maßstäbe, sondern auch beim Schlüsseltausch. Beim X3DH-Schlüsseltausch liegen nicht die Public-Keys auf dem Server, sondern abgeleitete Schlüssel, die nur in Kombination mit den echten privaten Keys auf den primären Endgeräten der Nutzer sinnvoll genutzt werden können.[13]

  Bei X3DH könnte ein bösartiger Provider die Verbindungsaufnahme blockieren. Es ist aber (nach aktuellem Stand) nicht möglich, modifizierte Keys einzuschleusen.

[13] https://signal.org/docs/specifications/x3dh/

- WhatsApp verwendet mit dem ECDH-Schlüsseltausch ein ähnliches Verfahren, dass ebenfalls von den Signal-Entwicklern entwickelt wurde.
- Die meisten anderen Messenger publizieren die Public-Keys auf den Servern und weisen mit Icons darauf hin, dass die Schlüssel verifiziert werden sollten.

Link-Previews in Messengern

Einige Messenger bieten einen Link-Preview, wenn man eine URL in das Eingabefeld tippt oder kopiert. Man kann den hübschen-Preview versenden oder vor dem Versand löschen.

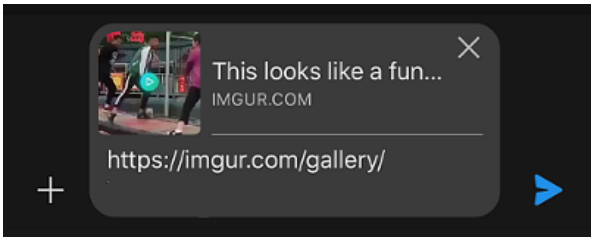


Abbildung 11.4: Link-Preview in einem Chat in Signal App

Voraussetzung für einen Link-Preview ist, das die Webseite im HTML-Header die Open-Graph-Metatags enthält. Anhand dieser Metatags wird der Preview generiert:

```
<HTML>
<HEAD>
...
<meta property="og:title" content="Ein Beispiel">
<meta property="og:description" content="Das ist nur ein sinnloses
↪  Beispiel">
<meta property="og:image"
↪  content="https://beispiel.tld/images/preview01.png">
...
```

Um einen Link-Preview zu generieren, kontaktiert der Messaging-Client den Webserver und versucht, die Webseite zu laden, sobald eine URL im Eingabefeld erkannt wird. Wenn die Webseite im Header die Open-Graph-Tags enthält, wird ein Preview generiert und evtl. das Bild heruntergeladen. Den Ablauf kann man sehr unterschiedlich implementieren:

- WhatsApp hat die einfachste Implementierung gewählt. Der WhatsApp-Messenger kontaktiert den Webserver direkt und hinterlässt damit Einträge in den Logs. Anhand der IP-Adresse kann damit die Verknüpfung zu einer Person erfolgen, wenn man bspw. den Link zu einer Facebook-Seite versendet und dabei gleichzeitig bei Facebook eingeloggt ist. (Aber WhatsApp-Nutzer stört das wahrscheinlich nicht.)
- Signal App generiert Link-Previews nur für Webseiten, die via HTTPS erreichbar sind, kontaktiert den Webserver ebenfalls direkt und tarnt sich dabei als *WhatsApp*. In den Datenschutz-Einstellungen von Signal kann man die Previews abschalten.
- Telegram hat eine mittelmäßige Lösung implementiert. Die Link-Previews werden auf dem Telegram-Server generiert. Das verhindert Implikationen für die Privatsphäre wie bei

WhatsApp, da nur der Telegram-Server die Webseiten kontaktiert und das Abrufen der Informationen keinem Nutzer individuell zugeordnet werden kann.

Bei unverschlüsselten Chats kann man das als brauchbare Lösung betrachten. Bei geheimen Chats, die Ende-zu-Ende-verschlüsselt sind, sollte der Telegram-Server aber keine Informationen über die Inhalte der Chats sammeln können. Deshalb sollte man die Link-Previews für geheime Chats abschalten. Die Option findet man in den Einstellungen unter *Privatsphäre und Sicherheit → Dateneinstellungen*.

- matrix macht es ähnlich wie Telegram. Bei unverschlüsselten Chats werden die Link-Previews vom Matrix-Server generiert. Dieses Feature kann in den Einstellungen von deaktiviert werden. Bei Ende-zu-Ende-verschlüsselten Chats sollen laut Spezifikation keine Link-Previews generiert werden.

11.1.1 Messenger Threema

Threema ist ein datenschutzfreundlicher Messenger aus der Schweiz. Chats, Gruppenchats sowie Audio- und Videotelefonie werden standardmäßig verschlüsselt. Es wird nicht die Telefonnummer als Kennung verwendet, sondern eine zufällige Buchstabenkombination.

Die Client-Apps sind Open-Source und die gesamte Software wurde mehrfach auditiert.[14] Die Finanzierung erfolgt durch geringe, einmalige Kosten beim Download der App. Außerdem gibt es mit *Threema Work* und *Threema OnPrem* kommerzielle Lösungen für Unternehmen, mit denen weitere Einnahmen für die Firma erwirtschaftet werden. Die Server stehen in der Schweiz.

Das Erstellen von Channels und Bots (die bei Telegram populär sind) ist nur mit dem kostenpflichtigen Zusatzfeature Threema/Broadcast[15] möglich, was den Missbrauch reduziert. Die Channels und Bots können aber von allen Threema-Nutzern abonniert werden.

Threema bietet horizontale Anonymität (Anonymität gegenüber Kommunikationspartnern). Man kann seine Threema-ID mit einem Link *https://threema.id/<8-stellige-ID>* in einem Blog o. Ä. veröffentlichen, um Anderen eine Möglichkeit zur anonymen Kontaktaufnahme zu geben, ohne die eigene Identität zu kompromittieren.

Zum **Erstellen eines Accounts** benötigt man ein Smartphone oder irgendein Gerät mit Android OS bzw. iOS mit Internetverbindung (Tablet o. Ä. geht auch). Eine SIM-Karte mit Telefonnummer ist nicht nötig. Auf diesem Phone bzw. Tablet installiert man die kostenpflichtige Threema-App.

Wenn man Threema vorrangig für die private Kommunikation mit Bekannten verwendet und nicht die Anonymität im Vordergrund steht, kann man in den Profileinstellungen **die Threema-ID mit einer Telefonnummer** oder einer E-Mail-Adresse **verbinden**. Dabei wird ein Hashwert der Telefonnummer mit der Threema-ID auf dem Server gespeichert. (Das Hashen der Telefonnummer bietet ein bisschen Schutz, sollte aber nicht überbewertet werden. Ein Angreifer, der Zugriff auf die Daten auf dem Server hat, kann mit überschaubarem Aufwand eine Rainbow Table mit den Hashwerten aller möglichen Telefonnummern erstellen und damit die Nummern aus den Hashwerten ermitteln.)

Kommunikationspartner können dann Kontakte aus dem Adressbuch schnell finden und anhand der farbig dargestellten Vertrauensstufe verifizieren, dass sie mit dem Bekannten verbunden sind, mit dem sie die bereits die Telefonnummer ausgetauscht haben.

Threema kennt folgende **Vertrauensstufen** bei Kontakten:

[14] https://threema.ch/de/faq/code_audit
[15] https://broadcast.threema.ch/de

- **rot:** ID und öffentlicher Schlüssel wurden vom Server geholt. Da kein passender Kontakt im Adressbuch gefunden wurde, kann man sich nicht sicher sein, ob die Person wirklich die ist, die sie in ihren Nachrichten vorgibt zu sein.
- **orange:** Der Kontakt wurde im Adressbuch gefunden. Da der Server Handynummern und E-Mail-Adressen prüft, kann man sich ohne zusätzliches Verifizieren relativ sicher sein, dass diese Person wirklich diejenige ist, die man meint.
- **grün:** Der öffentliche Schlüssel der Person wurde persönlich durch Scannen des QR-Codes verifiziert. Solange das Gerät der Person nicht gestohlen oder gehackt wurde, ist es für Dritte unmöglich, die Nachrichten zu fälschen oder mitzulesen.

Ende-zu-Ende-Verschlüsselung ist bei Threema standardmäßig aktiv. Im Dezember 2022 hat Threema dafür das neue Protokoll Ibex eingeführt und im August 2023 standardmäßig aktiviert, welches einige Schwächen beseitigt und auch Forward Secrecy bietet. Im Gegensatz zum alten Protokoll wird für die Übertragung jeder Nachricht ein individueller Session-Key ausgehandelt.

Verschlüsselte **Audio- und Videotelefonie** bietet Threema ebenfalls. Man startet ein Telefonat am einfachsten in einem Chatfenster, indem man oben rechts auf den Telefonhörer tippt. Während des Telefonates kann jeder Teilnehmer unabhängig vom anderen seine Kamera aktivieren.

Um in Android 14+ verschlüsselte Anrufe so einfach annehmen zu können wie normale Telefonanrufe, muss man Vollbildbenachrichtigungen auf dem Sperrbildschirm zulassen. In den Android Einstellungen findet man die Option unter *Apps* → *Threema* → *Benachrichtigungen*.

Ende-zu-Ende verschlüsselte **Audio- und Videokonferenzen** sind mit bis zu 16 Teilnehmern möglich. Um eine Konferenz zu starten sammelt der Konferenzleiter alle potentiellen Teilnehmer in einer Chatgruppe und tippt in dem Chatfester des Gruppenchats oben rechts auf das Telefonsymbol. Alle Gruppenmitglieder erhalten eine Pushbenachrichtung und können der Audiokonferenz beitreten. Während der Audiokonferenz können die Teilnehmer individuell ihre Kamera aktivieren.

Ein **Backup** der Daten ist (im Gegensatz zu anderen Messengern) wichtig. Bei Threema speichert der Client alle Informationen zu Kontaktlisten, Mitgliedschaften in Gruppenchats usw. lokal auf dem Smartphone. Die Server haben keine Informationen. Wenn man das Smartphone wechselt oder verliert, muss man ohne Backup komplett neu beginnen und verliert alle Kontakte!

Das Backup wird mit einem Passwort verschlüsselt und kann auf dem Threema-Server oder auf einem beliebigen WebDAV-Server gespeichert werden. Wenn man das Backup auf einem eigenen WebDAV-Server speichern möchte, muss man dort ein Verzeichnis für Threema Safe anlegen (beispielsweise *threema-safe*) und ein Unterverzeichnis *backups*. In dem Threema-Safe-Verzeichnis ist die Datei *config* mit folgendem Inhalt anzulegen:

```
{
   "maxBackupBytes": 524288,
   "retentionDays": 180
}
```

Dann kann man auf dem Smartphone ein Threema-Safe-Backup erstellen und als Experte die eigene WebDAV-Adresse des Threema-Safe-Verzeichnisses inklusive Login Credentials für den WebDAV-Server angeben (Abb. 11.5).

Der Name der Backupdatei ist die mit dem Backup-Passwort verschlüsselte Threema-ID. Auch wenn das Backup auf dem Threema-Server rumliegt, ist nicht erkennbar, zu welchem Account es

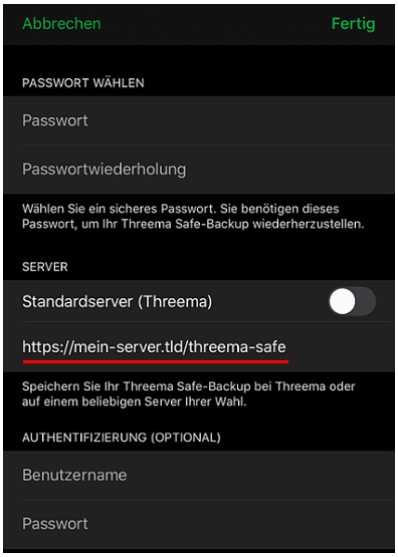


Abbildung 11.5: Eigenen WebDAV-Server für das Threema-Backup auswählen

gehört. Trotzdem kann die Datei beim Restore eindeutig gefunden werden. Dieses Konzept ist bisher unter Messengern einmalig.

Threema selbst erfordert zwar keine Telefonnummer. Durch die Nutzung der **Push Services** von Google (FCM) oder Apple (APN) für Benachrichtigungen vom Threema Server können die Accounts aber durch Google/Apple anhand der Push-Token mit einer Telefonnummer, Gerätekennung oder anderen persönlichen Informationen verknüpft werden (siehe Kapitel 21.7).

Auf iPhones gibt es keine Schutz dagegen und keine Alternative zum APN Push Service.

Für Android-Smartphones bringt Threema 4.71+ einen eignen Threema Push Service mit, der die Probleme für Privatsphäre und die mögliche Deanonymisierung anonymer Threema-Accounts durch Googles Push Service (FCM) vermeidet und den Akkuverbrauch nur wenig erhöht.

- Threema Push statt Google FCM kann man in den Einstellungen aktivieren: *Über Threema → Fehlerbehebung → Threema Push benutzen.*

  (Hinweis: Wenn auf Google-freien Smartphones kein Google Push Service (FCM) verfügbar ist, wird automatisch Threema Push verwendet.)

- Außerdem muss man für die Threema-App *Hintergrundaktivität* und *Hintergrunddatenverkehr* erlauben, damit es funktioniert. Bei einigen Android-Smartphones muss man auch für den Akkubetrieb für Threema die Option *nicht einschränken* aktivieren.

- Weitere Hinweise für spezielle Smartphone-Typen finden man in den FAQ.[16]

Für Android-Phones gibt es neben Google Play weitere **Downloadmöglichkeiten**:

- Threema Libre ist eine Google-freie Version von Threema, die keine proprietären Bibliotheken von Google o. A. enthält und über ein F-Droid-Repository installiert wird.[17]

  Beim Wechsel von Threema aus dem Play Store auf Threema Libre muss man eine neue Lizenz kaufen, da kein Zugriff auf die alte Lizenz im Play Store möglich ist.

[16] https://threema.ch/de/faq/push_andr2
[17] https://threema.ch/de/blog/posts/threema-libre-de

- Im Webshop[18] von Threema kann man die App für Android-Smartphones kaufen, wenn man keinen Google Play Store und kein F-Droid-Repository verwenden möchte.

Parallel zur Smartphone-App kann man **Threema Desktop**[19] auf dem PC oder Laptop installieren, was nach dem Download relativ simpel ist und nicht weiter erklärt werden muss. Wenn man Threema Desktop startet, muss man mit der Threema-App auf dem Smartphone den angezeigten QR-Code scannen, um beide Geräte zu verbinden. Die Smartphone App ist dabei der Boss in dem Verbund und in den Einstellungen können die aktiven Desktop Clients verwaltet werden.

Multi-Device Support bietet Threema noch nicht. Aber wenn man mehrere Smartphones nutzt, kann man sich mit einem kleinen Trick behelfen und die Gruppenchats dafür missbrauchen.

1. Anton verwendet mehrere Geräte und erstellt auf jedem Gerät eine Threema-ID.
2. Für die Kommunikation mit Beatrice erstellt er eine Gruppe mit allen seinen Accounts und fügt außerdem den Account von Beatrice hinzu.
3. Für die Kommunikation mit Conrad erstellt er eine weitere Gruppe mit seinen Accounts und fügt den Account von Conrad dazu.
4. Dann muss er Beatrice und Conrad noch erklären, dass sie die jeweilige Gruppe verwenden sollen, wenn sie ihm schreiben wollen, und nicht eine von seinen Threema-IDs.

Das ist ein bisschen umständlicher als bei echtem Multi-Device Support, aber machbar.

11.1.2 Messenger Signal App

Signal App ist kostenlos. Betrieb und Entwicklung werden von der Signal Foundation finanziert. Die Kapitaleinlagen der Fondation stammen u.a. von WhatsApp Gründer B. Acton, von der Shuttleworth Foundation und Spenden von Nutzern. Der Quellcode ist bei Github verfügbar.[20]

Signal App wird von Security-Experten aufgrund der guten Ende-zu-Ende-Verschlüsselung empfohlen. Das 2013 veröffentliche Krypto Protokoll X3DH[21] wurde von vielen Messengern adaptiert und entwickelte sich zu einem Quasi-Standard für verschlüsselte Chats. 2023 begann Signal als erster Messenger mit der Umstellung auf Post-Quantum-Crypto und veröffentlichte das Protokoll PQXDH[22], das robust gegen zukünftige Angriffe mit Quantencomputer ist.

Auch für die Forensikexperten von Elcomsoft und Cellbrite, die sich darum bemühen, auf Smartphones gespeicherte Daten auszulesen, ist Signal *state of the art* bei der Datensicherheit.

> *For the record - @moxie writes crypto software that blinds the #NSA & #GCHQ. He is their nightmare. Usable crypto developer with a backbone!* (J. Appelbaum)

Aus Sicherheitsgründen kann man Signal App nur mit einem Smartphone nutzen. Mehrere Smartphones mit dem gleichen Account sind nicht möglich. Zusätzlich kann man bis zu 5 Desktop-Clients mit dem Account verbinden. Um Signal Desktop mit einem Account zu verbinden, muss man den QR-Code von der Desktop-App mit dem Smartphone scannen.

[18] https://shop.threema.ch/
[19] https://threema.ch/de/download
[20] https://github.com/WhisperSystems
[21] https://signal.org/docs/specifications/x3dh
[22] https://signal.org/docs/specifications/pqxdh

Neben der Verschlüsselung setzt Signal auch konzeptuell neue Standards für Messenger. Alle Nachrichten, Kontaktlisten, Mitgliedschaften in Gruppenchats, persönliche Daten wie das Profilfoto usw. werden lokal in der Signal-App gespeichert. Die Server speichern keine Informationen sondern transportieren nur verschlüsselte Nachrichten und Statusinformationen zu den Empfängern, ohne die Absender zu kennen (Sealed Sender).

Für brisante Inhalte gibt es **verschwindende Nachrichten**. Wenn diese Option für einen Chat aktiviert wird, werden die Nachrichten eine einstellbare Zeit nach dem Lesen auf beiden Seiten gelöscht. In den Einstellungen kann man einen Standardwert von 30 Sekunden bis zu 4 Wochen für alle neuen Chats definieren.

Dass die **Telefonnummer als Identifier** verwendet wird, wurde oft kritisiert (Datensparsamkeit usw.) Dabei wird unterschlagen, dass die Verifizierung des Gegenüber anhand der Telefonnummer ein Sicherheitsfeature ist. Man kann sich relativ sicher sein, dass man wirklich mit der gewünschten Person verbunden ist, mit der man die Telefonnummer ausgetauscht und im Adressbuch gespeichert hat, und nicht irgendein unbekannter Dritter sich durch Vorspiegelung einer falschen Identität Vertrauen erschleicht. Außerdem erleichtert es das Finden von Kontakten und Etablieren einer sicheren Kommunikation mit Bekannten, was das Hauptziel von Signal App ist.

In den Einstellungen unter *Datenschutz* → *Telefonnummer* kann man konfigurieren, wer die Telefonnummer sehen kann und ob man anhand der Telefonnumer gefunden werden möchte.

- Die Anzeige der Telefonnummer ist sinnvoll bei Kontakten, bei denen man im Adressbuch steht, um eine weiche Verifikation zu ermöglichen. Ansonsten muss niemand meine Tel.-Nr. sehen.
- Anhand der Telefonnummer gefunden zu werden ist in der Regel ein sinnvolles Feature. Wenn man einem Bekannten seine Telefonnummer gibt, möchte man angerufen werden. Wenn der Bekannte dann sieht, dass er auch verschlüsselt via Signal telefonieren oder chatten könnte, ist das im Sinne des Angerufenen (von wenigen Ausnahmen abgesehen).

Einen **pseudonymen Benutzernamen** kann man in den Profil-Einstellungen festlegen, wenn man einen Signal Account erstellt hat. Der Benutzername besteht aus einer Buchstabenkombination, einem Punkt und einer zweistelligen Zahlenkombination. Die Zahlenkombination wird von Signal zufällig vorgeschlagen, ist zwar editierbar aber man sollte es bei der zufälligen Zufallszahl belassen (statt dem Geburtsjahr o.ä.), damit Dritte den Benutzernamen nicht einfach erraten.

Potentiellen Kommunikationspartnern kann man dann statt der eigenen Telefonnummer diesen pseudonymen Benutzernamen geben, man könnte ihn als Link auf Webseiten veröffentlichen (z.B. als Journalist, um für potentielle Whistleblower eine Ansprechmöglichkeit zu veröffentlichen) oder via QR-Code zum Scan anbieten. Das schützt vor Stalking oder ähnlichem Missbrauch der Telefonnummer (z.B. beim Casual Dating) und erweitert die Einsatzmöglichkeiten von Signal.

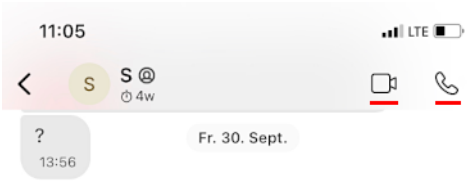
Die pseudonymen Benutzernamen sind aber kein Anonymitätsfeature sondern dienen nur dem Aufbau einer Kommunikationsbeziehung ohne Weitergabe der Telefonnummer. Da damit die weiche Verifizierung des Gegenüber anhand der Tel.-Nr. entfällt, muss man sich später darum kümmern. Dafür könnte man bei einem Treffen die Sicherheitsnummer des Chat vergleichen.

(Pseudonyme Benutzernamen bieten auch Missbrauchspotential. Falls euch jemand beispielsweise einreden möchte, ihr könntet unter dem Pseudonym *cane.69* den Chefautor vom PrHdb erreichen, dann klingt das für einige Leser vielleicht plausibel, wäre aber ein Fake!)

Hinweis: Wenn man von einigen Chatpartnern nur die Benutzernamen kennt und nicht die Telefonnummer im Adressbuch hat, muss man sich über Backups Gedanken machen. Ein Backup des Adressbuches reicht dann nicht mehr aus, um alle Kontakte bei Totalausfall wieder zu

erreichen. Man könnte Benutzernamen in einer Passwortdatenbank wie KeepassXC ablegen oder Signal-PIN aktivieren (verschlüsseltes Backup auf den Signal Servern, ohne Chatinhalte).

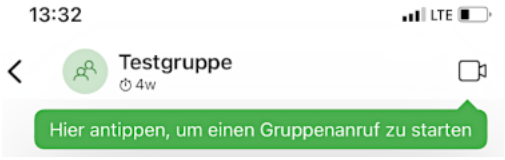
Verschlüsselte **Audio- und Videotelefonie** ist bei Signal App einfach. Einen Telefonanruf oder Videocall mit einer anderen Person startet man am einfachsten im Chatfenster.



Ob Signal-Anrufe in der globalen Call-History angezeigt und damit in die iCloud oder Google-Cloud synchronisiert werden, ist in den Einstellungen konfigurierbar.

Um in Android 14+ verschlüsselte Anrufe so einfach annehmen zu können wie normale Telefonanrufe, muss man Vollbildbenachrichtigungen auf dem Sperrbildschirm zulassen. In den Android Einstellungen findet man die Option unter *Apps* → *Signal* → *Benachrichtigungen*.

Videokonferenzen mit bis zu 40 Teilnehmern sind möglich. Für eine Konferenz erstellt man eine Gruppe mit den Teilnehmern und tippt auf das *Group-Call*-Symbol.



Storys sind eher unwichtige Social-Media-ähnliche Statusmeldungen (*Was mache ich gerade*). Man kann ein Foto knipsen und/oder einen kurzen Text verfassen und an eine vorbereitete Empfängergruppe schicken. Bei den Empfängern werden die Storys für 24 h wenig störend im Story-Tab angezeigt und dann automatisch gelöscht. In den Einstellungen kann man unter *Storys* mehrere Gruppen von Empfängern vorbereiten (Familie, Freunde, Kollegen usw.) oder die Funktion abschalten.

Der Messenger Signal entstand aus TextSecure, einer App zum verschlüsselten Versenden von SMS. Diese Wurzeln beeinflussen noch heute die Konzepte von Signal. Eine SMS wird üblicherweise an einen Kontakt aus dem Adressbuch versendet. Natürlich kann man auch eine Telefonnummer eingeben, aber das macht man eher selten. Ähnlich arbeitet Signal App. Die (verschlüsselten) Nachrichten werden an Kontakte gesendet, die über die Telefonnummer adressiert werden. Die Namen als Bezeichner (Anzeige) und die Telefonnummern als Adressen von Kontakten holt sich Signal primär aus dem Adressbuch.

Beim Zugriff auf das **Adressbuch** bemüht sich Signal um einen Kompromiss zwischen einfacher Benutzbarkeit und Datenschutz. Wenn man nach neuen Kontakten sucht, werden die Hashwerte der Telefonnummern aus dem Adressbuch zu den Servern hochgeladen und dort niemals gespeichert. Ein Blog-Artikel erklärt das Verfahren.[23]

Wenn man sein Smartphone verliert oder wechselt, dann verliert man auch alle Daten, die Signal App gespeichert hat. Die Daten werden nur lokal auf dem Smartphone gespeichert und nicht auf den Servern von Signal. Deshalb braucht man ein Backup.

Das **Backup-Konzept** von Signal App ist dreistufig:

[23] https://signal.org/blog/private-contact-discovery/

1. Das Adressbuch auf dem Smartphone dient als primäres Backup für den den *Social Graph* (Liste der Kontakte). Mit einem Backup vom Adressbuch hat man sofort alle Kontakte in Signal wiederhergestellt (außer Gruppenchats). Signal ist primär ein Messenger für die Kommunikation mit privaten Kontakten, deren Telefonnummern man im Adressbuch hat.

2. Optional kann man mit der Signal-PIN als zweite Backup-Stufe die Mitgliedschaften in Gruppen, das Profilbild sowie die Einstellungen und Daten neuer Funktionen wie Kontakte ohne Telefonnummer verschlüsselt auf den Signal-Servern ablegen, um sie auf einem anderen Smartphone wiederherzustellen. Die Einstellungen für die Signal-PIN findet man in der Sektion *Datenschutz*.

   Ein Blog-Artikel[24] erläutert die Voodoo Magie, wie aus einer einfachen, numerischen PIN ein starker Schlüssel für die Verschlüsselung abgeleitet wird. Man kann beim Festlegen der PIN aber auch eine alphanumerisches Passphrase als PIN wählen.

   Die Erinnerungsfunktion soll helfen, die PIN auswendig zu lernen. Wenn man die PIN in einem Passwortspeicher wie KeepassXC ablegt, braucht man es nicht. In den Einstellungen in der Sektion *Erweitert* kann man die PIN wieder deaktivieren.

3. Außerdem kann eine Registrierungssperre für die Übernahme des Accounts auf ein anderes Smartphone aktiviert werden, wenn eine PIN aktiviert wurde. Nach Ansicht der Entwickler reicht eine Sperrung für 7 Tage aus, um alle Kontakte zu informieren.

4. Ein vollständiges Backup inklusive aller Chatinhalte kann man unter Android nur lokal auf einer SD-Karte speichern und auf ein neues Smartphone übertragen.

Für **hohe Sicherheitsanforderungen** bietet Signal App einige zusätzliche Optionen in der Sektion *Datenschutz* in den Einstellungen:

- Die *Bildschirmsperre bei Inaktivität* kann dagegen schützen, dass ein Angreifer bei kurzzeitigem Zugriff auf das entsperrte Smartphone eine Signal-Desktop-Instanz initialisiert, um die Kommunikation mitzulesen. (Das BKA hat einen vergleichbaren Angriff bei WhatsApp gegen einen Terrorverdächtigen bereits aktiv eingesetzt.)

- Die Anrufe (Audio und Video) können immer über einen Signal-Proxy geleitet werden, um dem Kommunikationspartner nicht die eigene IP-Adresse zu verraten.

- Die Anzeige der Signal-Anrufe in der Call History kann abgeschaltet werden, damit die Metadaten dieser Anrufe nicht in der Cloud von Google landen.

Auf Android Smartphones kann man Signal App auch **Google-frei** nutzen. Auf der Signal-Webseite[25] gibt es die Signal-App *Danger Zone* zum Download, die keine Google-Services verwendet. Die Entwickler schreiben, dass man diese Version nur gaaanz besonderen Sonderfällen benötigt - aber das sind eigentlich alle, die die Datenübertragung an Google minimieren wollen. Diese Version von Signal funktioniert auch problemlos auf Google-freien Smartphones ohne GApps und ohne FCM Push Services, da sie den Pushservice von Signal verwendet.

Um bei dieser App Probleme mit Benachrichtigungen bei neuen Nachrichten oder eingehenden Anrufen zu vermeiden, müssen folgende Voraussetzungen erfüllt sein:

1. Man muss *Hintergrundaktivität* und *Hintergrunddatenverkehr* für Signal erlauben.

[24] https://signal.org/blog/secure-value-recovery/
[25] https://signal.org/android/apk/

2. Die App darf nicht durch Stromsparmaßnahmen abgeschossen werden. Bei einigen Smartphones muss man die Option *für Akku-Betrieb nicht einschränken* aktivieren.
3. Ein Support Artikel erläutert die Einstellungen für verschiedene Smartphones.[26]

Signal App verwendet keine eigenen Server für die Infrastruktur, sondern die Clouds von Microsoft, Google, Amazon und Cloudflare. Die Software nutzt Features wie Azure Confidential Computing oder SGI Secure Enclave, um die sensiblen Daten gegenüber dem Cloud-Provider zu schützen.

Signal Desktop

Um Signal als Messenger zu verwenden, benötigt man zwingend ein Smartphone, auf dem man die Signal-App installiert und seinen Hauptaccount mit der Telefonnummer registriert. Auf bis zu fünf Desktop-PCs oder Laptops können zusätzliche Clients eingerichtet werden, die mit allen Funktionen parallel zum Smartphone genutzt werden können.

- Für *Windows* gibt es auf der Download-Seite[27] eine EXE-Datei, die man nach dem Download startet, um die Anwendung Signal Desktop zu installieren.
- Für *Debian*-basierte Linux-Systeme steht ein Repository zur Verfügung, welches man zur Installation und Aktualisierung verwenden kann. Eine Anleitung zur Einbindung des Repositories gibt es auf der Webseite von Signal.[28]
- Für *Ubuntu* und abgeleitet Derivate gibt es ein Snap-Paket, das neben Signal-Desktop auch alle notwendigen Bibliotheken enthält. Da der Snap Daemon in Ubuntu(s) standardmäßig installiert wird, ist es die einfachste Variante, Signal Desktop zu installieren:

  ```
  > sudo snap install signal-desktop
  ```

- *Fedora, Linux Mint* und andere Linux Distributionen sind für die Installation von Flatpak Apps vorbereitet. Hier kann man Signal Desktop via Flathub installieren:

  ```
  > flatpak install org.signal.Signal
  ```

  Wenn man auf dem Desktop nicht alle Features von Signal möchte (beispw. weil man für Audio- oder Videotelefonate immer das Smartphone nutzt) kann man die Rechte der Signal Desktop App mit dem Tool *flatseal* weiter einschränken und die Sicherheit erhöhen.

im ersten Start von Signal-Desktop zeigt das Hauptfenster einen QR-Code, den man mit der Signal App auf dem Smartphone unter *Einstellungen* → *Gekoppelte Geräte* scannen muss, um den Desktop-Client mit seinem Account zu verbinden. Die Daten werden lokal gespeichert, so das die Aktivierung nur einmalig nötig ist. Das ist einerseits bequem, andererseits gibt es einem potentiellen Angreifer aber auch mehr Möglichkeiten.

Anschließend gibt man dem Desktop noch einen Namen. Unter diesem Namen wird die Desktop App in der Liste der *Gekoppelte Geräte* auf dem Smartphone angezeigt.

Dann kann man Signal parallel auf dem Desktop und dem Smartphone nutzen. Aus Sicherheitsgründen werden die bisher auf dem Smartphone vorhandenen Chats nicht mit neu gekoppelten Geräten synchronisiert.

[26] https://support.signal.org/hc/de/articles/360007318711-Problembehebung-bei-Benachrichtigungen
[27] https://signal.org/de/download/
[28] https://signal.org/de/download/

Als erstes könnte man an als Funktionstest sich selbst eine kleine Nachricht schicken. Diesen Chat mit dem Selbstgespräch kann man nutzen, um Daten zwischen unterschiedlichen Geräten auszutauschen. Das ist besser, als sich selbst E-Mails zu schicken, da man von der sicheren Ende-zu-Ende Verschlüsselung profitiert.

Abbildung 11.6: Hauptfenster von Signal Desktop

Wenn man den Signal-Account nicht mehr auf dem Desktop-PC oder Laptop verwenden möchte, sollte man unbedingt alle auf der Festplatte gespeicherten Daten löschen. Signal Desktop bietet in den Einstellungen mit einem Button die Möglichkeit, diese Daten sicher zu entfernen.

11.1.3 Messenger Telegram

Telegram bietet viele Social Features und ist als *zensurresistente Twitter-Alternative* populär geworden (z. B. bei Protesten in Hongkong und Belarus 2020). Für vertrauliche Kommunikation ist Telegram eher weniger geeignet als Signal App oder Threema, aber für den kleinen Hausgebrauch ist es besser als WhatsApp, wenn man einige Hinweise beachtet.

Im deutschen Mainstreams werden oft zwei unterschiedliche Varianten von Telegram beschrieben, die schwer zu unterscheiden sind. Das gute Telegram steht nur in Diktaturen wie Belarus, Iran o. ä. für Oppositionelle zur Verfügung, um regierungskritischen Protest zu artikulieren. In Deutschland gibt es leider nur das böse Telegram, dass von Regierungskritikern verwendet wird, um...

Telegram ist kostenlos nutzbar. Entwicklung und Betrieb werden aus dem Vermögen von Pavel Durov finanziert. Aber das Vermögen von P. Durov ist nicht unendlich und Telegram versucht, mit Premium-Features eigene Einnahmen zu erwirtschaften, um die Unabhängigkeit zu sichern.

Die **Registrierung** erfordert ein Smartphone und eine Telefonnummer, die eine SMS empfangen kann. Diese Telefonnummer wird zur Account-ID! Es muss nicht die Telefonnummer des Smartphones sein. Aber es sollte eine Nummer sein, die man selbst kontrolliert.

Bei fragment.com kann man eine +888-...-Telefonnummer als Telegram-ID kaufen und mit der Kryptowährung TONS bezahlen. Besonders einprägsame Nummern werden versteigert. Eine zufällige +888-...-Nummer bekommt man für 9 TONS.[29]

[29] https://fragment.com/number/random

Abbildung 11.7: Deaktivierung des Uploads der Kontakte in Telegram

Die versprochene Anonymität der +888-. . . -Nummern sollte man nicht überbewerten. Sie gilt nicht gegenüber dem Betreiber, da Telegram auch die IP-Adressen während der Nutzung speichert (und an Behörden weitergibt). Außerdem müsste man für starke Anonymität alle Transaktionen in der Kryptowährung TONS anonymisiert durchführen.

Nach der Registrierung kann man einen **pseudonymen Benutzernamen** festlegen und außerdem die **Anzeige der eigenen Telefonnummer** beim Gegenüber verbieten.

Man kann das Pseudonym statt der Telefonnummer an Chatpartner weitergegeben. Das schützt vor Stalking (beim Casual Dating o. Ä.), aber es bietet im Gegensatz zu Threema keine Anonymität gegenüber dem Betreiber oder Schutz vor staatlicher Repression. Die Zuordnung des Pseudonyms zum Account bzw. zur Telefonnummer wird auf Telegram-Servern gespeichert. Da Telegram bei Terrorismusverdacht mit Behörden kooperiert, ist ein Pseudonym kein Sicherheitsfeature für Aktivisten, die mit staatlicher Verfolgung rechnen.

> *If Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities.*

Es gibt allerdings eine Möglichkeit, die Telefonnummer zu ermitteln. Wenn ein Angreifer eine Vermutung hat, zu welcher Gruppe von Personen ein Pseudonym gehört, könnte er bis zu 1.000 Telefonnummern in sein Adressbuch eingeben. Wenn die Telefonnummer im Adressbuch steht, wird sie auch in Chats unter dem Benutzernamen angezeigt und über die Adressbuch-API könnte ein Angreifer dann den Namen herausfinden.

Den Zugriff auf das **Adressbuch** kann in den Einstellungen unter *Privatsphäre und Sicherheit* deaktiviert werden und ist DRINGEND empfehlenswert.

Wenn man den Zugriff auf das Adressbuch erlaubt, werden zusammen mit der Telefonnummer auch die Namen aus dem Adressbuch auf die Telegram-Server hochgeladen. Über eine API können Dritte diese Informationen abfragen und es könnte evtl. peinlich sein, wenn Dritte erfahren, dass man unter der Bezeichnung *Schnuckelchen* gespeichert wurde. A. Navalny hat diese Funktion im Dezember 2020 in einem Interview demonstriert. Er hat die Telefonnummer eines Co-Travellers bei einem Telegram-Bot eingegeben und als Antwort wurde u. a. *FSB Vladimir Alexandrovich Panyaev* angezeigt – echt peinlich.

Eine inverse Suche nach Telefonnummern, um den Inhaber einer Nummer zu ermitteln, ist auch in Telefonbüchern möglich. Allerdings findet man dort nur Personen bzw. Firmen, die gefunden werden möchten. Gegen die inverse Suche bei Telegram gibt es wenig Schutz und es betrifft nicht nur Telegram-Nutzer sondern alle, die ein Telefon oder Smartphone benutzen und einen Telegram-Nutzer kennen, der sein Adressbuch hochgeladen hat.

Nach der Registrierung sollte man die **zweistufige Bestätigung** für das Hinzufügen neuer Geräte aktivieren. Damit verhindert man (staatliche) Angriffe, welche die Multi-Device-Unterstützung exploiten. Die zweistufige Registrierung aktiviert man in den Einstellungen unter *Privatsphäre und Sicherheit*. Es wird ein zusätzliches Passwort für die Registrierung von Desktop-Clients für den Account festgelegt. Dieses Passwort sollte man nicht verlieren, da man irgendwann das Smartphone wechseln wird. (Man könnte es in einem verschlüsselten Passwortspeicher wie KeepassXC speichern.)

Abbildung 11.8: Zweistufige Bestätigung für neue Geräte aktivieren

Das Einrichten eines **Backups** wie bei Threema entfällt, da Telegram als Cloud-Messenger arbeitet. Die Nachrichten liegen auf den Telegram-Servern (und der Betreiber hat Zugriff auf die Chats). In den FAQ begründet Telegram diese Design-Entscheidung. Als Nutzergruppe wird der Massenmarkt anvisiert und diesen Nutzern muss man die Möglichkeit geben, bei Verlust oder Wechsel des Smartphones die Chat-Daten wiederherzustellen. Ein (möglicherweise unverschlüsseltes) Backup in der Google-Cloud oder iCloud wie bei WhatsApp bis 2018 war für Telegram keine Option. Daher hat sich Telegram selbst als Cloud und Live-Backup als hinreichend vertrauenswürdig definiert.

Ende-zu-Ende-Verschlüsselung kann für 1:1-Chats aktiviert werden (nicht für Gruppenchats). Um einen geheimen Chat zu starten, öffnet man den Kontakt, tippt auf den Button *Mehr...* und anschließend auf *Geheimen Chat starten*.

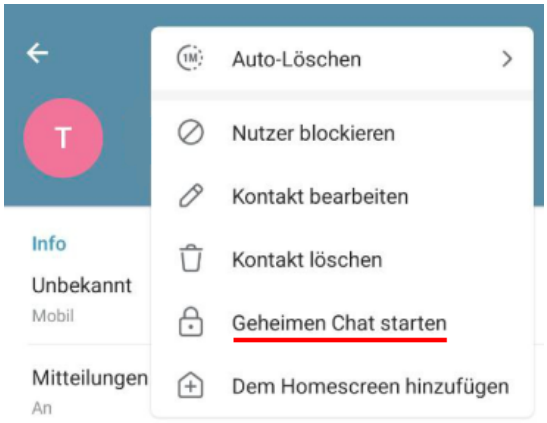


Abbildung 11.9: Geheimen Chat aktivieren

Diese *geheimen Chats* werden nicht in der Cloud gespeichert, sondern auf dem Smartphone. Im Gegensatz zu Threema oder Signal werden die geheimen Chats auf dem Smartphone aber unverschlüsselt(!) abgelegt. Dieses Verhalten ist als *Mannings Bug* bekannt, da ein Angreifer mit physischem Zugriff auf das Smartphone die *geheimen Chats* auslesen kann. Elcomsoft oder Cellbrite liefern die nötigen Tools.

In einigen Blogs wird behauptet, das Telegram eine selbst entwickelte Krypto einsetzen würde. Das ist Bullshit. Telegram verwendet RSA2048, SHA256 und AES-IGE. Der Countermode IGE für AES ist keine Erfindung von Telegram, sondern seit 2006 in der kryptografischen Literatur beschrieben. AES-IGE wurde entwickelt, um Schwächen von AES-CBC auszubügeln. Das gesamte Verschlüsselungsprotokoll MTProto 2.0 von Telegram wurde analysiert und für gut befunden.[30]

Audio- und Videotelefonie in 1:1-Chats ist immer Ende-zu-Ende-verschlüsselt. Auch dabei kommt MTProto 2.0 zum Einsatz. Zur Verifizierung der Verschlüsselung werden oben rechts vier Emojis angezeigt. Wenn beide Seiten die gleichen Emojis sehen, ist die Verschlüsselung sicher.

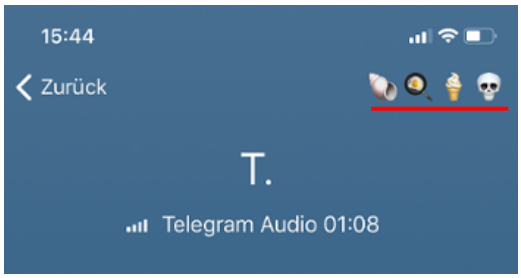


Abbildung 11.10: Verifizierung der Verschlüsselung für Audio- und Videotelefonie

Um in Android 14+ verschlüsselte Anrufe so einfach annehmen zu können wie normale Telefonanrufe, muss man Vollbildbenachrichtigungen auf dem Sperrbildschirm zulassen. In den Android Einstellungen findet man die Option unter *Apps* → *Telegram* → *Benachrichtigungen*.

Telegram-Gruppen können bis zu 200.000 Mitglieder enthalten. Teilnehmer mit Admin-Status können mit einem Klick eine Telefonkonferenz mit den Gruppenteilnehmern starten und kontrollieren, wer sprechen darf. Teilnehmer können mit einem Handzeichen auf sich aufmerksam machen.

Es gibt keine Ende-zu-Ende-Verschlüsselung für Telegram-Gruppenchats. Trotzdem ist das Mitlesen für externe Dritte ohne Unterstützung des Betreibers nicht trivial, wie die Versuche des BKA bei der Infiltrierung rechtsextremer Gruppenchats zeigen.

Wenn man den Zugriff auf das Adressbuch für Telegram blockiert hat, muss man Bekannte zuerst zur Telegram-Kontaktliste hinzufügen, bevor man sie in eine Gruppe einladen kann.

Telegram-Kanäle sind eines der besonderen Social-Media-Features des Messengers. Man kann diese Kanäle nutzen, um einem breiten Publikum seine Meinung vorzustellen oder bei Protesten Millionen Follower ohne eine Beschränkung auf 200 Zeichen zu informieren.

Kanäle können neben Text, Bildern und Videos auch Audiostreaming senden, so dass man einen Radiokanal oder Live-Talks ähnlich wie bei der Clubhouse-App anbieten kann. Die Audiostreams können aufgezeichnet werden. Im Unterschied zu Gruppen bleiben die passiven Teilnehmer (Leser bzw. Zuhörer) in einem Kanal anonym. Man kann nicht sehen, wer einem Kanal folgt. Nur die Anzahl der Follower wird angezeigt.

[30] https://arxiv.org/pdf/2012.03141

- In Russland werden auf diesem Weg immer wieder Informationen über Korruption in unterschiedlichen Behörden publiziert.
- 2020 wurden diese Kanäle bei den Protesten in Hongkong gegen China und in Weißrussland gegen den Wahlbetrug genutzt, um Millionen Anhänger zu mobilisieren.
- In Deutschland bieten viele Online-Medien einen Telegram-Kanal, um Hinweise auf neue Artikel zu posten. Telegram bietet sich somit als News-Aggregator an, der schnell und übersichtlich über Neuigkeiten informiert, ähnlich wie RSS-Feeds früher.

  Hinweis: Die in den Kanälen geposteten Links zu den vollständigen Artikeln enthalten häufig Tracking-Parameter in den URLs. Man sollte den Browser zum Öffnen der Links also datenschutzfreundlich konfigurieren, um die Tracking-Parameter zu entfernen.

Für die steigende Verbreitung der Telegram-Kanäle als Social-Media-Tool zur Mobilisierung von (mehr oder weniger großen) Massen gibt es mehrere Gründe. Telegram wird von Millionen Menschen bereits für die tägliche Kommunikation genutzt und sie sind mit dem Tool vertraut.

Sperrungen/Zensur bei Kanälen, Bots und Gruppen gibt es auch bei Telegram. Der Dienst gilt allgemein als zensur-resistent und ist staatlich schwer kontrollierbar. Er ist aber kein rechtsfreier Raum. Kanäle, Bots und Gruppen werden auf zwei Ebenen zensiert, gelöscht oder gesperrt.

1. Telegram sperrt jeden Monat 15.000 - 20.000 Kanäle und Bots, die dem Telegram-Abuse gemeldet werden und eindeutig als Terror- und Hasspropaganda, Kinderpornografie, Spam oder gefakte Userkennungen eingeordnet werden können.

   Im Januar 2021 wurden beispielsweise 19.672 Kanäle und Bots gesperrt, im Dezember 2021 waren es 23.082. Zahlen über gesperrte Kanäle werden vom *isiswatch bot* publiziert.[31]

   Europol vertritt die Einschätzung (2018), dass Telegram sich erfolgreich bemüht, Terror- und Hasspropaganda sowie Aufrufe zu Straftaten zu entfernen:[32]

   Wenn man (zufällig) illegale Inhalte findet, kann man sie mit wenigen Klicks an das Telegram Abuse Team melden. Im Menü oben rechts im Kanal tippt man auf *melden* und kann danach angeben, warum man den Kanal (oder Bot) meldet.

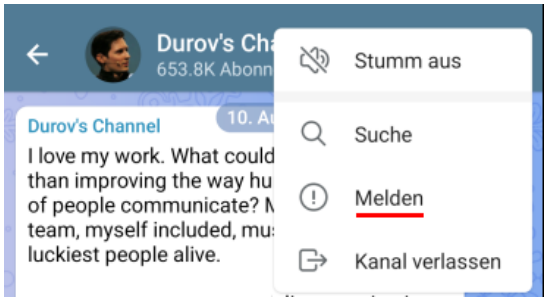


Abbildung 11.11: Illegale Inhalte bei Telegram melden

2. Google und Apple haben bei den Telegram-Apps, die aus dem Play-Store oder App-Store heruntergeladen werden, weitere Möglichkeiten, Kanäle oder Gruppen zu zensieren und machen auch davon Gebrauch. Apple ist z. B. ein bisschen prüde, und sperrt auf den iPhones alles, was pornografisch ist:

[31] https://t.me/s/isiswatch
[32] https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online

Außerdem werden von Google und Apple Telegram-Kanäle und -Gruppen in den Smartphone-Apps gesperrt, die als Fake-News o. Ä. klassifiziert, aber von Telegram als freie Meinungsäußerung eingestuft und nicht gelöscht werden.

Um diese Sperren in den Smartphone Apps zu umgehen, gibt es Möglichkeiten:

- Für Android-Phones gibt es Telegram[33] im F-Droid-Store und auf der Telegram-Webseite ein APK[34] zum Download, in denen Google nichts zensieren kann.
- Außerdem könnte man sich auf dem PC oder Laptop Telegram-Desktop installieren. Dort können Google und Apple ebenfalls nichts zensieren.[35]
- Kanäle kann man auch im Browser lesen: https://t.me/s/<Kanalname>.

3. Staatliche Zensur ist bei Telegram ebenfalls möglich. Dabei kooperiert Telegram mit den Behörden des Landes und sperrt auf deren Wunsch Kanäle, die lokale Gesetze des Landes verletzten, für die Nutzer mit einer Telefonnummer, die mit der jeweiligen Landeskennung beginnt. Diese Sperrungen sind seit Februar 2022 für Nutzer mit Telefonnummern +49-. . . in Deutschland für einige Kanäle des veganen Kochs aktiv und können nicht mit Telegram Desktop, Telegram FOSS oder VPNs umgangen werden.

   Als Grund für die Sperrung der Kanäle wurden Morddrohungen genannt. Ok – jeder weiß, wer der vegane Koch ist und wo er sich aufhält. Wenn er für seine Straftaten nicht zur Verantwortung gezogen wird, ist nicht Telegram dafür verantwortlich . . . (Schamhaftes Verstecken der Straftat durch Zensur ist ein Eingeständnis der Schwäche und Unfähigkeit des Rechtsstaates bei der Durchsetzung von Recht.)

   Seit 04. März 2022 sperrt Telegram die Kanäle von russischen Nachrichtenmedien für Nutzer mit Telefonnummern aus der EU aufgrund einer Verordnung der EU.

   Die juristischen Grundlagen für diese Verordnung, die Provider zur Zensur ausländischer Medien zwingt, sind zumindest fragwürdig (nach Meinung von Juristen). Ohne Diskussion im Parlament werden Grundrechte der EU-Menschenrechtscharta und des Grundgesetzes außer Kraft gesetzt, die einen unzensierten Zugang zu Informationen garantieren sollten.

4. Vollständige Blockade von Telegram gibt es bisher nur in echten Diktaturen wie Iran, Saudi-Arabien oder China. Unsere Bundesinnenministerin spielt ebenfalls mit dem Gedanken, Telegram staatlich zu blockieren, was die Reichweite des Messengers fraglos etwas einschränken könnte, aber aus mehreren Gründen eine blödsinnige Idee ist:

   - Man löst gesellschaftlich-soziale Probleme nicht mit Sperrung eines Messengers.
   - Deutschland und andere EU-Staaten haben technisch nicht die Möglichkeiten, Telegram zu blockieren. Die Technik dafür werden die ISPs nicht installieren.

   Um eine Blockade von Telegram auf Netzwerkebene zu umgehen, kann man ein paar Euro für einen VPN-Provider investieren oder man nutzt die in Telegram eingebaute Anti-Zensur-Technik MTProxy bzw. SOCKS Proxy. Die Proxys aktiviert man in den Einstellungen unter

[33] https://f-droid.org/de/packages/org.telegram.messenger
[34] https://telegram.org/android
[35] https://desktop.telegram.org/

Daten und Speicher → *Proxy*. Eine Liste von MTProxys kann man z. B. im Telegram-Kanal MTProtoProxies[36] finden, den man auch im Browser öffnen kann.

RSS-Feeds sind ein Relikt aus der Bronzezeit des Internet, aber immer noch praktisch. Man muss nicht ständig die vielen Blogs abklappern, für die man sich interessiert, sondern abonniert die RSS-Feeds der Blogs und wird bei Veröffentlichungen benachrichtigt.

Es gibt mehrere Möglichkeiten, RSS-Feeds in Telegram zu verarbeiten. Die einfachste Methode zum Lesen von RSS-Feeds ist, den *Feed Reader Bot*[37] zu verwenden, der in der Bedienung sehr einfach ist. Bei kostenloser Nutzung werden die Feeds alle 3 Stunden aktualisiert, für Premium-Nutzer alle 20 min und bei Elite-Nutzern noch öfter.

Telegram Nearby ist ein Social-Feature, das man eher bei Dating-Apps wie Tinder vermuten würde. Man kann unter *Kontakte* → *Leute in der Nähe finden* nach Personen und lokalen Gruppen suchen, die ihren Standort für diese Funktion freigegeben haben. (In den naheliegenden Gruppen bieten fliegende Händler oft Drogen an und bei den Leuten in der Nähe gehört ein erheblicher Teil zum horizontalen Gewerbe (mein Eindruck aus Berlin).)

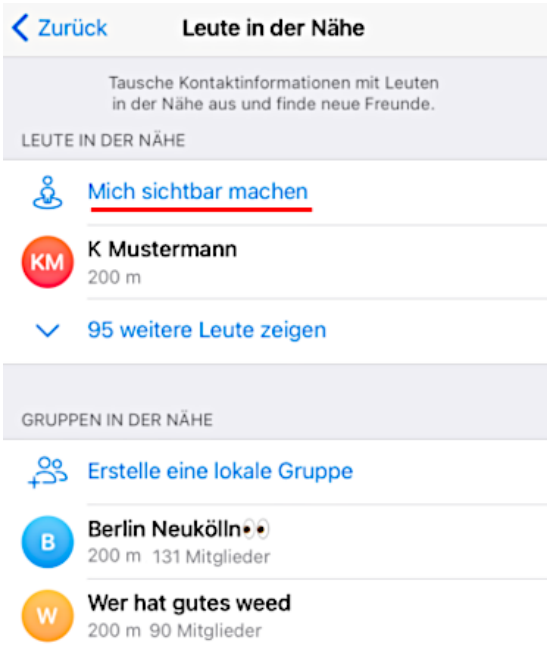


Abbildung 11.12: Personen und Gruppen in der Umgebung suchen

Wenn man selbst seinen Standort für die Leute in der Nähe freigibt, dann können Leute in der Umgebung auch den Standort ermitteln. Telegram zeigt nur die Entfernung an, aber mittels Triangulation (ein paar Meter nach rechts und nach links gehen) kann man den Standort interpolieren. Für Heise ist das ein Security-Bug,[38] aber Telegram kommentierte:

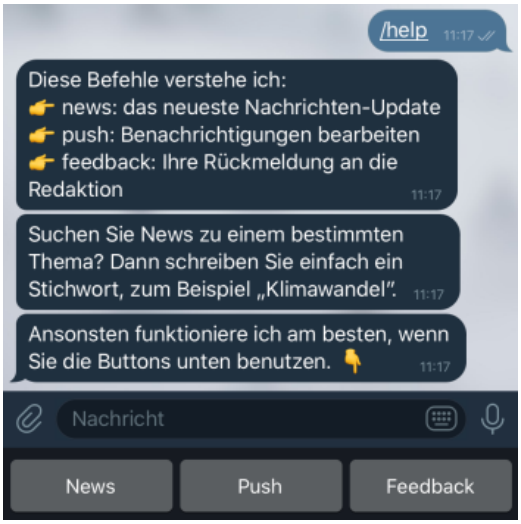
> *People in the Nearby section intentionally share their location, this feature is disabled by default. It's expected that determining the exact location is possible under certain conditions.*

[36] https://t.me/s/MTProtoProxies
[37] https://t.me/TheFeedReaderBot
[38] https://heise.de/-5004687

Telegram-Bots sind ein weiteres populäres Feature des Messengers. Ein Bot ist ein Chatpartner, der auf simple Kommandos reagieren kann oder automatisiert Informationen liefert. Es ist keine grandiose, neue Erfindung, das gab es schon im letzten Jahrhundert bei IRC, aber aktuell sind Bots vor allem bei Telegram wieder populär geworden.

Ein einfaches, simples Beispiel ist der News-Bot der ARD-Tagesschau:

1. Einen Bot findet man über die Suche nach Kontakten in der Telegram-App oder als Link auf Webseiten und startet einen Chat wie mit anderen Chatpartnern.
2. */start* ist das erste Kommando, das jeder Bot kennt und bei Beginn des Chats ausführt. Es zeigt meist eine kurze Einführung und am unteren Rand ein paar Buttons für weitere Kommandos für die nächsten Schritte.
3. */help* ist ein weiteres Kommando, das jeder Bot kennen muss und das man ihm immer schicken kann, wenn man nicht weiter weiß.



Dieser einfache Bot versteht also die Kommandos */news, /push* und */feedback*.

Der Bot der ARD-Tagesschau ist ein sehr einfaches Beispiel. Es gibt wesentlich ausgefeiltere Bots, die komplette Shopsysteme emulieren, inklusive Auswahl aus den Angeboten, Bewertung der Verkäufer, Bezahlung usw. In diesen Shops kann man auch Dinge finden, die nach dem Betäubungsmittelgesetz illegal sind, gefälschte Dokumente oder Waffen. Man muss nur lange genug suchen und darf natürlich nicht auf Fakes hereinfallen. Es bildet sich ein neues Darknet, ähnlich wie bei den illegalen Marktplätzen auf Tor-Onion-Services, welches allerdings auch zukünftig von der Policy der Telegram-Betreiber abhängig ist.

Die Sicherheit illegaler Handelsplätze für Drogen oder Waffen ist bei Telegram wesentlich geringer als im Darknet (bspw. Tor-Onion-Services), da ein zentraler Ansprechpartner als Betreiber existiert, der unter Umständen auch mit der Strafverfolgung kooperiert. Im Oktober 2020 wurden mehrere Chat-Kanäle der Drogenszene mit mehr als 8.000 Nutzern vom BKA übernommen. Die Chatverläufe konnten analysiert werden, es gab mehrere Festnahmen und das BKA hat eine Informationsseite in den übernommenen Gruppen anzeigen lassen. Der letztere Schritt wäre ohne Kooperation des Betreibers nicht möglich gewesen.

Telegram Passport wurde 2018 als Ende-zu-Ende-verschlüsselter Cloud-Speicher eingeführt. Man kann Dokumente hochladen (Ausweiskopie, Führerschein o. Ä.). Diese Dokumente können

von einem Webdienst angefragt werden und der Nutzer hat die Möglichkeit, die angeforderten Daten mit wenigen Klicks via Telegram zu verschicken. (In Deutschland ist das ein eher unüblicher Vorgang und wird hier wenig genutzt werden.)

Außerdem kann Telegram Passport als Identity Provider für den Login genutzt werden:

11.1.4 Messenger basierend auf [matrix]

[matrix] ist eine moderne Alternative zu Jabber/XMPP. Die Serverkomponenten (Matrix) sind Open Source und es ist der Aufbau einer föderalen Infrastruktur möglich. Jeder Interessierte kann einen eigenen Server betreiben, der mit allen anderen Accounts auf anderen Servern kommunizieren kann. Es gibt mehrere Client-Apps, wobei Element.io die größte Verbreitung hat.

Im F-Droid-Store gibt es eine Google-freie Version von Element.io für Android, die keine Google Services für Push Notifications nutzt. Statt dessen wird ein Hintergrundprozess für die Synchronisation der Nachrichten verwendet, der ein bisschen mehr Energie vom Akku benötigt. In den Einstellungen kann man einen individuellen Kompromiss zwischen Häufigkeit der Aktualisierung und Energieverbrauch konfigurieren.

Nach der Installation einer Client-App kann man einen **Account erstellen**. Den Account kann man auf einem beliebigen Server entsprechend den eigenen Präferenzen frei wählen, unabhängig von der Telefonnummer. Diesen Server nennt man im [matrix]-Jargon den Homeserver. Die meisten [matrix]-Nutzer drängeln sich auf dem Homeserver von matrix.org, aber es gibt gute Alternativen:

- https://nitro.chat/ (von der Nitrokey GmbH)
- https://nope.chat/ (von adminForge.de)
- https://tchncs.de/matrix (von einem Technikkollektiv)
- https://wir.freiburg.social/angebote/matrix/ usw.

Über Identitätsserver kann man den Account auf Wunsch mit einer Telefonnummer oder E-Mail-Adresse verbinden, sodass man leichter gefunden wird. Meistens wird der Server *vector.im* verwendet, der damit eine zentrale Funktion übernimmt.

Die **Räume** sind das zentrale Konzept beim Chatten via [matrix]. Man kann sich auf seinem Homeserver neue *Räume* einrichten und dort erst mal Selbstgespräche führen. Wenn man eine zweite Person in den Raum einlädt und diese Person die Einladung annimmt, kann man chatten, Dateien austauschen oder telefonieren. Wenn man mehrere Personen in den *Raum* einlädt, hat man einen Gruppenchat. Innerhalb des *Raumes* lassen sich sehr detaillierte Rechte vergeben: wer etwas sagen darf, wer administrieren bzw. moderieren darf, wer Dritte einladen darf usw.

Mit den **Spaces** kann man Umgebungen für kollaboratives Arbeiten in Teams oder Communitys definieren. Es gibt offene Spaces, die jeder betreten kann, oder private Spaces, in die man nur mit

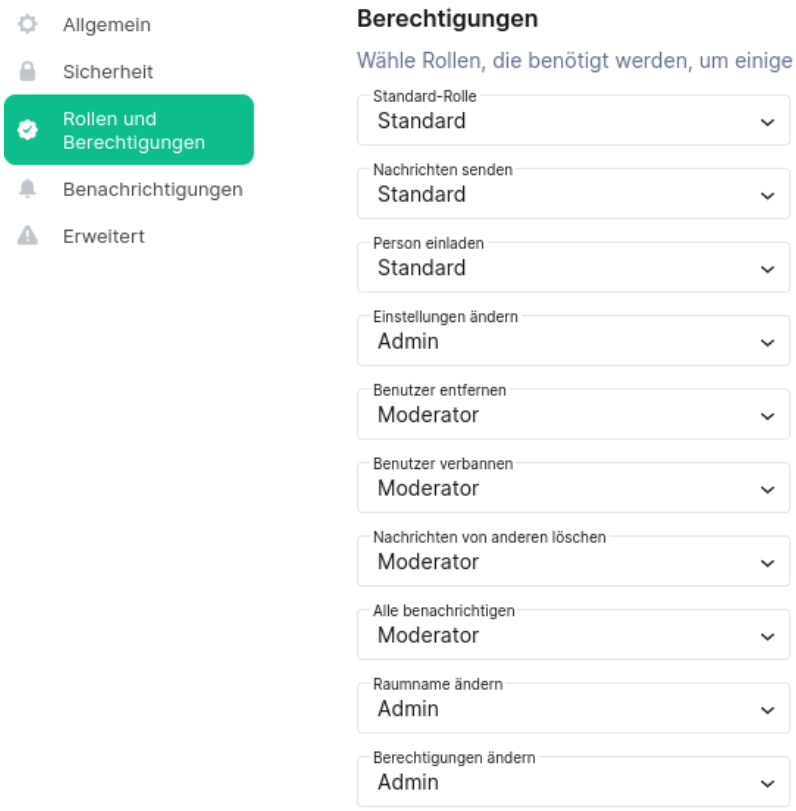


Abbildung 11.13: Detaillierte Einstellungen für Rechte in [matrix]-Räumen

Einladung rein kommt. Innerhalb eines Space können Räume oder Sub-Spaces erstellt werden. Die Berechtigungen in Spaces sind ähnlich detailliert konfigurierbar wie in Räumen.

Konzeptuell ist [matrix] ein **Multi-Cloud-Messenger**. Im Gegensatz zu Threema oder Signal App, die keine Daten auf den Servern speichern, werden bei [matrix] alle Kontaktlisten, Mitgliedschaften in Gruppenchats und persönlichen Informationen auf dem Homeserver gespeichert. Außerdem werden Räume inklusive der Nachrichteninhalte für unbegrenzte Zeit auf allen [matrix]-Servern in Kopie gespeichert, die an der Kommunikation beteiligt sind.

Im Gegensatz zu anderen Messengern wirbt [matrix] nicht damit, dass Nutzer die volle Kontrolle über ihre Kommunikation behalten. Der Vorteil ist laut [matrix]-Werbung:

> *There is no single point of control or failure in a Matrix conversation which spans multiple servers: the act of communication with someone elsewhere in Matrix shares ownership of the conversation equally with them.*

Neben den Techies (Admins der beteiligten Server) und Hackern (April 2019: *Matrix.org chat server hacked, chat history lost*[39]) haben auch Behörden im Rahmen von Auskunftsersuchen darauf Zugriff. Mit Umsetzung des im Dezember 2019 vorgelegten Gesetzentwurfes zur Bekämpfung von Rechtsterrorismus und Hasskriminalität könnte jeder Dorfpolizist ohne richterliche Prüfung die Daten von dem bevorzugten Server abrufen, der sich juristisch in seiner Reichweite befindet. Sollten die Inhalte der Nachrichten Ende-zu-Ende-verschlüsselt sein, können trotzdem detaillierte

[39] https://www.zdnet.com/article/matrix-hack-forces-servers-offline-user-credentials-leaked/

Metadaten der Kommunikation für die Kommunikationsanalyse abgerufen werden (wer mit wem, wie häufig usw.).

Nach der Rechtsprechung des BVerfG unterliegen Nachrichten nicht mehr dem Telekommunikationsgeheimnis nach §10 GG, wenn der Empfänger die Nachricht gelesen hat und die Gelegenheit hatte, sie zu löschen. Auf dem eigenen Homeserver kann man Nachrichten löschen, indem man eine Nachricht antippt und den Menüpunkt *Entfernen* wählt. Der Homeserver wird diesen Löschwunsch auch an alle anderen Server weitergeben, die Kopien der Nachricht gespeichert haben. Die Dokumentation weist man darauf hin, das damit nur ein Wunsch des Nutzers zum Ausdruck gebracht wird. Es kann nicht sichergestellt werden, dass die anderen Server diesen Wunsch auch befolgen.

> *This means that every server[!] has total self-sovereignty over its users data ...*

Open-Source-Enthusiasten argumentieren oft, dass man bei föderalen Systemen problemlos einen eigenen Server aufsetzen kann, wenn man keinen vertrauenswürdigen Server findet. Bei [matrix]/Riot ist dieses Argument falsch. Man muss nicht nur dem eigenen Server vertrauen, sondern auch den Admins aller anderen Server, die an einer Kommunikation beteiligt sind, da alle beteiligten Server eine komplette Kopie der Kommunikation speichern.

Die **Ende-zu-Ende-Verschlüsselung** ist Teil des Sicherheitskonzeptes von [matrix] und standardmäßig aktiviert. Für hohe Sicherheitsansprüche gibt es folgende Optionen:

1. Überprüfung der Kommunikationspartner: Die Verifizierung der Partner soll sicherstellen, dass man wirklich mit dem gewünschten Gegenüber verbunden ist, und erfolgt durch Scannen von QR-Codes bei einem persönlichen Treffen oder mit Emojis, die man über einen getrennten Kommunikationskanal (out-of-band) prüfen muss.

2. Cross-Signing mehrerer Geräte: Wenn man selbst mehrere Geräte verwendet, sollte man das Cross-Signing aktivieren. Dabei werden Signaturschlüssel und Key-Backup auf dem Homeserver abgelegt und mit einem zusätzlichen Passwort verschlüsselt, das sich von dem Account-Passwort unterscheiden sollte. Alternativ kann man den Schlüssel für das Cross-Signing herunterladen und lokal speichern. Die Signaturschlüssel werden verwendet, um eigene, neue Geräte zu signieren und das in die Vertrauensbasis bestehender Verifizierungen einzuschließen.

   Wenn man Cross-Signing aktiviert, müssen verifizierte Kommunikationspartner nicht mehr jedes einzelne Gerät verifizieren. Man entscheidet selbst, welche Geräte vertrauenswürdig sind und verifiziertes Vertrauen wird auf neue Geräte übertragen.

Nach einer Verifizierung der Kommunikationspartner und der eigenen Geräte sollte man zusätzlich die Kommunikation mit nicht-verifizierten Geräten verbieten, damit man sicherheitsmäßig von der Verifizierung profitiert.

Schwächen im Protokoll der Ende-zu-Ende-Verschlüsselung wurden 2022 in dem Paper *Practically-exploitable Cryptographic Vulnerabilities in Matrix*[40] aufgezeigt. Das Paper beschreibt 6 Angriffe, mit denen ein bösartiger Homeserver die Ende-zu-Ende-Verschlüsselung kompromittieren könnte. Er kann zusätzliche Nutzer in E2E-verschlüsselte Räume einfügen oder neue Geräte für einen User registrieren und damit alle E2E-verschlüsselten Chats dieses Nutzers mitlesen, solange der Nutzer das zusätzliche Gerät oder den neuen Teilnehmer im Raum (Gruppenchat) nicht bemerkt. Außerdem könnte ein bösartiger Homeserver Sessions kompromittieren und sich selbst

[40] https://nebuchadnezzar-megolm.github.io/

als Man-in-the-Middle in ausgewählten Räumen platzieren oder sich als vertrauenswürdiges Gerät eines Nutzers ausgeben und ein Backup anfordern, das Zugriff auf alle Daten bietet.

Zusammenfassung: grundsätzliche Anforderungen an eine Ende-zu-Ende-Verschlüsselung werden bei [matrix] nicht erfüllt. Auf den Homeservern sitzt genau der Angreifer (Mallory), gegen den die Ende-zu-Ende-Verschlüsselung eigentlich schützen soll.

Hinsichtlich Sicherheit der **Transportverschlüsselung** (TLS) könnte man noch anmerken, dass Certificate Pinning als Schutzmaßnahme gegen Man-in-the-Middle-Angriffe bei [matrix] aus den gleichen Gründen nicht möglich ist wie bei Jabber/XMPP. Mit einer föderalen Infrastruktur, wo jeder Interessierte Admin einen eigenen Server betreiben kann, ist es unmöglich, diese Sicherheitsempfehlung umzusetzen. Im Gegensatz zu Threema oder Signal App sind [matrix]-Clients damit anfällig für Angriffe, die 2009 in *Certified Lies – Detecting and Defeating Government Interception Attacks against SSL*[41] beschrieben wurden.

Neben den Smartphone-Clients gibt es für [matrix] eine *Browserversion* als Desktop-Client oder für den Einsatz auf einem Webserver. Aufgrund konzeptueller Schwächen kann man bereits ohne Prüfung der finalen Version sagen, das eine Webversion nicht für hohe Sicherheitsansprüche geeignet ist:

- Dass Webserver-basierte Chat-Clients für die Sicherheitsansprüche politischer Aktivisten, Menschenrechtsaktivisten o. Ä. generell nicht geeignet sind, hat Patrick Ball 2012 in einem Essay bei Wired am Beispiel von Cryptocat dargelegt.[42]
- riot-web speichert die privaten kryptografischen Schlüssel für die Ende-zu-Ende-Verschlüsselung im HTML5-Storage des Browsers. Im *HTML5 Security Cheat Sheet*[43] wird vom OWASP empfohlen, keine sensitiven Informationen im HTML5-Storage zu speichern, da es kein sicherer Speicher ist und diese Daten leicht kompromittiert werden könnten, bspw. mit XSS-Angriffen.

  In der Dokumentation wird darauf hingewiesen, dass man das Web-GUI nicht auf dem gleichen Server installieren sollte wie den [matrix]-Server, da ein Angreifer mit XSS-Angriffen die [matrix]-API kompromittieren könnte. Man findet aber keine Warnung dazu, dass auch die privaten Schlüssel für Ende-zu-Ende-Verschlüsselung mit den gleichen Angriffen kompromittiert werden könnten.

11.1.5 Chatten mit Jabber/XMPP

Jabber/XMPP begleitet mich und andere Nerds seit vielen Jahren. Die Software ist Open Source und ein kooperatives, weltweites Netz von tausenden Servern wird von Enthusiasten betrieben. Bei Jabber/XMPP lebt noch der Geist des frühen Internet.

Übergriffe auf die Privatsphäre durch Datendiebstahl (z. B. von Adressbüchern) hat es bei Jabber/XMPP nie gegeben und der Account kann frei gewählt werden, unabhängig von Telefonnummern.

Neben 1:1-Chats gibt es bei Jabber/XMPP spezielle Konferenzräume als Gruppenchats und der Austausch von Bildern und Dateien ist mit allen Clients möglich. Audio- und Videotelefonie ist grundsätzlich als Feature definiert, wird aber nicht von allen Jabber/XMPP-Clients implementiert.

Bei der Ende-zu-Ende-Verschlüsselung gibt es mehrere Alternativen:

[41] https://crypto.stanford.edu/cs155old/cs155-spring11/papers/ssl-mitm.pdf
[42] http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/
[43] https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html

1. Off-the-Record (OTR) wurde 2001 mit dem Ziel entwickelt, möglichst einfach einsetzbar zu sein. OTR ist nicht Multi-Device-fähig und verschlüsselt nur direkte Chats. Gruppenchats und Dateitransfer werden nicht verschlüsselt.

2. OpenPGP wurde bereits im Kapitel E-Mails verschlüsseln behandelt. Die Erstellung und der Austausch der Schlüssel ist etwas komplizierter als bei OTR und OMEMO. Die Vertrauenswürdigkeit der Verschlüsselung muss aber nicht extra verifiziert werden, da sie durch das Vertrauen in die OpenPGP-Schlüssel gegeben ist. OpenPGP verschlüsselt ebenfalls nur direkte Chats.

   Bei OpenPGP gibt es zwei Standards. Die meisten Jabber-Clients implementieren XEP-0027, der inzwischen für obsolet erklärt wurde, da er einige Sicherheitslücken enthält. Der neuer XEP-0373 ist bisher noch als experimentell gekennzeichnet und wird nur von sehr wenigen Jabber-Clients unterstützt.

3. OMEMO (OMEMO Multi-End Message and Object Encryption, XEP-384) ist eine relativ neue Ende-zu-Ende-Verschlüsselung für Jabber/XMPP. Sie basiert auf Axolotl Ratchet, das von WhisperSystems für Signal App entwickelt wurde. Sie bietet wie OTR einen automatischen Schlüsseltausch, Forward Secrecy und Deniability. Zusätzlich bietet OMEMO verschlüsselte Offline-Messages und verschlüsselten Dateitransfer via HTTP-Upload. Mit XEP-391 gibt es einen Standard für den verschlüsselten Jingle-Dateitransfer, der bisher aber nur von wenigen Clients umgesetzt wird.

Im Vergleich zu den im Punkt Sicherheit führenden Messengern hinkt Jabber/XMPP bei der Umsetzung moderner Sicherheitsfeatures hinterher. Die Ursachen dafür liegen in der föderalen Serverstruktur und der Community-basierten Entwicklung. Gerade diese beiden Punkte sind für Open-Source-Dogmatiker die Pluspunkte von Jabber/XMPP und werden vehement verteidigt, ohne dass die Nachteile bezüglich Sicherheit erwähnt werden.

Einige Beispiele für kryptografische Schwächen bei Jabber/XMPP:

1. Certificate Pinning für die TLS-Transportverschlüsselung zwischen Apps und Servern ist seit Jahren Bestandteil der Sicherheitsempfehlungen für die Entwicklung von Smartphone-Apps, um Angriffe auf die TLS-Verschlüsslung zu verhindern, die bereits 2009 in der wissenschaftlichen Arbeit *Certified Lies – Detecting and Defeating Government Interception Attacks against SSL*[44] beschrieben wurden.

   Bei Jabber/XMPP ist es aufgrund der föderalen Infrastruktur nicht möglich, Certificate Pinning einzuführen. Im Gegensatz zur Threema oder Signal ist Jabber/XMPP damit weiterhin anfällig für Man-in-the-Middle-Angriffe auf die TLS-Verschlüsselung mit gefakten TLS-Zertifikaten. (Einige Jabber-Clients wie ChatSecure oder CoyIM speichern die zuletzt verwendeten SSL-Zertifikate der Server und warnen bei unerwarteten Änderungen, um diese Schwäche teilweise zu kompensieren. Die Warnungen muss man allerdings verstehen und nicht einfach ohne Nachdenken auf Ok klicken.)

   Diese Schwäche hat es einem (vermutlich) staatlichem Angreifer 2023 ermöglicht, monatelang den TLS-verschlüsselten Traffic der Jabber Server jabber.ru und xmpp.ru als man-in-the-middle abzuhören. Die Abhörtechnik wurde in den Rechenzentren von Hetzner und Linode installiert (wo die beiden russischen Jabber/XMPP Server gehostet werden) und nutzte ein falsches TLS-Zertifikat, welches von Let's Encrypt ausgestellt war.[45]

   Threema und Signal App nutzen CA-Pinning, um diese Angriffe zu verhindern.

[44] https://crypto.stanford.edu/cs155old/cs155-spring11/papers/ssl-mitm.pdf
[45] https://notes.valdikss.org.ru/jabber.ru-mitm/

2. Alle Kontaktlisten, Mitgliedschaften in Gruppenchats und persönliche Informationen wie Profilfotos u. Ä. (VCards) werden bei Jabber/XMPP unverschlüsselt auf den Servern gespeichert, damit man von unterschiedlichen Geräten mit unterschiedlichen Clients darauf zugreifen kann (siehe: RFC 6121). Neben den Techies (Admins der Server) haben auch Behörden darauf Zugriff.

   Bei Threema und Signal App werden diese Daten ausschließlich auf den Clients gespeichert. Die Serverbetreiber haben keine Informationen über Kontaktlisten, Mitgliedschaften in Gruppenchats, Profilfotos o. Ä. Das schränkt aber zugunsten der Sicherheit die Flexibilität bei der Verwendung unterschiedlicher Geräte ein.

3. Signal App und Threema haben ein Sicherheitskonzept, bei dem die Ende-zu-Ende-Verschlüsselung der gesamten Kommunikation inkl. Audio- und Videotelefonie sowie von Gruppenchats fester Bestandteil und durch Audits bestätigt ist.

   Bei Jabber/XMPP sind bisher alle Versuche einer Ende-zu-Ende-Verschlüsselung unvollständig und können nicht sicherstellen, dass die gesamte Kommunikation zwischen zwei oder mehreren Partnern sicher verschlüsselt wird.

   - Teilweise werden XEPs zur Verschlüsselung durch die Community-basierte Entwicklung nur langsam umgesetzt und es dauert mehrere Jahre, bis man davon ausgehen kann, dass sie von einer Mehrheit der Clients unterstützt werden.
   - Die Standards selbst sind teilweise unvollständig und umfassen nicht die Verschlüsselung des gesamten möglichen Datenaustausches zwischen zwei oder mehreren Nutzern, wie beispielsweise auch bei OMEMO (XEP-384). Es gibt bisher keinen Standard, der die Ende-zu-Ende-Verschlüsselung der gesamten Kommunikation bei Jabber/XMPP als Zielstellung definiert hat, da es unübersichtlich viele Erweiterungen gibt.

     (Man kann aber einen reduzierten Jabber-Client bauen, der nur Features bietet, die von einer Ende-zu-Ende-Verschlüsslung unterstützt werden. CoyIM mit OTR ist so ein Beispiel. Mit CoyIM kann man nur chatten, der Austausch von Dateien und Gruppenchats sind möglich. Aber wenn OTR aktiviert wurde, kann man sicher sein, dass alles, was mit CoyIM möglich ist, auch verschlüsselt wird.)
   - Teilweise liegt es auch an mangelnder konzeptueller Vorarbeit. Es wird einfach erst mal irgendwas verschlüsselt – wird schon ok sein. Das Audit von OMEMO bemängelt gleich im ersten Absatz, dass es kein Angreifermodell gibt, gegen das die OMEMO Verschlüsselung schützen soll, und dass keine Anforderungen beschrieben wurden. Damit ist es unmöglich, OMEMO qualifiziert zu auditieren, weil man ohne Zielvorgaben nicht prüfen kann, ob sie erfüllt werden.

4. Das Audit von OMEMO zeigte, das nicht verifizierte Verbindungen anfällig für Man-in-the-Middle-Angriffe sind, die den Multi-Device-Support von OMEMO ausnutzen. Ein Man-in-the-Middle kann ein zusätzliches Gerät im Namen des Opfers registrieren und dann die verschlüsselten Chats mitlesen, ohne dass das Opfer es bemerkt.

   In Auswertung des Audits wurde die Möglichkeit der Verifizierung von Schlüsseln eingeführt, die den Multi-Device Support (ursprünglich ein Killerfeature von OMEMO) wieder einschränkt. (Ob die gegenseitige Verifizierung der Fingerprints der Schlüssel für eine größere Gruppe von Nicht-IT-Nerds praktisch umsetzbar ist?)

   Threema und Signal App sind gegen vergleichbare Angriffe robust, da man ein zusätzliches Gerät für einen Nutzer nur mit physischen Zugriff auf das Smartphone mit dem Hauptaccount des Nutzers hinzufügen kann. Eine gegenseitige Verifizierung der Schlüssel ist möglich, aber wesentlich weniger wichtig.

5. In der Regel speichern Jabber/XMPP auch die Ende-zu-Ende-verschlüsselte Kommunikation unverschlüsselt in den Logs ab. Das ist als *Mannings* Bug bekannt.

   Es ist inzwischen anerkannter Standard, das Ende-zu-Ende-verschlüsselte Kommunikation auch lokal sicher verschlüsselt zu speichern ist.

6. Eine letzte Bemerkung: einige Jabber/XMPP Clients speichern auch die Login-Credentials (Passwörter) unverschlüsselt in den lokalen Konfigurationsdateien ab.

   Unter Linux sollte man die verschlüsselte Speicherung von Passwörtern im GNOME Keyring oder KWallet aktivieren, wenn es konfigurierbar ist.

Angesichts all dieser Mängel sollte man dennoch nicht die Schlussfolgerung ziehen, dass XMPP unbrauchbar sei. Wer Spaß daran hat, kann es weiterhin verwenden, wenn der Sicherheitslevel ausreichend ist. Bei der Diskussion über Alternativen sollte man aber nicht dogmatisch auf Open Source und föderalen Strukturen beharren, ohne die Mängel in der Kryptografie einzugestehen.

11.1.6 Messenger Wire

Wire ist in erster Linie eine gute Kollaborationsplattform für Unternehmen. Das in Berlin arbeitende Entwicklerteam gehört zur Wire Swiss GmbH, die eine Tochterfirma der Wire Group Holdings GmbH in München (DE) ist und die Server der Infrastruktur betreut.

Die Software ist Open Source, Client Apps gibt es für Smartphones und PCs. Accounts kann man ohne Angabe einer Telefonnummer anlegen und dann auf bis zu 8 Geräten mit Smartphones oder PCs unabhängig von der Telefonnummer nutzen. Für die Inhalte der Kommunikation wird mit Proteus eine Ende-zu-Ende-Verschlüsselung verwendet, die standardmäßig aktiv ist.

Neben Messaging bietet Wire auch verschlüsselte Audio- und Videotelefonie sowie Audiokonferenzen mit bis zu 25 und Videokonferenzen mit bis zu 12 Teilnehmern.

Das Angreifermodell als Basis für das Sicherheitskonzept von Wire ist deutlich schwächer als bei Signal App oder Threema. Ein Angreifer mit physischem Zugriff auf das Dateisystem des Gerätes wird bei Wire nicht in Betracht gezogen. Eine verschlüsselte Speicherung der Daten (wie bei Threema oder Signal App) ist im Whitepaper[46] von Wire ausdrücklich nicht vorgesehen.

Das Whitepaper postuliert, dass unter Android der Schutzwall gegen Zugriffe auf die gespeicherten Daten durch andere Apps ausreichend ist, und empfiehlt auf PCs und Laptops die Verschlüsselung der Festplatte (was aber auf Mehrbenutzersystemen nicht gegen Zugriffe durch Dritte schützt).

Außerdem speichert Wire die Metadaten der Kommunikation dauerhaft unverschlüsselt in der europäischen Amazon-Cloud. Im Privacy Statement findet man keinen Hinweis auf diese Mini-VDS und auch keine Informationen darüber, wie lange die Metadaten gespeichert werden. (Für Unternehmen mit Compliance-Anforderungen und eigenen Servern ist das nicht relevant.)

Haben wir 20 Jahre gegen die Vorratsdatenspeicherung bei E-Mails gekämpft, um sie dann bei einem Messenger *aus technischen Gründen* ohne Widerstand zu akzeptieren?

Vor einigen Jahren war Wire der deutsche Shooting-Star unter den Krypto-Messengern, aber die Umsetzung einer föderalen Infrastruktur der Server wurde auf unbekannte Zeit verschoben und die Vorteile gegenüber WhatsApp sind gering. Als Argument könnte man anerkennen, das die Adressbücher nicht an Datensammler weitergegeben werden.

Wire Enterprise ist vom BSI für VS-NfD zugelassen und der bevorzugte Messenger der Bundesregierung. Zudem ist es eine gute Kollaborationsplattform für Unternehmen.

[46] https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf

11.1.7 Einige weitere Messenger (unvollständig)

WhatsApp ist mit 2 Mrd. Nutzern weltweit der populärste Messenger. Es folgen der Facebook Messenger mit 1,3 Mrd. und WeChat mit 1,2 Mrd. Nutzern. Telegram und Signal App sind unter den Top10 und Threema ist unter den Top20 (Stand Oktober 2020). Die Verteilung der Messenger-Nutzung in Deutschland zeigt Abb. 11.14 (Stand: November 2019).

Abbildung 11.14: Nutzung der Messenger in Deutschland (2019)

Facebook Messenger ist keine Alternative zu WhatsApp. Man kann zwar eine Ende-zu-Ende-Verschlüsselung aktivieren, aber Facebook kann bei Bedarf trotzdem die verschlüsselten Chats mitlesen. Dabei wird nicht die Krypto gebrochen, sondern auf Anforderung eine unverschlüsselte Kopie der Nachricht an Facebook gesendet.

Delta-Chat missbraucht das E-Mail-Protokoll. Die Chat-Nachrichten werden per E-Mail ausgetauscht und Delta-Chat verwendet dafür einen vorhandenen E-Mail-Account.

Die Verschlüsselung erfolgt mit OpenPGP und der Schlüsselaustausch per Autocrypt. Warum Autocrypt kein sicherer Schlüsseltausch ist, kann man im Kapitel Pretty Easy Privacy (PEP) und Autocrypt nachlesen. Diese Verschlüsselung bietet nur geringe Sicherheit,

konzeptuell bedingt nur *Some Protection Most of the Time*. Mit anderen Worten: Sie wird genau dann nicht funktionieren, wenn man sie gebraucht hätte, also wenn sich ein ernsthafter Angreifer für die Inhalte der Chats interessiert.

Mit der Erweiterung *countermitm* versucht Delta-Chat, die Schwächen des Autocrypt-Schlüsseltausches etwas abzumildern. Es wird damit die Möglichkeit zur Verifizierung von Schlüsseln eingeführt und Man-in-the-Middle-Angriffe auf verifizierte Schlüssel werden verhindert.

Bei der E-Mail-Kommunikation fallen aber viele Metadaten beim Provider an.

E-Mail ist das am häufigsten genutzte Medium für Textnachrichten. Als Realitätscheck ein Vergleich mit den genannten Messenger-Diensten:

- Die Grundlage für die seit vielen Jahren hohe Nutzung von E-Mail bilden offene Protokolle, die eine föderale Serverlandschaft von vielen Anbietern auf Basis von Open-Source-Software erlauben.
- E-Mails werden in der Regel unverschlüsselt gesendet. Die großen E-Mail-Provider wie Google oder Microsoft lesen ungeniert mit. Auch wenn man selbst einen datenschutzfreundlichen E-Mail-Provider nutzt, ist man gegen das Mitlesen nicht geschützt, weil:

  Google has most of my emails, because it has all of yours.
- Die zusätzliche Installation und Konfiguration von OpenPGP für die Ende-zu-Ende-Verschlüsselung ist kompliziert. Es gibt keine Ende-zu-Ende-Verschlüsselung mit *Forward Secrecy* für E-Mails.
- Der Austausch von Schlüsseln für OpenPGP oder S/MIME muss per Hand erfolgen, es gibt keinen vertrauenswürdigen Automatismus. Außerdem müssen die Schlüssel per Hand verifiziert werden.
- Die Sicherheit der Transportverschlüsselung (SSL/TLS) zwischen den Mailservern schwankt von *nicht vorhanden* bis *möglicherweise verschlüsselt, wenn keiner angreift.* Garantierte TLS-Verschlüsselung und Certificate Pinning in Form von DANE/TLSA gibt es erst in kleinen Ansätzen bei sehr wenigen Mailprovidern.

Schlussfolgerung: Trotz der Mängel haben die oben genannten Alternativen zu WhatsApp wie Signal oder Threema erhebliche Vorteile gegenüber E-Mails hinsichtlich der Verschlüsselung. Deshalb stehen Messenger im Crypto War 3.0 generell im Focus bei der Forderung nach Backdoors, während (bisher) keine Backdoors für verschlüsselte E-Mails gefordert werden.

11.2 Verschlüsselte Telefonie

Für verschlüsselte Telefonie gibt es mehrere Protokolle:

- SRTP/ZRTP von Phil Zimmermann kümmert sich um die Verschlüsselung des Datenstroms bei Audio- und Videotelefonie. Die Ende-zu-Ende-Verschlüsselung des Datenstroms erfolgt mit SRTP, den automatischen Schlüsseltausch erledigt ZRTP und die Verifizierung erfolgt mit SAS. Die Verbindung zwischen den Clients kann entweder via SIP-Protokoll aufgebaut werden oder auch über andere Protokolle.

- WebRTC wurde maßgeblich von Google und Mozilla initiiert, um der Konkurrenz von Microsoft Skype etwas entgegenzusetzen. Es wurde vom W3C standardisiert und ist seit 2017 in allen Browsern enthalten. Es wird aber auch in einigen Messengern für verschlüsselte Audiotelefonie verwendet.

  Der Datenstrom wird bei WebRTC ebenfalls mit SRTP verschlüsselt. Die Verwaltung der Accounts erfolgt auf zentralen Servern, aber die Sprachkommunikation läuft über eine direkte Verbindung zwischen den Clients. Für den Aufbau der Verbindung kann ICE (Internet Connectivity Establishment) genutzt werden. Wenn keine direkte Verbindung zwischen den Clients möglich ist, werden TURN-Server als Proxys genutzt.

- Das GSMK-Protokoll verschlüsselt den Datenstrom doppelt mit AES256 und Twofish. Die niedrige, feste Datenrate von 4,8 kBit/s soll eine Kommunikation auch dann ermöglichen, wenn verschlüsselte VoIP-Telefonie mittels DPI blockiert wird, wie es bspw. in einigen Gebieten von Frankreich, in VAE oder Saudi-Arabien üblich ist.

Verschiedene Forschungsergebnisse wie *Language Identification in Ecrypted VoIP Traffic*[47] (2007), *Uncovering Spoken Phrases in Encrypted VoIP Conversation*[48] (2008) und *Phonotactic Reconstruction of Encrypted VoIP Conversations*[49] (2011) zeigen, dass es bei der Verschlüsselung von Telefonie Angriffsmöglichkeiten gibt, um gesprochene Phrasen anhand der variierenden Datenrate aus dem Datenstrom zu rekonstruieren, ohne die Verschlüsselung knacken zu müssen. Deshalb wird für hohe Sicherheitsanforderungen die Verwendung einer festen Datenrate empfohlen.

Bei WhatsApp ist die Technik im Einsatz. Als bei einem (angeblich sicher verschlüsseltem) WhatsApp Telefonat im März 2023 mit einer Bekannten, die in Brüssel bei der EU im Engergiesektor arbeitet, im Nebensatz das Wort *Gazprom* fiel, wurde die Verbindung kurz unterbrochen.

Hallo, hallo - bist Du nach da??? Als die Verbindung nach eingen Sekunden wieder aufgebaut war ein Lachen am anderen Ende der Leitung: *Das passiert immer, wenn ich Gazprom sage.* Nachdem die belanglose Konversation 5min weiterging wieder eine kurze Unterbrechung.

WhatsApp verwendet die SRTP Verschlüsselung allerdings ohne ZRTP zum Schlüsseltausch und ohne SAS zur Verifikation, so dass man die Verschlüsselung nicht einfach verifizieren kann.

In den Einstellungen könnte man unter *Account* → *Sicherheit* die Sicherheitsbenachrichtigungen aktivieren, so dass im Beispiel (vermutlich) eine Warnung hätte angezeigt werden müssen, wenn es für Lawful Interception keine Sonderbehandlung gibt, die diese Warnung unterdrückt(?) Die Option ist standardmäßig deaktiviert. Aber wer sicher kommunizieren will, würde sich wahrscheinlich nicht auf WhatsApp verlassen, dessen Mutterkonzen PRISM Partner der NSA ist.

11.2.1 SRTP/ZRTP-Verschlüsselung

Das SRTP/ZRTP-Protokoll[50] von Phil Zimmermann (Erfinder von PGP) spielt eine zentrale Rolle bei verschlüsselter Telefonie. Es gewährleistet eine sichere Ende-zu-Ende-Verschlüsselung der Sprachkommunikation. Wenn beide Kommunikationspartner eine Software verwenden, die das ZRPT-Protokoll beherrscht, wird die Verschlüsselung automatisch ausgehandelt. Kurze Erläuterung der Begriffe:

[47] https://www.usenix.org/legacy/events/sec07/tech/full_papers/wright/wright.pdf
[48] https://www.cs.unc.edu/~fabian/papers/oakland08.pdf
[49] https://www.cs.unc.edu/~fabian/papers/foniks-oak11.pdf
[50] https://tools.ietf.org/html/draft-zimmermann-avt-zrtp-22

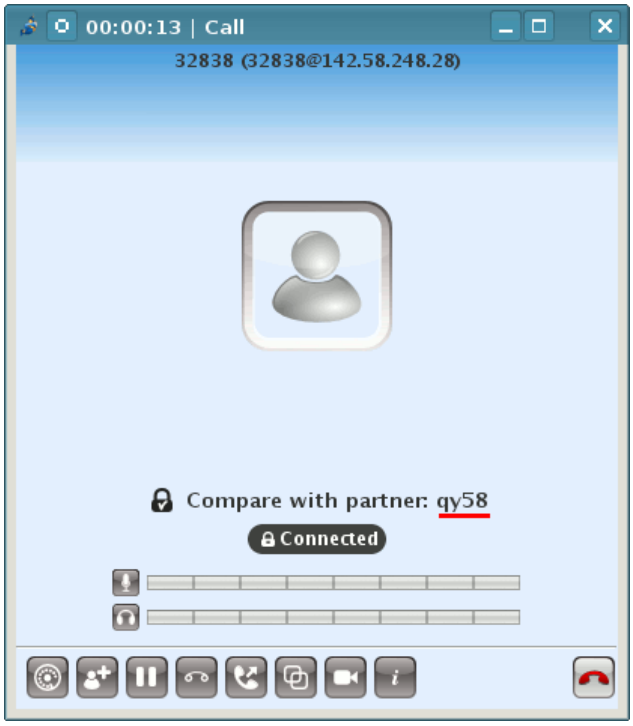


Abbildung 11.15: SAS Authentication bei Jitsi als Beispiel

SRTP definiert die Verschlüsselung des Sprachkanals. Die Verschlüsselung der Daten erfolgt symmetrisch mit AES128/256 oder Twofish128/256. Für die Verschlüsselung wird ein gemeinsamer Schlüssel benötigt, der zuerst via ZRTP ausgehandelt wird.

ZRTP erledigt den Schlüsselaustausch für SRTP und nutzt dafür das Diffie-Helman-Verfahren. Wenn beide VoIP-Clients ZRTP beherrschen, wird beim Aufbau der Verbindung ein Schlüssel für SRTP automatisch ausgehandelt und verwendet. Der Vorgang ist transparent und erfordert keine Aktionen der Nutzer. Allerdings könnte sich ein Man-in-the-Middle einschleichen und die Verbindung kompromittieren (belauschen).

SAS dient dem Schutz gegen Man-in-the-Middle-Angriffe auf ZRTP. Den beiden Kommunikationspartnern wird eine 4-stellige Zeichenfolge angezeigt, die über den Sprachkanal zu verifizieren ist.

Üblicherweise nennt der Anrufer die beiden ersten und der Angerufene die beiden letzten Buchstaben. Wenn die Zeichenfolge identisch ist, kann man davon ausgehen, dass kein Man-in-the-Middle das Gespräch belauschen kann.

Moderne Messenger mit verschlüsselter Telefonie (außer WhatsApp) haben ein ähnliches Feature zur Verifikation implementiert, verwenden aber meist 4 Emojis statt Buchstaben.

11.2.2 Verschlüsselt chatten und telefonieren mit qTox

Tox ist ein Protokoll für verschlüsselte Telefonie und Chats. Die Kommunikation läuft direkt von Client zu Client. Die Teilnehmer finden sich gegenseitig über eine Distributed Hash Table (DHT). Es gibt keinen Provider, der Kommunikationsprofile erstellen oder zur Implementierung von Backdoors für Behörden gezwungen werden könnte.

Tox verwendet für die Krypto nicht die üblichen, vom NIST standardisierten Verfahren, sondern Verfahren von D. J. Bernstein. Der ECDHE-Schlüsseltausch nutzt curve25519, statt AES wird XSALSA20 verwendet und statt SHA256 kommt POLY1350 zum Einsatz.

Es gibt mehrere Clients, die das Protokoll beherrschen. Für PCs und Laptops eignet sich **qTox**. Für Android gibt es **aTox**. Für iPhones gibt es keinen Tox-Client.

Bei Smartphones ist zu beachten, dass die Call History (Liste aller Anrufe) an Google übertragen wird, wenn die App die Anrufe auf dem Sperrbildschirm anzeigen kann. Dort werden die Daten für 4–6 Monate gespeichert (private Vorratsdatenspeicherung bei NSA-PRISM-Partnern). Geheimdienste haben Zugriff auf diese Daten und die Firma Elcomsoft liefert die nötigen Tools für die Auswertung. Die Datenspeicherung lässt sich deaktivieren, indem man die Nutzung der Google Cloud Services komplett deaktiviert.

Installation von qTox

Windows: auf der Downloadseite steht eine Setup-Datei zur Verfügung. Nach dem Download muss man das Ausführen der Setup-Datei zulassen, da die Datei aus dem Internet stammt und die Ausführung deshalb möglicherweise blockiert wird. Dafür klickt man mit der rechten Maustaste auf die Datei und wählt den Menüpunkt *Eigenschaften*. Danach startet man das Setup mit einem Rechtsklick auf die Datei, wählt den Menüpunkt *Als Administrator ausführen* und folgt dem Installationsassistenten.

Fedora, Debian 10+, Ubuntu 19.04+, SuSE usw. bieten qTox in den Repositorys zur Installation an. Für Installation und Aktualisierung kann man den bevorzugten Paketmanager nutzen:

```
Fedora:  > sudo dnf install qtox
Ubuntu:  > sudo apt install qtox
```

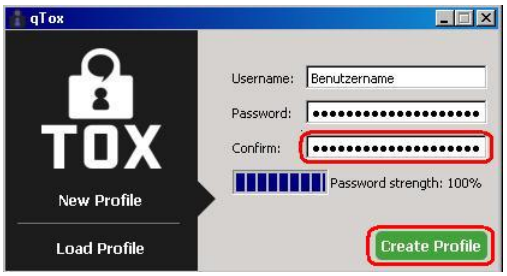
Anwender von Fedora sollten das RPMFusion-Repository vorher aktivieren, damit die notwendigen Codecs für Audio- und Videotelefonie mitinstalliert werden.

***BSD:** Einen aktuellen Port findet man in PKGSRC unter *net-im/qTox*. Die Installation erfolgt wie üblich mit make und benötigt einige Zeit:

```
# cd /usr/ports/net-im/qTox
# make install clean
```

Account erstellen

qTox lässt sich mit Klick auf das Programmsymbol starten. Es öffnet sich das Profilmenü. Hier hat man die Wahl, ein bereits bestehendes Profil zu laden (*LoadProfile*) oder ein neues Profil anzulegen. Zunächst wählt man den Benutzernamen und das Passwort:



Es sollte ein starkes Passwort gewählt werden, denn je größer die Basis der möglichen Zeichen ist (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen), je zufälliger diese Zeichen gewürfelt werden und je mehr Stellen das Passwort hat, desto stärker ist es.

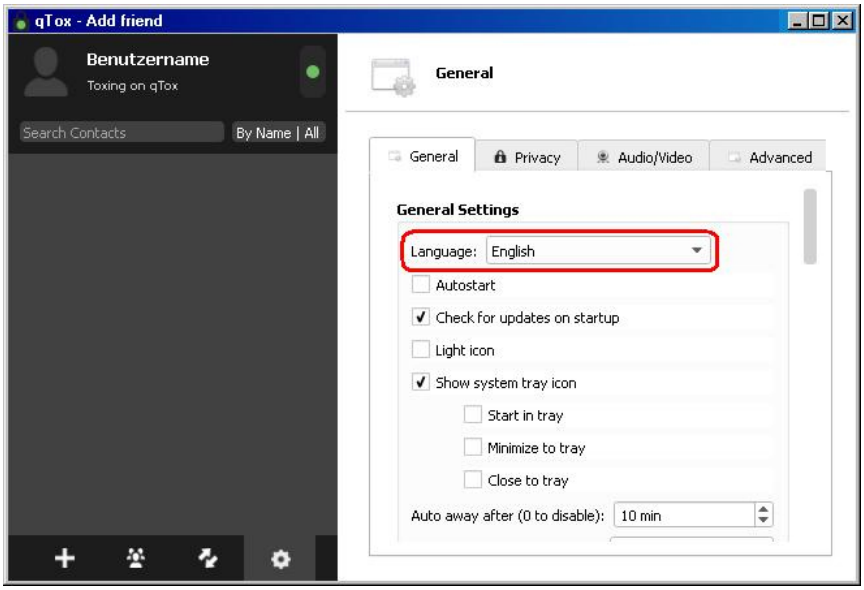
Konfiguration von qTox

Im Hauptmenü wählt man in den Einstellungen, die man jederzeit durch Klick auf das Zahnrädchen erreicht, zunächst die Registerkarte *General*. Bei *Language* lässt sich die Sprache umstellen indem man auf *English* klickt und die Sprache *Deutsch* wählt.

Hier lassen sich nun folgende Einstellungen vornehmen:

- ob qTox bei jedem Systemstart mitgestartet werden soll,
- ob man regelmäßig nach Updates suchen möchte,
- ob in der Systemleiste ein Icon angezeigt werden soll,
- ob qTox bei Programmstart zunächst nur mit diesem Icon oder mit einem Fenster starten soll,
- ob qTox beim Minimieren in die Systemleiste statt in die Taskleiste minimiert werden soll,
- ob bzw. nach welcher Zeit der Abwesenheit qTox den Status *Abwesend* anzeigen soll
- und ob geteilte Dateien automatisch angenommen werden sollen.

Aus Sicherheitsgründen sollten Dateien nie automatisch angenommen werden!



Auf der Registerkarte *Privatsphäre* kann man die Speicherung des Chat-Verlaufes deaktivieren. Die Speicherung verschlüsselter Chats ist als *Mannings-Bug* bekannt geworden. Außerdem kann man die Schreibbenachrichtigungen für Chats deaktivieren.

Auf der Registerkarte *Audio/Video* kann man die Audio- und Videoeinstellungen konfigurieren und testen.

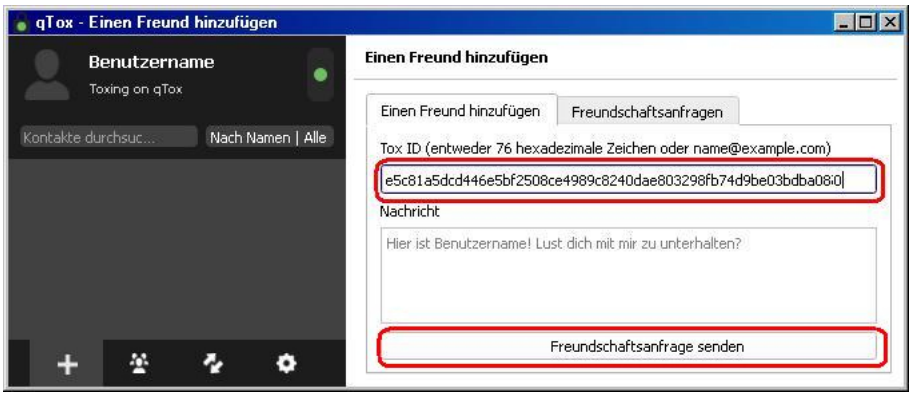
Auf der Registerkarte *Erweitert* kann man qTox in eine portable Programmversion umwandeln, die man auf dem USB-Stick mitnehmen kann.

Kontakt aufnehmen

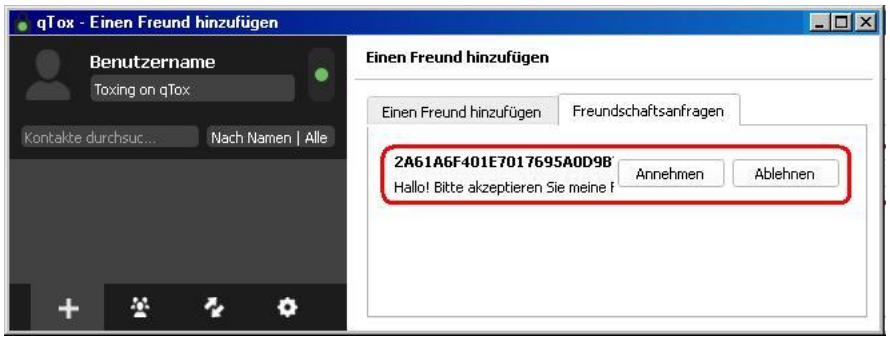
Wenn Anton und Beatrice Tox für die Kommunikation nutzen wollen, müssen sie die Tox-ID austauschen. Das könnte in folgenden Schritten ablaufen:

1. Anton schickt seine Tox-ID irgendwie an Beatrice.
2. Beatrice sendet eine Freundschaftsanfrage an diese Tox-ID.
3. Anton akzeptiert die Freundschaftsanfrage von Beatrice.

Um eine Freundschaftsanfrage zu senden, benötigt man die 76-stellige Tox-ID des Kontakts, die über einen sicheren Kanal ausgetauscht werden muss. Die eigene Tox-ID findet man, wenn man sich das eigene Profil anzeigen lässt. Zusammen mit der Freundschaftsanfrage wird eine Nachricht gesendet. Anhand dieser Nachricht kann der Empfänger den Anfragenden erkennen.

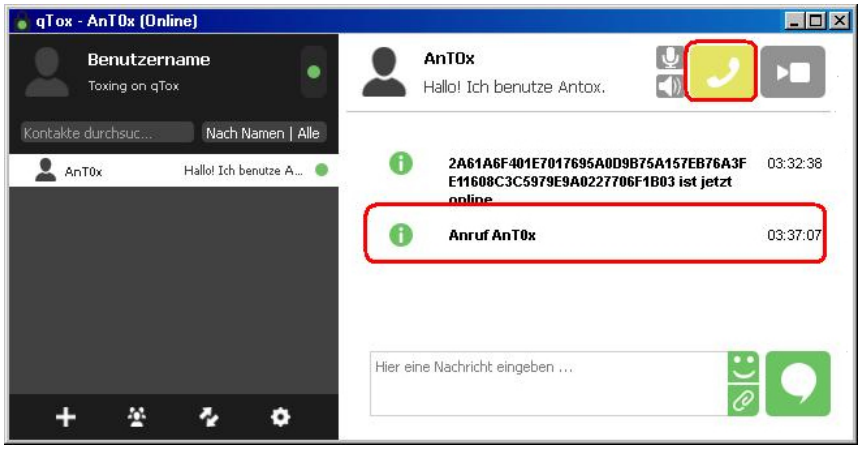


Erhält man eine Freundschaftsanfrage eines anderen Benutzers, so wird oben links im Programmfenster ein grünes Feld mit der Aufschrift *1 neue Freundschaftsanfrage* angezeigt. Durch Klick auf diese grüne Schaltfläche werden weitere Infos zur Freundschaftsanfrage angezeigt – etwa die ID, eventuell auch der Benutzername und/oder ein Begrüßungstext. Man hat nun die Wahl, die Freundschaftsanfrage anzunehmen oder abzulehnen. Mit der Annahme der Freundschaftsanfrage werden die nötigen Krypto-Schlüssel ausgetauscht, die für die verschlüsselte Kommunikation benötigt werden.

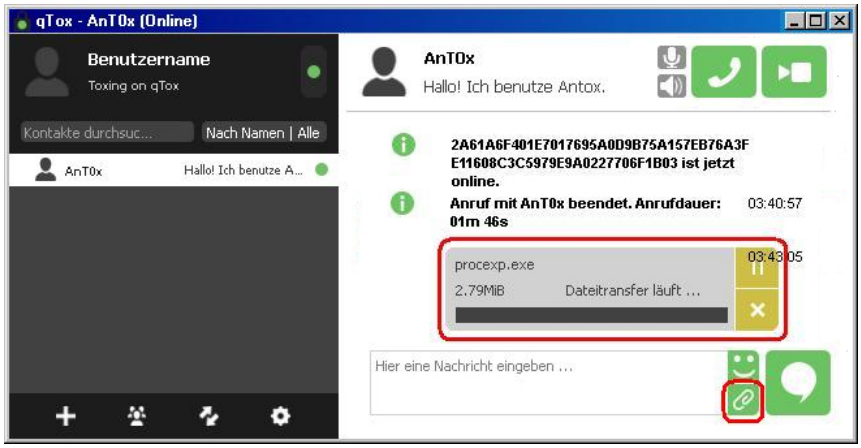


Kontakte anrufen, Dateien schicken oder chatten

Wenn man auf das Profil eines Kontakts klickt, hat man viele Möglichkeiten. Man kann telefonieren und per Video schnattern (Buttons oben rechts) ...



... oder chatten und Dateien verschicken (Buttons unten rechts).



11.2.3 Skype???

Der bekannteste Anbieter für Internettelefonie (Voice over IP, VoIP) ist zweifellos **Skype**. Die Installation und das Anlegen eines Account ist einfach. Man benötigt lediglich eine E-Mail-Adresse. Skype-Verbindungen sind schwer zu blockieren. Die Client-Software findet fast immer eine Verbindung zum Netz, auch hinter restriktiven Firewalls. Skype bot eine gute Verschlüsselung und kann Verbindungen ins Festnetz herstellen.

Nach der Übernahme von Skype durch Microsoft wurde die zensurrobuste Infrastruktur von Skype umgebaut und die Ende-zu-Ende-Verschlüsselung von Skype kompromittiert. Statt einer Peer-to-Peer-Infrastruktur nutzt Skype jetzt sogenannte Super-Nodes, die alle in Microsoft-Rechenzentren stehen. Die Keys für die Verschlüsselung werden in der Microsoft-Cloud hinterlegt und Microsoft nutzt die sich daraus ergebenden Möglichkeiten zum Mitlesen[51] (juristisch korrekt wird in den Datenschutzbestimmungen darauf hingewiesen).

Abhörschnittstellen

Anfang der 90er-Jahre des letzten Jahrhunderts wurde das Festnetz in den Industriestaaten digitalisiert und die GSM-Verschlüsselung für Handytelefonate wurde eingeführt. Klassische

[51] https://heise.de/-1857620

Abhörmaßnahmen für einen Telefonanschluss waren ohne Kooperation der Telekommunikationsanbieter und ohne vorbereitete Schnittstellen nicht mehr möglich.

Als Antwort auf diese Entwicklung wurden in allen westlichen Industriestaaten Gesetze beschlossen, die die Telekommunikationsanbieter zur Kooperation mit den Strafverfolgungsbehörden und Geheimdiensten verpflichten und Abhörschnittstellen zwingend vorschreiben. In den USA war es der *CALEA Act*[52] von 1994. In Deutschland wurde 1995 auf Initiative des Verfassungsschutzes die *Fernmeldeverkehr-Überwachungsverordnung* (FÜV)[53] beschlossen, die 2002 durch die *Telekommunikations-Überwachungsverordnung* (TKÜV)[54] ersetzt wurde.

2005 wurde der CALEA Act durch das höchste US-Gericht so interpretiert, dass er auch für alle VoIP-Anbieter gilt, die Verbindungen in Telefonnetze weiterleiten können. Skype zierte sich anfangs, die geforderten Abhörschnittstellen zu implementieren. Mit der Übernahme von Skype durch Ebay im November 2005 wurde die Diskussion beendet. Heute bietet Skype Abhörschnittstellen in allen westeuropäischen Ländern und zunehmend auch in anderen Ländern wie Indien. In Deutschland sind Abhörprotokolle aus Skype-Gesprächen alltägliches Beweismaterial.[55]

Skype ist seit 2011 PRISM-Partner der NSA und damit direkt an das Spionagesystem der USA angeschlossen. Mit der Übernahme durch Microsoft 2012 und dem technischen Umbau konnte die von der NSA analysierte Datenmenge aus Skype verdreifacht werden.[56]

11.3 Videokonferenzen

Für die Teilnahme an einer Videokonferenz benötigt man neben dem Link zur Webkonferenz und evtl. einem Passwort nur einen Webbrowser, der nicht zu restriktiv konfiguriert ist. Die wenigsten Probleme soll es mit dem Google Chrome Browser oder Chromium geben. Auch Firefox kann verwendet werden, jedoch müssen dafür einige Voraussetzungen erfüllt sein:

- Die Verwendung von WebRTC muss möglich sein und der OpenH264-Codec muss zur Verfügung stehen, was nicht bei allen Firefox-Versionen Standard ist (siehe Kapitel 4.17).
- Um Firefox etwas zu zähmen, könnte man die minimale user.js verwenden.
- Wenn man eine restriktive Firefox-Konfiguration für spurenarmes Surfen verwendet, kann man unter *about:profiles* ein neues Profil erstellen, starten und dann passend konfigurieren (inklusive Lesezeichen für die bevorzugten Konferenz-Server).

  Wenn man dieses Profil bspw. *Videokonferenz* genannt hat, kann man es direkt mit folgendem Kommando starten oder als Starter-Icon auf dem Desktop ablegen:

  ```
  > firefox -P Videokonferenz -no-remote
  ```

OpenTalk-Videokonferenzserver

OpenTalk ist eine moderene Videokonferenzlösung, die in Deutschland entwickelt wird.

[52] https://secure.wikimedia.org/wikipedia/en/wiki/Calea
[53] http://www.online-recht.de/vorges.html?FUEV
[54] https://de.wikipedia.org/wiki/Telekommunikations-%C3%9Cberwachungsverordnung
[55] http://www.lawblog.de/index.php/archives/2010/08/17/skype-staat-hort-mit/
[56] https://heise.de/-1916340

Der Konferenzleiter (der Einladende) benötigt auf dem Videokonferenz Server einen registrierten Account, den man bei kostenfreien Angeboten mit der üblichen E-Mail Verifikation erstellen kann. Die Teilnahme als Gast ist im Browser via Einladungslink ohne Registrierung möglich.

OpenTalk ermöglicht planbare Erstellung von (wiederkehrenden) Terminen für Videokonferenzen. Die Aufzeichnung der Meetings ist möglich und es gibt Produktivitätsgadgets wie Whiteboard, ein Kaffeepausentimer (ganz wichtig) u.a.m. Außerdem kann ein Warteraum aktiviert werden, wo der Konferenzleiter die Teilnehmer vor dem Einlass in Videokonferenz überprüfen kann, um die Überraschung zu vermeiden, dass unerwünschte Dritte in einer Konferenz auftauchen.

- OpenTalk selbst bietet Videokonferenzen für Geschäftskunden, nicht für Privatkunden.[57]
- Kunden von mailbox.org ab dem Tarif *Standard* können zu OpenTalk(s) einladen.
- adminForge bietet einen kostenfreien OpenTalk Service für private Videokonferenzen.[58]

BigBlueButton-Videokonferenzserver

BigBlueButton ist in Firmen und im Bildungsbereich bei Universitäten/Schulen populär.

Die Universität Darmstadt bieten einen Konferenzserver[59] mit BigBlueButton, der mit Spenden finanziert wird und für Teilnehmer an einer Konferenz auch Telefoneinwahl anbietet. Registrierte Nutzer können sich auch permanente Konferenzräume einrichten.[60]

Jitsi-Meet-Videokonferenzserver

Jitsi Meet ist eine einfach bedienbare Videokonferenzsoftware. Auch für den Konferenzleiter (den Eindadenden) ist auf den Servern keine Anmeldung nötig. Einfach eine Ad-hoc Konferenz starten und den Link zur Konferenz kurzfristig via Messenger oder Mail verschicken.

Die Teilnahme an einer Videokonferenz kann mit einem Passwort geschützt werden und es kann eine *Lobby* (Warteraum) für eine Videokonferenz aktiviert werden, wo Gäste auf Einlass durch den Konferenzleiter warten müssen, um das unerwünschte Auftauchen von Dritten zu verhindern.

Allerdings ist es schwierig, ohne die Registrierung eines Accounts eine längerfristig teminlich geplante Videokonferenz vorzubereiten und Aufzeichnungen der Meetings sind nicht möglich.

Es gibt viele öffentlich verfügbare Jitsi-Meet-Instanzen.[61] Hier eine kleine Auswahl an Empfehlungen für Server, die von vertrauenswürdigen IT-Professionals betrieben werden:

1. Single-Server-Instanzen ermöglichen Konferenzen mit bis zu 8 oder 10 Teilnehmern:
   - Jitsi-Meet-Server der Nitrokey GmbH: https://meet.nitrokey.com
   - Jitsi-Meet-Server von Golem.de: https://meet.golem.de
2. Einige spendenfinanzierte Servercluster sind auch für größere Videokonferenzen mit 50–70 Teilnehmern geeignet:
   - Jitsi-Cluster vom Freifunk München: https://meet.ffmuc.net

[57] https://opentalk.eu/de
[58] https://teamjoin.de
[59] https://public.senfcall.de/
[60] https://lecture.senfcall.de/signin
[61] https://jitsi.github.io/handbook/docs/community/community-instances/

- Jitsi-Meet-Server der Horizon44 GmbH: https://sichere-videokonferenz.de/

3. Kunden von mailbox.org, die den Standard- oder Premium-Tarif gebucht haben, können sich im Web-GUI zwei Videokonferenzen anlegen und bis zu 25 Teilnehmer einladen.

Kapitel 12

Anonymisierungsdienste

Anonymisierungsdienste verwischen die Spuren im Internet bei der Nutzung herkömmlicher Webdienste. Die verschlüsselte Kommunikation verhindert auch ein Belauschen des Datenverkehrs durch mitlesende Dritte. Diese Dienste sind für den anonymen Zugriff auf Websites geeignet und ermöglichen auch unbeobachtete, private Kommunikation via E-Mail, Jabber, IRC usw.

Die unbeobachtete, private Kommunikation schafft keine rechtsfreien Räume im Internet, wie Demagogen des Überwachungsstaates immer wieder behaupten. Sie ist ein grundlegendes Menschenrecht, das uns zusteht. Nach den Erfahrungen mit der Diktatur Mitte des letzten Jahrhunderts findet man dieses Grundrecht in allen übergeordneten Normenkatalogen, von der UN-Charta der Menschenrechte bis zum Grundgesetz.

Anonymisierungsdienste sind ein Hammer unter den Tools zur Verteidigung der Privatsphäre, aber nicht jedes Problem ist ein Nagel. Das Tracking von Anbietern wie DoubleClick verhindert man effektiver, indem man den Zugriff auf Werbung unterbindet. Anbieter wie z. B. Google erfordern es, Cookies und JavaScript im Browser zu kontrollieren. Anderenfalls wird man trotz der Nutzung von Anonymisierungsdiensten identifiziert.

12.1 Gedanken zur Anonymität

Es gibt keine simple Anonymität, die man mit dem Verwenden eines Anonymisierungsdienstes wie Tor Onion Router einfach anknipst und fertig. Bei der Behauptung von Anonymität muss man hinzufügen, gegenüber welchem Angreifer man anonym sein will.

Beispiele: Anton ist ein subversives Individuum, das beim Diskutieren in einem Forum, beim Schreiben von Kommentaren oder im Chat einer Selbsthilfegruppe gern anonym bleiben möchte. Eve ist die Angreiferin.

1. Eve kann als gleichberechtigte Teilnehmerin im Forum/Chat die Beiträge lesen.

   Um gegenüber dieser Eve anonym zu bleiben, reicht es aus, ein willkürliches Pseudonym zu wählen und keine privaten, individuellen Informationen zu verraten.

   Ein kleiner Missgriff von Anton auf dieser Ebene ist die Wahl eines möglichst kreativ-auffälligen Avatar-Bildchens. Wenn man manche (besonders kreativen) Avatare der anonymen Teilnehmergruppen von Privacy-Foren durch eine inverse Bildersuche schickt und die Spuren weiter verfolgt, kann man in 10 Minuten den realen Namen finden, manchmal sogar den Wohnsitz.

2. Eve hat als Webmaster oder Hackerin Zugriff auf die Registrierungsdaten.

   Anton schützt sich, indem er statt seiner realen eine temporäre E-Mail-Adresse oder einen E-Mail-Alias exklusiv für die Registrierung des Accounts verwendet, und bleibt damit auch gegenüber dieser Eve anonym.

3. Eve hat Zugriff auf die IP-Adressen der Nutzer bei einer großen Anzahl von Webseiten oder kann mit polizeilichen Befugnissen die Identität der Person hinter einer IP-Adresse ermitteln.

   Um Deanonymisierung anhand der IP-Adresse durch Auskünfte bei Telekommunikationsprovidern oder Korrelation mit Aktivitäten unter realem Namen (Einkäufe, Bankgeschäfte online usw.) zu verhindern, muss Anton sich ein bisschen mehr bemühen. Für seine anonymen Aktivitäten muss er mindestens ein VPN mit wechselnden Servern und zusätzlich ein separates Browserprofil nutzen.

4. Eve kann als potente (staatliche) Angreiferin einen erheblichen Teil des Internet-Traffics direkt kontrollieren oder Daten bei den Backbone-Providern kaufen und VPNs deanonymisieren.

   Dann muss Anton die Hammer-Tools der Anonymisierung verwenden, wie Tor.

5. Eve arbeitet beim BKA, FBI oder Scotland Yard und hat den Auftrag, Anton zu finden. Für diesen Auftrag hat sie Zugriff auf (fast) alle irgendwo gesammelten Daten.

   Dann reicht es nicht mehr aus, wenn Anton einfach nur den TorBrowser startet. Jeder kleine Fehler kann die Verknüpfung von Datenspuren ermöglichen, die am Ende zur Deanonymisierung führen. Unter Umständen reicht es aus, sein Smartphone im gleichen WLAN zu benutzen[1] oder man wird von Metadaten in einem Foto[2] verraten.

   Ein Student wollte bspw. vor einigen Jahren eine Prüfung verhindern und schickte eine Bombendrohung als E-Mail via TorBrowser an die Universität. Der Verdacht fiel schnell auf den einzigen Studenten, der im WLAN der Bibliothek der Universität den Tor Onion Router nutzte, und eine forensische Analyse seines Computers bestätigte den Verdacht. (Die genauen Details habe ich leider vergessen.)

Anonymität hat nicht nur Vorteile sondern auch Schattenseiten (z. B. wenig Reputation, Vertrauen oder Respekt). Oft wird man daher mehrere Identitäten mit unterschiedlichem Schutzlevel im Internet verwenden. Die Aktivitäten mit den unterschiedlichen Identitäten sind strikt zu trennen.

12.2 Was können Anonymisierungsdienste wie Tor?

Anonymisierungsdienste verstecken die IP-Adresse des Nutzers und verschlüsseln die Kommunikation zwischen dem Nutzer und den Servern des Dienstes. Außerdem werden spezifische Merkmale modifiziert, die den Nutzer identifizieren könnten (Browser-Typ, Betriebssystem usw.).

1. **Profilbildung:** Nahezu alle großen Suchmaschinen generieren Profile von Nutzern. Facebook und andere Anbieter speichern die IP-Adressen für Auswertungen. Nutzt man Anonymisierungsdienste, ist es für die Anbieter nicht möglich, diese Information sinnvoll auszuwerten.

[1] Kevin D. Mitnick, „Die Kunst der Anonymität im Internet“
[2] John McAfee, 2012

2. **Standortbestimmung:** Die Anbieter von Webdiensten können den Standort des Nutzers nicht via Geolocation bestimmen. Damit ist es nicht möglich:
   - die Firma zu identifizieren, wenn der Nutzer in einem Firmennetz sitzt;
   - bei mobiler Nutzung des Internet Bewegungsprofile zu erstellen.
3. **Belauschen durch Dritte:** Die verschlüsselte Kommunikation mit den Servern des Anonymisierungsdienstes verhindert ein Mitlesen des Datenverkehrs durch Dritte in unsicheren Netzen (Cafés, WLANs am Flughafen oder im Hotel, TKÜV usw.).
4. **Rastern:** Obwohl IP-Adressen die Identifizierung von Nutzern ermöglichen, sind sie rechtlich in vielen Ländern ungenügend geschützt. In den USA können sie ohne richterliche Prüfung abgefragt werden. Die TK-Anbieter genießen Straffreiheit, wenn sie die nicht vorhandenen Grenzen übertreten. Wenig verwunderlich, dass man IP-Adressen zur tagtäglichen Rasterfahndung nutzt. Facebook gibt täglich 20–30 IP-Adressen an US-Behörden, AOL übergibt 1000 Adressen pro Monat ...
5. **Zensur:** Der Datenverkehr kann vom Provider oder einer restriktiven Firewall nicht manipuliert oder blockiert werden. Anonymisierungsdienste ermöglichen einen unzensierten Zugang zum Internet. Sie können sowohl die *Great Firewall* von China und Mauretanien als auch die in westeuropäischen Ländern verbreitete Zensur durch Kompromittierung des DNS-Systems durchtunneln.
6. **Repressionen:** Blogger können Anonymisierungsdienste nutzen, um kritische Informationen aus ihrem Land zu verbreiten, ohne die Gefahr persönlicher Repressionen zu riskieren. Für Blogger aus Südafrika, Syrien oder Burma ist es teilweise lebenswichtig, anonym zu bleiben. Der Iran wertet Twitter-Accounts aus, um Dissidenten zu beobachten
7. **Leimruten:** Einige Websites werden immer wieder als Honeypot genutzt. Ein Beispiel sind die Leimruten des BKA. In mehr als 150 Fällen wurden die Fahndungsseiten von LKAs oder des BKA als Honeypot genutzt und die Besucher der Webseiten in Ermittlungen einbezogen.[3] Surfer wurden identifiziert und machten sich verdächtig, wenn sie sich auffällig für bestimmte Themen interessierten.
8. **Geheimdienste:** Sicherheitsbehörden und Geheimdienste können mit diesen Diensten ihre Spuren verwischen. Nicht immer geht es dabei um aktuelle Operationen. Die Veröffentlichung der IP-Adressbereiche des BND bei Wikileaks ermöglichte interessante Schlussfolgerungen zur Arbeitsweise des Dienstes. Beispielsweise wurde damit bekannt, dass der BND gelegentlich einen bestimmten Escort-Service in Berlin in Anspruch nimmt.
9. **Belauschen durch den Dienst:** Im Gegensatz zu einfachen VPNs oder Web-Proxys schützen Anonymisierungsdienste auch gegen Beobachtung durch die Betreiber des Dienstes selbst. Die mehrfache Verschlüsselung des Datenverkehrs und die Nutzung einer Kette von Servern verhindert, dass einzelne Betreiber des Dienstes die genutzten Webdienste einem Nutzer zuordnen können.

[3] http://heise.de/-1704448

12.3 Tor Onion Router

Das Onion Routing wurde von der US-Navy entwickelt. Die Weiterentwicklung liegt beim TorProject.org und wird durch Forschungsprojekte u. a. von deutschen Universitäten oder im Rahmen des *Google Summer of Code* unterstützt.

Tor nutzt ein weltweit verteiltes Netz von 6.000–7.000 aktiven Nodes. Aus diesem Pool werden jeweils drei Nodes für eine Route ausgewählt. Die Route wechselt regelmäßig in kurzen Zeitabständen. Die zwiebelartige Verschlüsselung sichert die Anonymität der Kommunikation. Selbst wenn zwei Nodes einer Route kompromittiert wurden, ist eine Beobachtung durch mitlesende Dritte nicht möglich. Da die Route durch das Tor-Netzwerk ständig wechselt, müsste ein großer Teil des Netzes kompromittiert worden sein, um einen Nutzer zuverlässig deanonymisieren zu können.

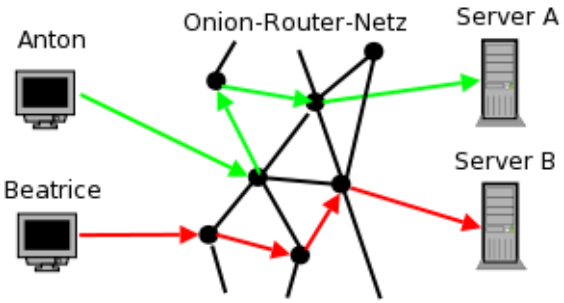


Abbildung 12.1: Das Prinzip von Tor Onion Router

Tor ist neben Surfen auch für IRC, Instant-Messaging, den Abruf von Mailboxen o. Ä. nutzbar. Dabei versteckt Tor nur die IP-Adresse! Für die sichere Übertragung der Daten ist SSL- oder TLS-Verschlüsselung zu nutzen. Sonst besteht die Möglichkeit, dass *Bad Exit Nodes* die Daten belauschen und an Userkennungen und Passwörter gelangen.

Der Inhalt der Kommunikation wird 1:1 übergeben. Für anonymes Surfen bedarf es weiterer Maßnahmen, um die Identifizierung anhand von Cookies, EverCookies oder JavaScript-Fingerprinting zu verhindern. Das TorBrowserBundle ist für anonymes Surfen mitzunutzen.

Verschiedene Sicherheitsforscher demonstrierten, dass es mit schnüffelnden *Bad Exit Nodes* relativ einfach möglich ist, Daten der Nutzer zu sammeln.

- Dan Egerstad demonstrierte, wie man in kurzer Zeit die Account-Daten von mehr als 1000 E-Mail-Postfächern erschnüffeln kann, u. a. von 200 Botschaften.[4]
- Auf der Black Hack 2009 wurde ein Angriff auf die HTTPS-Verschlüsselung beschrieben. In Webseiten wurden HTTPS-Links durch HTTP-Links ersetzt. Innerhalb von 24 Stunden konnten mit einem Tor Exit Node folgende Accounts erschnüffelt werden: 114x Yahoo, 50x GMail, 9x Paypal, 9x Linkedin, 3x Facebook.[5]

  2012 haben mehrere russische Exit-Nodes diesen Angriff praktisch umgesetzt.
- Die Forscher um C. Castelluccia nutzten für ihren Aufsatz *Private Information Disclosure from Web Searches (The case of Google Web History)*[6] einen schnüffelnden Tor Exit Node, um private Informationen von Google-Nutzern zu gewinnen.

[4] https://heise.de/-95770
[5] http://blog.internetnews.com/skerner/2009/02/black-hat-hacking-ssl-with-ssl.html
[6] http://planete.inrialpes.fr/projects/private-information-disclosure-from-web-searches/

- Um reale Zahlen für das Paper *Exploiting P2P Applications to Trace and Profile Tor Users* zu generieren, wurden sechs modifizierte Tor-Nodes genutzt und innerhalb von 23 Tagen mehr als 10.000 User deanonymisiert.[7]

Man kann davon auszugehen, dass die Geheimdienste verschiedener Länder ebenfalls im Tor-Netz aktiv sind. Deshalb sollte man die Hinweise zur Sicherheit beachten: sensible Daten nur über SSL-verschlüsselte Verbindungen übertragen, Warnungen nicht wegklicken, Cookies und JavaScript deaktivieren usw. Dann ist Tor für anonyme Kommunikation geeignet.

Tor bietet nicht nur anonymen Zugriff auf verschiedene Services im Web. Die *Tor-Onion-Services* bieten Möglichkeiten, anonym und zensurresistent zu publizieren.

Finanzierung von TorProject.org

Formal ist TorProject.org unabhängig. Über 20 Jahre hing das Projekt jedoch an der Finanzierung durch die US-Regierung. Erst durch diese langjährige Finanzierung durch das US-Verteidigungsministerium, das US-State-Department, das Broadcasting Board of Governors (BBG)[8] und andere US-Behörden konnte das Projekt zum größten und erfolgreichsten Anonymisierungsprojekt werden.[9]

Seit 2015 bemüht TorProject.org sich darum, die Finanzierung zu diversifizieren und den Anteil der US-Regierung zu senken. Dieser Anteil sank von 85 % (2015) auf 39 % (2019).

Für die verbleibenden 61 % der insgesamt 4,6 Mio. Dollar wurden 2020 folgende Geldgeber genannt:

- 15,4 % von einer Behörde des schwedischen Außenministeriums,
- 13,4 % von der Mozilla Foundation,
- 6,2 % von der US-amerikanischen Stiftung Media Democracy Fund,
- 4,1 % von der Organisation Handshake Open Source Pledge,
- 11,9 % Einzelspenden.

Tor ist eine Triple-Use-Technik

Anonymisierungsdienste und Kryptografie allgemein sind Triple-Use-Techniken. Am Beispiel von Tor Onion Router kann man es deutlich erkennen:

1. Ganz normale Menschen nutzen Tor, um ihre Privatsphäre vor Datensammlern und staatlicher Überwachung/Repressalien zu schützen. Dieses Szenario steht oft im Mittelpunkt der Diskussion mit Aktivisten, ist aber vielleicht die kleinste Gruppe.

   Bei den Protesten im Sommer 2020 nach den Wahlen in Weißrussland hätte Tor Onion Router seine Attraktivität für politische Aktivisten beweisen können. Zwei Jahre zuvor hatte die weißrussische Regierung modernste Überwachungs- und Filtertechnik für 2,5 Mio. Dollar gekauft und rechtzeitig vor den Wahlen in Betrieb genommen.

[7] http://hal.inria.fr/inria-00574178/en/

[8] BBG ist ein Spin-Off der CIA, das auch Medien wie Voice of America, Radio Free Europe oder Radio Liberty beaufsichtigt.

[9] https://surveillancevalley.com/blog/fact-checking-the-tor-projects-government-ties

Unmittelbar nach den Wahlen begannen massive Proteste, auf welche die Regierung mit Gewalt und Blockaden von Internetdiensten reagierte. Tor war mit den Bridges in der Lage, die Blockaden zu umgehen. Aber die Statistik zeigt, dass es in Weißrussland keine nennenswerte Zunahme der Nutzung von Tor während der Proteste gab. Vor, während und nach dem Höhepunkt der Proteste gab es weniger als 6.000 Tor-Clients in Weißrussland.

Signal App und Telegram konnten die Internetsperren gleichfalls umgehen und oppositionelle Telegram-Kanäle wie *Nexta* hatten zeitweise mehr als 2 Mio. Follower.

2. Kriminelle nutzen in großem Umfang Tor, um verschiedenste Formen der Kommunikation geheim zu halten. Beispielsweise verwenden Botnetze Tor, um die Kommunikation mit den C&C Servern geheim zu halten. Das bekannteste Beispiel ist das Mevade.A-Botnet. Im Sommer 2013 waren zeitweise 80–90 % der Tor-Clients Mevade.A-Bots, wie man in Abb. 12.2 sehen kann.

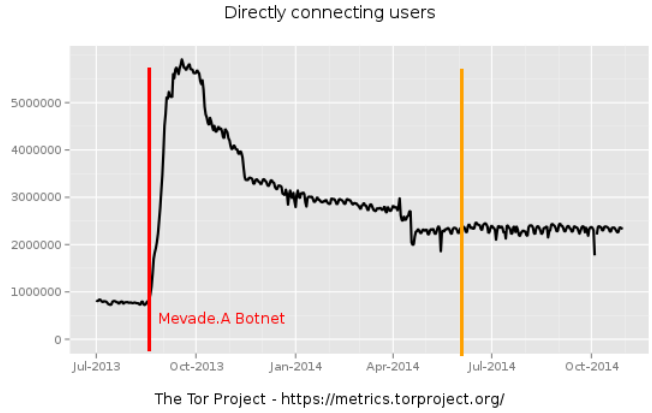


Abbildung 12.2: Mevada.A-Botnetz von metrics.torproject.org

Außerdem nutzen Drogenhändler u. a. die Technik der Tor Onion Sites (Tor-Hidden-Services), um ihre Waren anzubieten. Im Rahmen der Operation Onymous konnte das FBI mehr als 400 Drogenmarktplätze abschalten. Das FBI hatte dabei technische Unterstützung von der Carnegie Mellon Unversity bei der Deanonymisierung von Tor Onion Sites.

Die Nutzung von Anonymisierungsdiensten durch Kriminelle betrifft nicht nur Tor. Im Jahresbericht 2015 befürchten die Analysten von Europol, dass Kriminelle zukünftig das Invisible Internet Project (I2P) oder OpenBazaar statt Tor Onion Sites nutzen könnten, was die Verfolgung erschweren würde.

3. Geheimdienste nutzen Tor in erheblichem Umfang, um Kommunikation geheim zu halten. Außerdem ist Tor eine Waffe im Arsenal der CIA und des US-Cybercommand.

   Im Frühjahr 2014, auf dem Höhepunkt der Ukraine-Krise, wurde bspw. ein Botnetz in Russland hochgefahren, dass der russischen Gegenseite ernsthafte Probleme bereitet hat. In Abb. 12.3 sieht man den Anstieg der Tor-Nutzer in Russland (aber nicht international), der typisch für ein aktiviertes Botnetz ist.

   Die russische Regierung hat offiziell 4 Mio. Rubel für einen Exploit geboten, um die beteiligten Tor-Nodes zu deanonymisieren. Der russische Militärdienstleister Kalaschnikow hatte den Auftrag übernommen, konnte aber keine Ergebnisse liefern.

   Die vom Journalisten Y. Levine veröffentlichten FOIA-Dokumente belegen, das insbesondere die CIA Tor Onion Router aktiv als Werkzeug bei Kampagnen zur Destabilisierung unbequemer Länder nutzt:

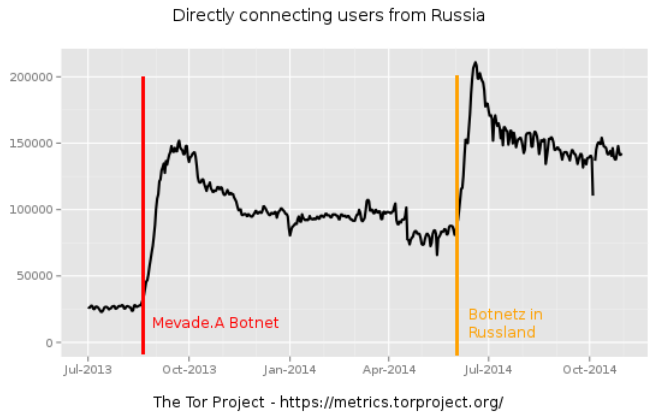


Abbildung 12.3: Botnetze mit Tor in Russland von metrics.torproject.org

> *The documents showed Tor employees taking orders from their handlers in the federal government, including hatching plans to deploy their anonymity tool in countries that the U.S. was working to destabilize: China, Iran, Vietnam, Russia.*

Die Nutzung von Tor Onion Router ist ein **Spiegel der gesellschaftlichen Probleme**:

1. Das in der UN-Menschenrechtscharta und der Europäischen Menschenrechtskonvention deklarierte Recht auf unbeobachtete private Kommunikation ist durch die staatlich organisierte Massenüberwachung und kommerzielle Datensammlungen praktisch abgeschafft. Bundesinnenminister Friedrich empfahl Selbstschutz, weil die technischen Möglichkeiten zur Ausspähung nun einmal existieren (die Bankrotterklärung der Politik), und Tor ist eine Technik zum Selbstschutz.

2. Kriminalität wie Wirtschaftskriminalität, Eigentumsdelikte, Drogenkriminalität usw. oder ganz allgemein *Handlungen im Widerspruch zu geltenden Gesetzen* sind gesellschaftliche Phänomene, für die man nicht den technischen Hilfsmitteln die Schuld geben kann.

3. Im Rahmen der erneuten Eskalation des *Kalten Krieges* wird jede Technik hinsichtlich ihrer Brauchbarkeit als Waffe geprüft. Tor war von Anfang an ein Projekt der US-Army und wird deshalb von der US-Regierung finanziert. Auf der Webseite von TorProject.org wird diese Nutzung ausdrücklich beworben. Diese Verwendung sollte auch denen klar sein, die sich als freiwillige Unterstützer an der Finanzierung eines Tor-Node beteiligen oder selbst einen Tor-Node betreiben.

Durch diese unterschiedlichen Interessen entstehen skurrile Situationen, wenn das FBI der Carnegie Mellon Unversity 1 Mio. Dollar zur Verfügung stellt, um Tor-Onion-Services für die Operation Onymous zu deanonymisieren,[10] die Universität die wissenschaftlichen Ergebnisse auf der BlackHat-Konferenz aber nicht publizieren darf,[11] um die US-Cyberoperationen in Russland nicht zu gefährden, und die Entwickler bei TorProject.org auf Vermutungen angewiesen sind,[12] um die Bugs zu fixen, damit sie politischen Aktivisten wie Wikileaks eine vertrauenswürdige Infrastruktur bereitstellen können.

[10] https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users
[11] https://web.archive.org/web/20140705114447/http://blackhat.com/us-14/briefings.html
[12] https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/

12.3.1 Security Notes

Die Sicherheit von IP-Anonymisierern wie Tor Oinion Router ergibt sich nicht alleine aus der Qualität der Software und der Kryptografie. Durch Fehler bei der Nutzung oder falsche Konfiguration kann die Anonymität komplett ausgehebelt werden.

- Auch wer in seinem Standardbrowser nur die Proxy-Einstellungen anpasst, um Tor zu verwenden, ist nicht sicher anonym. Mit WebRTC oder Java-Applets ist eine Deanonymisierung möglich. Cookies und andere Trackingfeatures können langfristig ebenfalls zu einer Deanonymisierung des Surfverhaltens führen.
- Viele Messenger verwenden *Interactive Connection Establishment* (ICE) für den Aufbau einer direkten Verbindung zwischen Clients für Audio- und Videochats. ICE ist Bestandteil von WebRTC und libjingle (XMPP). Dabei werden dem Kommunikationspartner alle verfügbare IP-Adressen (auch die öffentliche IP des Routers) zugeschickt. Via UPnP-Protokoll wird dann versucht, einen direkten Tunnel durch den Router zu bohren. Mit einem Audio- oder Videoanruf kann man also deanonymisiert werden.
- Einige nicht anonyme Peer-2-Peer-Protokolle wie BitTorrent übertragen die IP-Adresse des eigenen Rechners zusätzlich in Headern des Protokoll-Stacks, ähnlich wie bei ICE. Damit ist es ebenfalls möglich, User zu deanonymisieren. Eine wissenschaftliche Arbeit zeigte, wie 10.000 BitTorrent-Nutzer via Tor deanonymisiert werden konnten.[13]
- Der Assistent zur Einrichtung eines E-Mail-Accounts in Thunderbird umgeht die Proxy-Einstellungen beim Abrufen der Autoconfig-Datei mit den Servereinstellungen und sendet dabei die eigene E-Mail-Adresse an den Provider. Der E-Mail-Provider erhält damit die echte IP-Adresse zusammen mit der E-Mail-Adresse und man ist deanonymisiert, bevor man die erste E-Mail geschrieben oder empfangen hat.
- Softwaredownloads aus fragwürdigen Quellen können Backdoors zur Deanonymisierung enthalten, was grade beim TorBrowser regelmäßig vorkommt.

  Die Gruppe ANONYMOUS demonstrierte dies schon 2011, indem sie auf einer Webseite eine modifizierte Version des Firefox-Add-ons TorButton zum Download anboten. Dieses Add-on enthielt eine Backdoor, um die Nutzer von einigen Tor-Hidden-Services mit kinderpronografischem Material zu identifizieren. Die Liste der damit deanonymisierten Surfer wurde im Internet veröffentlicht.

  Kaspersky warnte 2022 vor einem Download, der massiv in YouTube-Videos beworben wurde, aber zwecks Deanonymisierung den Trojaner TorPoison enthielt.

  Wenn im Jahr 2022 die gesamte IT-Infrastruktur von Continental verseucht wurde, weil ein Mitarbeiter einen Browser heruntergeladen hatte, dann tippe ich auch in diesem Fall auf den TorBrowser. (Auf Computern des Arbeitgebers hat das TorBrowserBundle nichts zu suchen. Dafür kann man wegen Gefährdung der IT-Sicherheit fristlos gekündigt werden, auch wenn es keine virenverseuchte Version ist. Diese Rechtsauffassung wurde von Arbeitsgerichten bereits mehrfach bestätigt.)

Schlussfolgerungen:

- TorProject empfiehlt für anonymes Surfen ausdrücklich das TorBrowserBundle. Das ist eine angepasste Version des Browsers Mozilla Firefox zusammen mit dem Tor-Daemon.

[13] http://hal.inria.fr/inria-00574178/en/

Nur diese Konfiguration kann nach dem aktuellen Stand der Technik als wirklich sicher gelten. Die vielen Sicherheitseinstellungen dieser Softwarekombination kann man selbst nur unvollständig umsetzen.

- Für alle weiteren Anwendungen sind die Anleitungen der Projekte zu lesen und zu respektieren. Nur die von den Entwicklern als sicher deklarierten Anwendungen sollten mit Tor genutzt werden.
- Verwenden Sie ausschließlich die Originalsoftware der Entwickler.

12.3.2 Anonym Surfen mit dem TorBrowserBundle

Das TorBrowserBundle enthält einen modifizierten Firefox als Browser sowie den Tor-Daemon. Die Download-Webseite[14] stellt das TorBrowserBundle für verschiedene Betriebssysteme zur Verfügung.

Wenn die Downloadseite gesperrt ist (z. B. in Jena[15] oder in Russland[16]), dann kann man den TorBrowser auch bei Github.com[17] herunterladen. Weitere alternative Downloadmöglichkeiten erhält man per E-Mail, wenn man eine Nachricht mit dem gewünschten Betriebssystem (Windows, Linux, OSX) an gettor@torproject.org schickt.

Neben der stabilen Version des TorBrowserBundle bietet TorProject.org auch eine Alpha-Version mit neuen Features zum Testen an. Diese Versionen enthalten manchmal Features, die man sich als Anwender sehr wünscht. Dennoch sollte man für den produktiven Einsatz nur die stabile Version nutzen und warten, bis die Entwickler die neuen Features als ausreichend getestet einstufen und übernehmen. Neben den möglichen Problemen der Stabilität ist auch die Anonymität ein Grund für diese Empfehlung, da die Anonymitätsgruppe mit der stabilen Version größer ist.

Installation

Das Archiv ist nach dem Download nur zu entpacken, es ist keine weitere Installation nötig.

- Unter **Windows** öffnet man nach dem Download das sich selbst entpackende EXE-Archiv mit einem Doppelklick im Dateimanager und beantwortet die Fragen des Assistenten.

  Damit man den TorBrowser zukünftig findet und einfach starten kann, sollte man im letzten Schritt Einträge im Startmenü und auf dem Desktop anlegen lassen.

- Unter **Linux** entpackt man das Archiv mit dem bevorzugten Archiv-Manager oder erledigt es auf der Kommandozeile mit:

  ```
  > tar -xavf tor-browser-* -C $HOME
  ```

  Danach kann man das TorBrowserBundle starten, indem man das Startscript auf der Kommandozeile aufruft oder mit einem Klick im Dateimanager startet:

  ```
  > $HOME/tor-browser/start-tor-browser.desktop
  ```

[14] https://www.torproject.org/download
[15] https://kubieziel.de/blog/archives/1613-Neue-Wege,-um-den-Tor-Browser-herunterzuladen.html
[16] https://blog.torproject.org/tor-censorship-in-russia/
[17] https://github.com/torproject/torbrowser-releases/releases/

Mit einem kleinen Kommando kann man den TorBrowser im Startmenü des Desktops in der Programmgruppe *Internet* hinzufügen, um den Start zu vereinfachen:

```
> cd tor-browser
> ./start-tor-browser.desktop --register-app
```

Um den TorBrowser im **Firejail** zu starten, ruft man folgendes Kommando auf:

```
> firejail --private=~/tor-browser ./start-tor-browser.desktop
```

... oder legt sich eine Datei *tbb-firejail.desktop* mit folgendem Inhalt auf den Desktop:

```
[Desktop Entry]
Name=TorBrowser im Firejail
Exec=firejail --private=~/tor-browser ./start-tor-browser.desktop
Icon=/home/<username>/tor-browser/Browser/browser/chrome/icons/default
↪ /default48.png
Terminal=false
Type=Application
```

(Das HOME-Verzeichnis im Pfad zum Icon ist anzupassen!)

Der erste Start

Beim ersten Start öffnet sich zuerst die Startseite (Abb. 12.4). In den Tor Network Settings kann man Bridges zur Umgehung von Blockierungen des Tor-Netzwerks auswählen oder Einschränkungen der Firewall konfigurieren (wenn eine Firewall nur Verbindungen zu Port 80 und 443 erlaubt). Die Einstellungen können auch später angepasst werden.

Mit dem Button *Connect* startet man den Tor Deamon im Hintergrund – und los geht's.

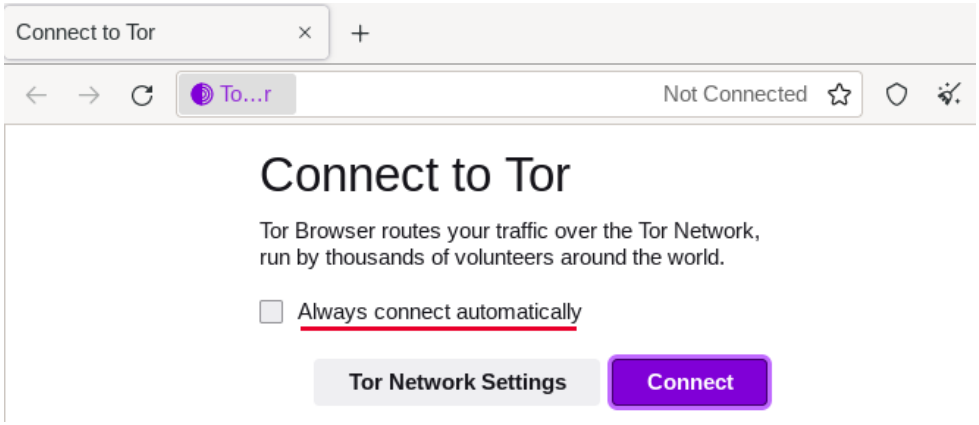


Abbildung 12.4: Start des TorBrowser

Um diesen Schritt in Zukunft zu überspringen, kann man die Option zum automatischen Verbinden beim Start aktivieren.

TorBrowser aktualisieren

Das TorBrowserBundle wird nicht mit den Updates des Betriebssystems aktualisiert, sondern lädt verfügbare Updates via Tor selbst herunter. Mit einem kleinen grünen Punkt auf dem Hamburger-Icon wird angezeigt, dass Updates verfügbar sind, die man mit einem Klick im Menü installieren kann (Abb. 12.5).

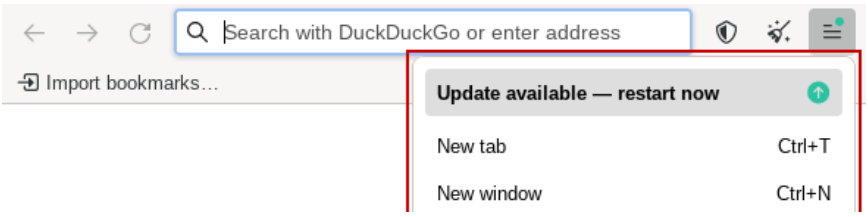


Abbildung 12.5: TorBrowser: Updates installieren

Größe des Browserfensters

Der TorBrowser startet mit einer festgelegten Größe des Browserfensters mit 1400 px Breite x N*100 px Höhe. Die Fenstergröße wird gleichzeitig als Bildschirmgröße via JavaScript bereitgestellt. Da die innere Größe des Browserfensters und die Bildschirmgröße als Tracking-Feature genutzt werden, sollte man die voreingestellte Größe des Browserfensters **nicht(!)** ändern.

Sicherheitseinstellungen

Die folgenden Beispiele für erfolgreiche Angriffe beziehen sich auf das FBI, weil es darüber Berichte gibt. Es sind aber nur Beispiele (nicht nur NSA und FBI haben fähige Hacker). *Rule 41 of the US Federal Rules of Criminal Procedure*[18] erlaubt dem FBI seit Dezember 2016 das massenweise Hacken von Tor- und VPN-Nutzern, unabhängig davon, in welchem Land die Tor-Nutzer sich befinden.

1. 2016 wurde auf der Tor-Mailingliste[19] ein Javascript-Bug gepostet, den das FBI aktiv mit Exploits ausnutzte, um einen Trojaner zu installieren, der Tor-Nutzer deanonymisiert. Der Einsatz wurde auf der vom FBI beschlagnahmten Onion-Site *Giftbox* nachgewiesen.[20]

2. 2015 verwendete das FBI einen Zero-Day-Exploit im TorBrowser, um einen Trojaner zu installieren und die Tor-Nutzer damit zu deanonymisieren. Welche Lücke im Firefox dabei ausgenutzt wurde, ist nicht bekannt. Mozilla und TorProject.org haben sich bemüht, aber die Informationen zur ausgenutzten Lücke wurden unter Hinweis auf die Nationale Sicherheit als geheim eingestuft.[21]

3. Im Sommer 2013 wurden tausende Tor-Nutzer mit dem FBI-Trojaner *Magneto* infiziert. Der Exploit zur Installation des Trojaners nutzte einen JavaScript-Bug im TorBrowser aus. Der installierte Trojaner sendete die IP-Adresse, die MAC-Adresse und den Namen des Rechners an einen FBI-Server, um Tor-Nutzer zu deanonymisieren.[22]

[18] https://blog.torproject.org/blog/day-action-stop-changes-rule-41
[19] https://lists.torproject.org/pipermail/tor-talk/2016-November/042639.html
[20] https://motherboard.vice.com/en_us/article/9a3mq7/tor-browser-zero-day-exploit-targeted-dark-web-child-porn-site-giftbox
[21] https://motherboard.vice.com/read/the-fbi-is-classifying-its-tor-browser-exploity
[22] http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/

4. Aus den Snwoden-Dokumenten geht hervor, dass die NSA das TorBrowserBundle auf Basis von Firefox 10 ESR über einen Bug in E4X, einer XML-Extension für JavaScript, automatisiert angreifen und Nutzer deanonymisieren konnte.[23]

Die Tor-Entwickler haben den Tradeoff zwischen einfacher Benutzbarkeit und Sicherheit in den Default-Einstellungen zugunsten der einfachen Benutzbarkeit entschieden. Es wird aber anerkannt, dass diese Einstellungen ein Sicherheitsrisiko sind. In den FAQ steht:

> *There's a tradeoff here. On the one hand, we should leave JavaScript enabled by default so websites work the way users expect. On the other hand, we should disable JavaScript by default to better protect against browser vulnerabilities (not just a theoretical concern!).*

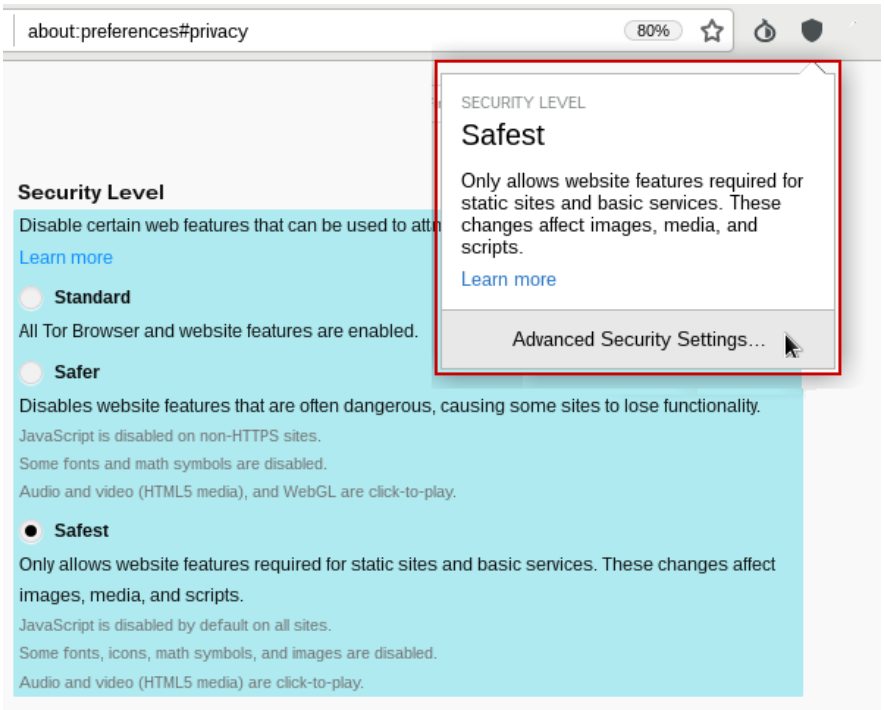


Abbildung 12.6: Sicherheitslevel im TorBrowser anpassen

Beim Start wird man darauf hingewiesen, dass man die Sicherheitseinstellungen anpassen kann. TorBrowser startet standardmäßig mit dem niedrigsten Sicherheitslevel *Standard*, um das Surferlebnis möglichst wenig einzuschränken.

Für sicherheitsbewusste Nutzer ist der umgekehrte Weg empfehlenswert. Man kann standardmäßig im höchsten Sicherheitslevel *Safest* surfen und wenn es ein Login bei einer Webseite erfordert, auf den mittleren Level *Safer* wechseln. Fast alle Websites, die einen Login erfordern (E-Mail-Provider u. Ä.), kann man mit dem Level *Safer* problemlos nutzen.

Um den Sicherheitslevel anzupassen, klickt man auf das Symbol mit dem Schild (2. Symbol rechts neben der URL-Leiste) und in dem ausklappenden Menü auf *Advanced Security Settings*. Im Browser wird dann die Seite mit den Einstellungen geöffnet.

[23] http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

Die Überwachungsdichte und die Aggressivität der Angreifer ist im Tor-Netzwerk viel höher als im normalen Internet. Daher sollte man auch die erforderlichen Schutzmaßnahmen deutlich höher ansetzen als bei einem normalen Browser.

Suchmaschinen im TorBrowser

Standardmäßig verwendet der TorBrowser die Suchmaschine DuckDuckGo mit Default-Einstellungen. Die Suchanfragen werden via GET-Request gesendet, die moderate Filterung der Suchergebnisse ist aktiv und aufgrund der Einschränkungen bei den Fonts ist die Darstellung suboptimal.

Auf der Webseite des Privacy-Handbuches zum TorBrowser https://www.privacy-handbuch.de/handbuch_24a.htm kann man mit Klick der rechten Maustaste in die URL-Leiste Alternativen für die Websuche installieren.

Abbildung 12.7: Suchmaschinen im TorBrowser hinzufügen

- **DuckDuckGoOnion (PrHdb)** und **DuckDuckGo (Deutsch)** deaktivieren die moderate Filterung der Suchergebnisse, senden die Anfragen datenschutzfreundlicher via POST-Request, deaktivieren das Laden der Favicons der Webseiten, öffnen die Links in einem neuen Tab und verwenden die Noto-Fonts des TorBrowsers für bessere Lesbarkeit der Ergebnisseite.
- **Qwant (Deutsch)** und **Qwant Lite (Deutsch)** (JavaScript-frei) deaktivieren ebenfalls die standardmäßig aktive moderate Filterung sowie das Laden der Favicons, öffnen Links in einem neuen Tab und aktivieren Deutsch als Sprache der Webseite.
- Auf den Webseiten von anderen Suchmaschinen wie AHMIA (Suchmaschine für Onion-Services) kann man mit Rechtsklick in der URL-Leiste weitere Such-Plugins installieren.

In den Einstellungen des TorBrowsers kann man dann die Standardsuchmaschine wählen.

AdBlocker und Trackingschutz

Der TorBrowser enthält keinen AdBlocker und alle Trackingschutz-Features von Firefox sind vollständig deaktiviert. Es ist das Konzept des TorBrowser, Werbung und Trackingscripte nicht zu blockieren, sondern durch Anonymität die Privatsphäre zu gewährleisten.

- Das Anonymitätskonzept des TorBrowser verhindert, dass Nutzer individuell erkannt und beim Surfen verfolgt werden können.
- Viele Webseiten finanzieren sich durch Werbung. TorProject.org möchte in diesem Punkt keine Konfrontation, um die Akzeptanz des Browsers nicht zu belasten.

Es ist empfehlenswert, dem Konzept von TorProject.org zu folgen. Ein AdBlocker ist leicht erkennbar und unterschiedliche Filterlisten könnten als Merkmal für das Fingerprinting dienen. Es ist nahezu unmöglich, eine Anonymitätsgruppe mit identischen Filterlisten aufzubauen.

Cookies und EverCookies

Um Tackingcookies und EverCookies muss man sich beim TorBrowser keine Gedanken machen. Das von den Entwicklern umgesetzte Sicherheitskonzept *Cross-Origin Identifier Unlinkability* schützt zuverlässig gegen Tracking und Deanonymisierung mit Cookies oder EverCookies, ohne das Surferlebnis nennenswert zu beeinträchtigen.

- Für jede aufgerufene Domain wird automatisch ein Surf-Container erstellt. Dieser Container enthält in einer abgeschotteten Umgebung alle Daten, die von einer Website lokal im Browser gespeichert werden (Cookies, HTML5-Storage, IndexedDB, Cache, TLS-Sessions usw.). Diese Daten bilden dann den sogenannten *Context*.
- Der Zugriff auf Daten in einem anderen *Context* bzw. in einem anderen Surf-Container ist nicht möglich. Somit werden in den verschiedenen *Contexten* unterschiedliche Tracking-Markierungen gesetzt, wenn man unterschiedliche Domains aufruft.
- Beim Neustart oder wenn man den Button *Neue Identität* der in der Toolbar wählt, werden alle Container gelöscht. Für eine *Neue Identität* wird außerdem eine neue Route durch das Tor-Netzwerk mit einem anderen Tor-Exit-Node genutzt.

Man sollte dem Anonymitätskonzept des TorBrowser folgen und gelegentlich alle Cookies und anderen lokalen Daten löschen, indem man auf die Zwiebel neben der URL-Leiste klickt und *Neue Identität* wählt. Insbesondere nach einem Login auf einer Webseite ist es empfehlenswert, die Spuren zu beseitigen.

PDFs und andere Dokumente

Auf der Downloadseite des TorBrowserBundle findet man unten einige Sicherheitshinweise,[24] unter anderem zu PDFs und anderen Dokumenten:

> ***Don't open documents downloaded through Tor while online***
>
> *You should be very careful when downloading documents via Tor (especially DOC and PDF files) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP!*
>
> ***If you must work with DOC and/or PDF files, we strongly recommend either using a disconnected computer**, downloading the free VirtualBox and using it with a virtual machine image with networking disabled, or using Tails.*

[24] https://www.torproject.org/download/download

PDFs und andere Office-Dokumente können Trackingwanzen enthalten, die beim Öffnen des Dokumentes von einem Server geladen werden. Wenn man sie in einem PDF-Reader öffnet, während man online ist, dann kann man deanonymisiert werden. Standardmäßig öffnet TorBrowser PDFs im eigenen Viewer PDF.js. Damit sollte man zwar nicht deanonymisiert werden können, aber der Server kann zumindest das Öffnen des Dokumentes registrieren, auch nicht schön. Außerdem gibt es immer wieder Bugs in Mozillas PDF.js, die für einen Exploit genutzt werden können (z. B. mfsa2015-69 vom Juli 2015).

Um nicht immer daran denken zu müssen, mit der rechten Maustaste auf einen PDF-Link zu klicken und *Speichern unter...* zu wählen, kann man die Einstellung im TorBrowser für PDF-Dokumente ändern und auf *Speichern* setzen.

Die via Tor heruntergeladenen Dokumente kann man in einem besonderen Ordner speichern. Dann behält man den Überblick und weiß, dass man diese Dokumente nur öffnen darf, wenn man den Netzwerkstecker gezogen hat oder die WLAN-Verbindung ausgeschaltet wurde.

Hinweis: Man kann heruntergeladene PDF-Dateien von Wanzen säubern, indem man sie auf einem Rechner ohne Internetverbindung in einem PDF-Viewer öffnet und in eine neue PDF-Datei ausdruckt. Dabei werden sichtbare Fotos neu gerendert und unsichtbar eingebettete Wanzen entfernt.

12.3.3 Tor Onion Router für Android Smartphones

TorBrowser für Android wird von TorProject.org entwickelt und ist wie die Desktop-Version eine Kombination aus sicher konfiguriertem Browser und Tor Onion Router.

Wie beim TorBrowserBundle kann man auf Android zwischen drei Sicherheitsstufen wählen. Diese Option versteckt sich in den Einstellungen im Bereich *Datenschutz und Sicherheit*.

Standardmäßig ist der niedrigste Sicherheitslevel aktiv, weil es damit die wenigsten Probleme beim Surfen gibt. Mit dem mittleren Level funktioniert aber auch noch fast alles. Es sind einige Funktionen wie WebGL deaktiviert und Audio-/Videomedien werden nicht mehr automatisch abgespielt.

In der höchsten Sicherheitsstufe wird auch Javascript deaktiviert und das Internet ist damit nur schwer erträglich, nur für besonders hohe Sicherheitsanforderungen nötig.

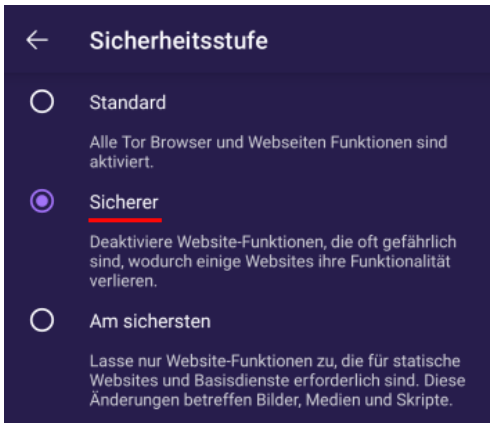


Abbildung 12.8: TorBrowser für Android: Sicherheitslevel für eine Webseite anpassen

OrBot ist der offizielle Tor-Client für Android. Er kann den Datenverkehr für alle oder einzelne Apps über das Tor-Netzwerk leiten und damit die IP-Adresse verstecken könnte.

Sicherheitshinweis: Viele Apps senden umfangreiche Daten an Werbenetzwerke und an die Anbieter der Dienste. Die Daten enthalten in der Regel eine eindeutige Tracking-ID, außerdem werden auch Standortdaten und weitere Informationen versendet. Das betrifft die Apps von Facebook und Twitter, verschiedene Dating-Apps, einfache Wetter-Apps und auch die App zur Mediathek des ZDF.

Diese Datensammlungen durch integrierte Trackingfunktionen in den Apps **heben die Anonymität vollständig auf**. Trotz Anonymisierung der IP-Adresse durch Verwendung von OrBot gibt es damit keine Anonymität bei der Nutzung dieser Apps.

Es gibt nur sehr wenige Apps, die in Kombination mit OrBot für anonyme Kommunikation geeignet sein könnten. Aber selbst für diese wenigen Apps gibt es keine Audits durch das Team von TorProject.org, ob die Anonymisierung wie gewünscht funktioniert.

Beide Apps können via Google Play Store oder F-Droid installiert werden. Bei F-Droid muss man in den Einstellungen das Repository vom *Guardian Projekt* als zusätzliche Paketquelle aktivieren.

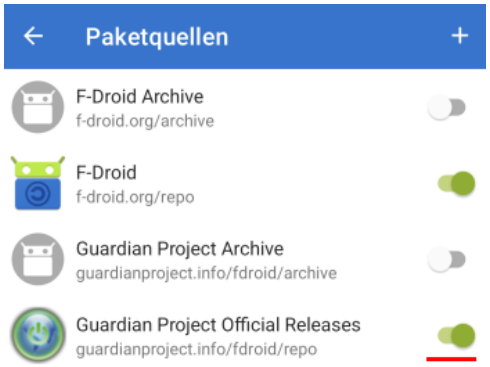


Abbildung 12.9: Repository für Guardian Project in F-Droid aktivieren

12.3.4 OnionBrowser für iPhones

Der OnionBrowser von Mike Tigas ist die von TorProject.org empfohlene App für anonymes Surfen auf dem iPhone. Im Gegensatz zum TorBrowserBundle ist der Tor Daemon nicht(!) im OnionBrowser enthalten. Die App OrBot muss zusätzlich installiert werden.

Beim ersten Start nach der Installation fragt der OnionBrowser, ob er sich direkt mit dem Tor-Netzwerk verbinden soll oder ob Bridges genutzt werden sollen, weil der Zugang zum Tor-Netzwerk zensiert wird. Bridges sind ein Extra-Thema und in Europa nicht nötig. Danach wird abgefragt, welcher Sicherheitslevel standardmäßig genutzt werden soll.

- Wenn man den höchsten Level *Gold* wählt, dann macht das Surfen keinen Spaß, weil Javascript komplett verboten wird und viele Webseiten damit unbenutzbar werden.
- Im Level *Silber* ist Javascript für HTTPS-verschlüsselte Webseiten erlaubt, aber es sind einige Techniken wie XHR, Websockets, WebRTC und Videos verboten.
- Den *Bronze* Level sollte man nicht nutzen, weil er wirklich unsicher ist. Es ist aber der einzige Level, mit dem YouTube-(oder Youporn-)Videos funktionieren.

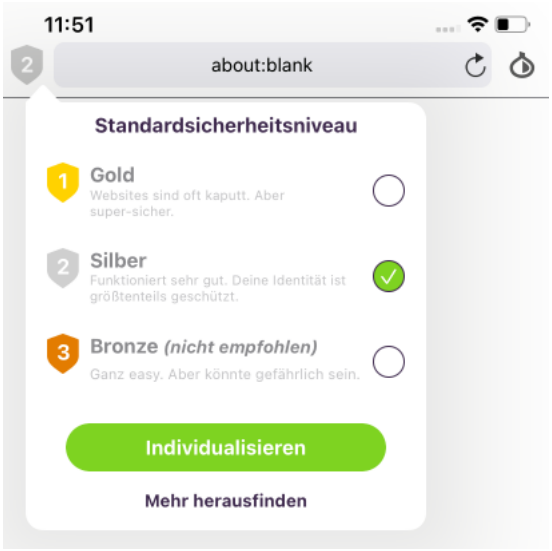


Abbildung 12.10: OnionBrowser: Sicherheitslevel für eine Webseite anpassen

Mit einem Klick auf das Icon oben links kann man den Sicherheitslevel definieren.

Die Buttons zur Verwaltung der Tabs, Lesezeichen und Einstellungen findet man wie üblich unten in der Fußzeile. Der OnionBrowser verwendet standardmäßig den Onion-Service von DuckDuckGo als Suchmaschine. In den Einstellungen kann man auch Startpage.com oder Google (???) als Suchmaschine wählen. Außerdem kann man in den TLS-Einstellungen die veralteten, unsicheren Protokolle TLS 1.0 und TLS 1.1 abschalten.

12.3.5 Sicherheitskonzept für hohe Ansprüche

Tor Onion Router schützt den Datenverkehr auch gegen Angriffe potenter Geheimdienste wie die NSA. Nach dem aktuellen Stand der Technik ist es nahezu unmöglich, die Verschlüsselung mathematisch zu brechen und Nutzer zu deanonymisieren.

Angriffe zur Deanonymisierung von Tor-Nutzern konzentrieren sich daher üblicherweise auf die Client-Anwendung (z. B. den Webbrowser). In mehreren bekannten Fällen wurde durch Ausnutzung von Security-Bugs im TorBrowser ein kleiner Trojaner auf dem Rechner von Zielpersonen installiert, der IP- und MAC-Adressen des Rechners ermittelt und an einen Server des Angreifers sendet.

Das FBI verwendet seit mehreren Jahren den Trojaner *Magneto*, der auf Webseiten platziert wird und nach Infektion des Systems via TorBrowser die Daten an einen Server der *Science Applications International Cooperation* sendet, die u. a. mit dem FBI kooperiert.

- Der Server des Projekts *Freedom Hosting* wurde vom FBI in Frankreich lokalisiert und in Kooperation mit dem Datacenter wurde vor Ort ein direkter Zugriff eingerichtet.

  Der Magneto-Trojaner wurde in mehrere Onion-Sites eingebaut und die Besucher wurden deanonymisiert. Neben Webangeboten mit kinderpornografischem Material waren auch der E-Mail-Service TorMail und die Bitcoin-Börse OnionBank betroffen (2013).[25]

[25] https://www.wired.com/2013/09/freedom-hosting-fbi/

- Der Onion-Service *Playpen* zur Verteilung von KiPo wurde vom FBI übernommen und noch zwei Wochen weiter betrieben. In dieser Zeit wurde der Trojaner auf der Webseite platziert und 8.700 Besucher aus 120 Ländern wurden deanonymisiert (2015).
- Auch der Onion-Service *Giftbox* wurde vom FBI übernommen. Wie üblich wurde der Trojaner installiert und die Besucher wurden deanonymisiert (2016).[26]

Bei den Beispielen ging es um echt schmutzige Dinge, die in Gerichtsverhandlungen bekannt wurden und mit denen das FBI seine Erfolge feierte. Rein technisch gesehen kann jedoch nicht nur das FBI solche Angriffe durchführen, sondern auch andere potente Angreifer sind dazu fähig.

Es gibt mehrere Lösungen zu Nutzung von Tor Onion Router (nicht nur das TorBrowserBundle), die unterschiedlich robust gegen die Deanonymisierung durch Trojaner sind:

1. Das *TorBrowserBundle* auf einem normalen PC oder Smartphone kann durch Standardtrojaner des FBI und anderen potenten Angreifern deanonymisiert werden, indem der Trojaner den Browser exploitet und Zugang zum OS auf User Level bekommt (siehe oben).
2. Die *Tor Live-DVD TAILS* leitet standardmäßig den gesamten Datenverkehr auf Systemebene durch Tor. Ein Angreifer muss nicht nur den Browser (oder eine andere Anwendung) mit dem Trojaner exploiten, sondern zusätzlich mit weiteren Exploits root Rechte erlangen, um die Schutzmaßnahmen von TAILS umgehen und den Nutzer deanonymisieren zu können.

   Das ist nicht unmöglich, wie ein Fall 2020 demonstrierte, bei dem das FBI eine Schwachstelle in Videocodecs ausnutzte, um mit einem Trojaner root Rechte in TAILS zu erlangen.[27]

   Da der TorBrowser im höchsten Sicherheitslevel keine Videos abspielt, musste das Target auch noch dazu überredet werden, das kompromittierte Video im Videoplayer aufzurufen.

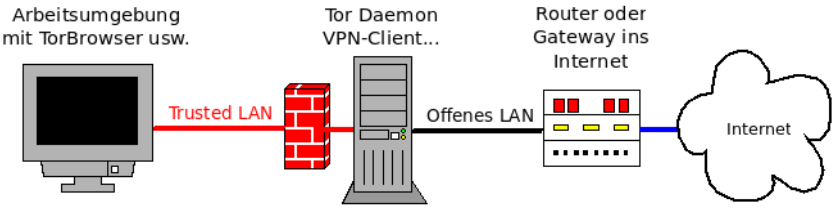
   Der Angriff war sehr teuer, ist nicht massentauglich und war ein (schmutziger) Einzelfall.
3. Das Sicherheitskonzept von *Whonix-Tor-VMs* erfordert es, nach Exploiten einer Anwendung (z.B. TorBrowser) und dem Erlangen von root Privilegien noch einer weitere Hürde zu überwinden. Der Angreifer muss danach noch aus der virtualisierten Arbeitsumgebung ausbrechen, um vom Hostsystem aus den Whonix Nutzer zu deanonymisieren.
4. Die ultimative Tor Festung erhält man, wenn man für die Arbeitsumgebung und die Verschlüsselung des Datenverkehrs unterschiedliche Hardware nutzt, wobei der Aufbau eines solchen Konstruktes nicht trivial ist.

   Man könnte die Designdokumente von Whonix als Vorlage nehmen und das Konzept von zwei virtuellen Maschine auf echte Hardware übertragen. Es gibt wahrscheinlich nur wenige Bedrohungsszenarien, die das erfordern könnten. Eine solche Festung müsste in ein sinnvolles Gesamtkonzept intergriert werden mit hochsicherer Festplattenverschlüsselung... usw.

Wenn **hohe Sicherheitsanforderungen** gestellt werden, muss die Verschlüsselung des Datenverkehrs mit dem Tor-Daemon (oder einem VPN-Client) in einer Umgebung erfolgen, die von der/den Arbeitsumgebung(en) mit den Internet-Anwendungen getrennt ist.

[26] https://www.vice.com/en/article/9a3mq7/tor-browser-zero-day-exploit-targeted-dark-web-child-porn-site-giftbox

[27] https://www.vice.com/en/article/v7gd9b/facebook-helped-fbi-hack-child-predator-buster-hernandez



Arbeitsumgebung(en) stellen die Anwendungen wie TorBrowser, E-Mail-Client, Messenger usw. dem Nutzer zur Verfügung. Es sind mehrere Arbeitsumgebungen möglich.

In den Arbeitsumgebungen wird für Anwendungen, die Verbindungen ins Internet aufbauen dürfen, sowie für System-Updates ein SOCKS5-Proxy konfiguriert (Proxy: Tor-Daemon). Es wird aber KEIN globaler Proxy gesetzt, um unerwünschte Verbindungen zu vermeiden.

Trusted LAN ist ein gekapseltes Netz, welches keine direkte Verbindung ins Internet oder in andere lokale Netzwerke ermöglicht. Es gibt keine Gateways in andere Netze!

Die Firewall sorgt dafür, dass nur zulässige Daten den Tor-Daemon erreichen. Bei der Nutzung von Tor Onion Router darf nur TCP-Traffic die Firewall passieren, der direkt an die *SocksPorts* des Tor Daemon adressiert ist.

Der Tor Server (non-Exit Tor Node) ist als Tor-Relay-Node (non-Exit) mit limitierter Bandbreite (für Cover-Traffic) konfiguriert und verschlüsselt alle Daten, die aus dem *Trusted LAN* kommen und ins Internet fließen sollen. Aus den Arbeitsumgebungen gibt es keinen Weg daran vorbei.

Ein kleines Konfigurationsbeispiel mit den Optionen für einen non-Exit Tor Node:

```
# Tor Client für Arbeitsumgebungen
SocksPort <Trusted-LAN-IP>:9050

# Tor Relay für Cover Traffic
Address <IP> oder <DynDNS>
Nickname <frei wählbar>

ORPort 9001
DirPort 9030

ExitPolicy reject *:*

# Limits für Bandbreite (anpassen)
RelayBandwidthRate 500 KB
RelayBandwidthBurst 800 KB
AccountingMax 1024 GB
AccountingStart month 1 00:00

ContactInfo Max Mustermann <max@mustermann.tld>
```

Wenn man beim Angreifermodell davon ausgeht, dass die Arbeitsumgebungen kompromittiert werden könnten, darf man den Arbeitsumgebungen keinen Zugriff auf den Tor-*ControlPort* geben (nur SocksPorts!). Es gibt einige Control-Kommandos, welche die Anonymität gefährden können. Zur Vereinfachung der Tor-Server-Administration könnte man den *ControlPort* lokal freischalten:

```
# für lokale Admin-Tools
ControlPort 127.0.0.1:9051
CookieAuthentication 1
CookieAuthFile /var/lib/tor/control_auth_cookie
CookieAuthFileGroupReadable 1
DataDirectoryGroupReadable 1
```

StreamIsolation ist ein weiteres Feature, das man aktivieren kann. Für Internet-Anwendungen mit Login-Kennung werden mehrere SocksPorts zur Verfügung gestellt. Der Traffic für diese Ports wird isoliert und über unterschiedliche Routen durch das Tor-Netz geleitet, um eine Deanonymisierung durch Korrelationen zu vermeiden.

```
# SocksPort mit StreamIsolation
SocksPort <Trusted-LAN-IP>:9101 IsolateDestAddr IsolateDestPort
SocksPort <Trusted-LAN-IP>:9102 IsolateDestAddr IsolateDestPort
SocksPort <Trusted-LAN-IP>:9111 IsolateDestAddr
SocksPort <Trusted-LAN-IP>:9112 IsolateDestAddr
```

Für den TorBowser wird StreamIsolation NICHT empfohlen, aber Thunderbird könnte z. B. Port 9101 verwenden, ein Messenger Port 9111, wget den Port 9112 usw.

Der Router braucht evtl. einen DynDNS-Namen und ein Port-Forwarding für den konfigurierten ORPort und den DirPort des Tor-Daemon (für den Cover Traffic).

Wenn eine Arbeitsumgebung kompromittiert wird, kann der Angreifer nur IP-Adressen aus einem privaten Netzwerkbereich ermitteln und den Nutzer nicht deanonymisieren.

Möglicherweise könnte ein Angreifer mit einem Trojaner zur Online-Durchsuchung persönliche Daten wie Kontonummern oder Kreditkartennummern o. Ä. finden, die zur Deanonymisierung führen können? Darüber muss man selbst nachdenken!

Auch die beste Technik kann nicht vor Fehlern beim eigenen Verhalten schützen. So wurde Ross Ulbricht 2011 als Betreiber des Darknet-Markplatzes *Silk Road* identifiziert, weil er in einem Forum Werbung für sein Projekt postete und dabei eine Bitcoin-Adresse angab. Durch Analyse der Blockchain wurden weitere Bitcoin-Adressen ermittelt, die zu einer Bitcoin-Börse führten, wo er eine GMail-Adresse mit seinem realen Namen angegeben hatte. (Wieder so ein schmutziges Beispiel. Falls jemand bessere Beispiele hat, gerne weiterleiten.)

Warum ist Cover-Traffic sinnvoll? Ein Beispiel: Es gab einen Studenten, der eine Bombendrohung per E-Mail an seine Universität sendete. Die *Sender-IP* im Header E-Mail verwies auf einen Tor-Exit-Node. Das Log des zentralen HTTP-Proxys der Universität zeigt nur eine Verbindung ins Tor-Netzwerk, die aus der Bibliothek der Universität kam. In der Bibliothek nutzte zum fraglichen Zeitpunkt nur ein einziger Student das Uni-Netz – FAIL.

12.3.6 Whonix-Tor-VMs

Whonix setzt das Konzept für hohe Sicherheitsansprüche bei der Nutzung von Tor Onion Router für den Hausgebrauch mit virtuellen Maschinen um. Eine virtuelle Maschine (VM) ist einfach gesagt ein kleiner, gekapselter Computer im Computer mit eigenen Dateien, Betriebssystem usw., der von einer Virtualisierungsumgebung bereitgestellt wird.

Whonix stellt zwei vorbereitet virtuelle Maschine bereit:

1. Die virtuelle Maschine **Gateway** enthält den Tor-Daemon, der die Verbindung zum Tor-Netzwerk herstellt und den Datenverkehr verschlüsselt ins Internet schickt.
2. Die virtuelle Maschine **Workstation** enthält alle Programme zur Internetnutzung (Tor-Browser, Thunderbird, OnionShare usw.). Diese VM kommuniziert ausschließlich mit dem Tor-Gateway und hat keine direkte Verbindung zum Internet. Jeder Datenverkehr, der diese VM verlässt, wird vom Tor-Daemon in der Gateway-VM verschlüsselt und durch das Tor-Netzwerk gejagt.

Um Whonix zu nutzen, muss man zuerst **VirtualBox**[28] als Virtualisierungsumgebung installieren. Dann kann man die beiden Whonix-VMs herunterladen, im VirtualBox-GUI importieren und starten. Die Whonix-Dokumentation erklärt die einzelnen Schritte.[29]

Hinweise für einige Linux-Distributionen

Qubes Whonix ist eine speziell angepasste Version für die Linux-Distribution QubesOS, welche neben der Trennung zwischen Arbeits-VM und Tor-VM mit einer disposable Arbeits-VM auch die Vorteile einer Live-DVD bietet, die keine Veränderungen oder Spuren der Nutzung speichert. Qubes Whonix steht als Templates zur Verfügung und wird in der *dom0* installiert:

1. Zuerst der Download der Templates *whonix-gw* und *whonix-ws*:

```
> qvm-template --enablerepo=qubes-templates-community install
↪  whonix-gw-17
> qvm-template --enablerepo=qubes-templates-community install
↪  whonix-ws-17
```

2. Dann werden die VMs auf Basis der Templates initialisiert:

```
> sudo qubesctl state.sls qvm.anon-whonix
```

3. Zusätzlich kann man eine disposable Arbeits-VM initialisieren:

```
> sudo qubesctl state.sls qvm.whonix-ws-dvm
```

Debian 10/11 bietet i. d. R. keine brandaktuelle Software. Das gilt auch für VirtualBox. Debian Fast Track ist ein Repository, das aktualisierte Software enthält und auch für VirtualBox eine aktuellere Version bietet. Außerdem benötigt man die Backports.

1. Die Repositorys kann man wie folgt in der Datei */etc/apt/sources.d/* hinzufügen:

```
deb https://fasttrack.debian.net/debian/ bullseye-fasttrack main
↪  contrib
deb https://fasttrack.debian.net/debian/
↪  bullseye-backports-staging main contrib
```

   (Falls es Probleme mit HTTPS gibt, sollte man *apt-transport-https* installieren.)

2. Dann installiert man noch die PGP-Schlüssel vom Fasttrack-Repository:

```
> sudo apt install fasttrack-archive-keyring
```

3. Dann kann man VirtualBox und optional das Extension Pack installieren:

[28] https://www.virtualbox.org/wiki/Downloads
[29] https://www.whonix.org/wiki/Documentation

```
> sudo apt update
> sudo apt install virtualbox
> suod apt install virtualbox-ext-pack
```

Debian, Ubuntu, Fedora und RHEL können neben der Open-Source-Edition von VirtualBox aus den Repositorys auch eine kostenfreie Version von Oracle installieren.[30]

12.3.7 Anonyme E-Mail-Accounts

Es ist wenig sinnvoll, einen bisher ganz normal genutzten E-Mail-Account plötzlich anonym zu nutzen. In den letzten Monaten haben sich genug Daten angesammelt, die die Identifizierung des Nutzers ermöglichen. Der erste Schritt sollte also die Einrichtung eines neuen E-Mail-Accounts sein, der ausschließlich via Tor Onion Router genutzt wird.

Dieser neue E-Mail-Account sollte NICHT für den tagtäglichen E-Mail-Kleinkram genutzt werden, sondern nur für eine bestimmte Aufgabe, die Anonymität erfordert. Anhand der Kommunikationsdaten ist anderenfalls eine Deanonymisierung möglich, bspw. wenn die Bank oder ein Onlinehändler E-Mails mit der vollen Anrede und Adresse senden. Anonyme Kommunikation und Alltagskommunikation sollten immer streng getrennt sein.

Bei der anonymen Nutzung von E-Mail-Accounts müssen zwei Anforderungen erfüllt sein:

1. Anonymität: Es dürfen keine Lücken bei der Anonymisierung bestehen.
2. Sicherheit: Verschlüsselung mit OpenPGP sollte möglich sein.

Derzeit gibt es keinen E-Mail-Client, der für die Nutzung mit Tor von TorProject.org überprüft und für gut befunden wurde. Die eigenmächtige Nutzung einer Anwendung mit Tor als SOCKS5-Proxy ohne qualifizierte Prüfung durch Experten ist nicht ratsam, wie Thunderbird oder diverse Jabber-Clients zeigen. Anonymität ist damit nicht gesichert.

Mit dem TorBrowser das Webinterface des E-Mail-Providers nutzen

Eine Alternative ist die Nutzung des Webinterfaces eines E-Mail-Providers mit dem TorBrowser. Dabei sollte der E-Mail-Provider einen Tor-Onion-Service oder vergleichbare Lösungen anbieten, um die Gefahren durch Bad Exit Nodes zu reduzieren.

Die Verwendung eines Browsers erschwert die Verschlüsselung der E-Mails mit OpenPGP. Man könnte irgendwie versuchen, die Inhalte der E-Mails mit Copy/Paste zu verschlüsseln und zu entschlüsseln, wie bei der Verschlüsselung in Webformularen beschrieben, aber das macht keinen Spaß. Besser ist es, wenn der E-Mail-Provider OpenPGP im Webinterface unterstützt.

Die im Kapitel *E-Mail-Kommunikation* allgemein empfohlene Nutzung von POP3 zum Abrufen der E-Mails sowie die lokale Speicherung sind damit unmöglich. Die Mails müssen auf dem Server des Providers verwaltet und sollten daher möglichst verschlüsselt gespeichert werden.

- **Empfehlung:** ProtonMail bietet einen Tor-Onion-v3-Service incl. Verschlüsselung mit OpenPGP im Webinterface und verschlüsselte Speicherung von E-Mails/Adressbuch unter:

  https://account.protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion/login

[30] https://www.virtualbox.org/wiki/Linux_Downloads

  - Wenn man bei Protonmail einen neuen E-Mail-Account via TorBrowser erstellen und nutzen möchte, muss man im TorBrowser den Sicherheitslevel *Safer* wählen.
  - Bei der Registrierung muss eine E-Mail Adresse zur Verifikation angeben werden. Man kann temporäre Wegwerfadressen verwenden, die man ebenfalls via Torbrowser anfordert. Es kann vorkommen, das eine Wegwerf-E-Mail Domain bei Proton blockiert wird. Wenn eine E-Mail Adresse abgelehnt wird, kann man nacheinander mehrere temp. E-Mail Adressen von unterschiedlichen Anbietern probieren.
  - Nach dem ersten Login sollte man im Dashboard alle E-Mail Subscriptions deaktivieren. Die Häufung nichtzustellbarer Mails aus den Subscriptions an temp. Adressen führt zur Sperrung des Anbieters temporärer E-Mail Adressen bei Proton.

- Als **Alternative** könnte man auch mailbox.org für die anonyme Nutzung mit dem TorBrowser empfehlen, wenn man die angebotenen Features aktiviert:
  - Der Tor-Node von mailbox.org kann ähnlich wie ein Onion-Service mittels MapAddress-Konfiguration verwendet werden. Dafür muss man im Installationsverzeichnis des TorBrowsers die Datei *Browser/TorBrowser/Data/Tor/torrc* mit einem Texteditor öffnen und folgende Einträge am Ende hinzufügen:

    ```
    MapAddress mailbox.org
    ↪ mailbox.org.85D4088148B1A6954C9BFFFCA010E85E0AA88FF0.exit
    MapAddress *.mailbox.org
    ↪ *.mailbox.org.85D4088148B1A6954C9BFFFCA010E85E0AA88FF0.exit
    ```
  - OpenPGP-Verschlüsselung kann im Webinterface aktiviert werden. Allerdings ist mailbox.org Guard nicht für hohe Sicherheitsanforderungen geeignet, sondern bietet nur *hinreichende* Sicherheit, wie mailbox.org in den FAQ schreibt.
  - Das verschlüsselte Postfach sorgt für die verschlüsselte Speicherung der E-Mail-Inhalte auf dem Server. Das Feature muss in den Einstellungen aktiviert werden.
  - Ein verschlüsseltes Adressbuch gibt es nicht. Deshalb sollte man die automatische Sammlung von Adressen in den Einstellungen deaktivieren. Die Optionen findet man in den Einstellungen unter *E-Mail*.
  - Anonyme Bezahlung ist per Cash (Brief oder Überweisung) möglich.

- Es gibt weitere E-Mail-Provider, die die Voraussetzungen erfüllen. Die Liste ist nicht abschließend sondern soll einige Hinweise geben, worauf man achten kann.

E-Mail-Accounts mit der Tor-Live-DVD TAILS verwalten

Die Tor-Live-DVD TAILS ermöglicht die Verwendung von Thunderbird zur Verwaltung anonymer E-Mail-Accounts. Die Live-DVD enthält einen modifizierten Thunderbird, der die Features von dem Add-on TorBirdy umsetzt, das seit einiger Zeit nicht mehr weiterentwickelt und nicht an aktuelle Thunderbird-Versionen angepasst wird. Außerdem verhindert das Sicherheitskonzept von TAILS Verbindungen ins Netz, die nicht via Tor anonymisiert werden.

Da man Thunderbird nicht bei jedem Start der Live-DVD neu konfigurieren möchte, sollte man die persistente Speicherung der Daten von Thunderbird und GnuPG aktivieren.

1. Zuerst ist der persistente Speicher zu erstellen und zu konfigurieren, sodass die Daten von Thunderbird und GnuPG in dem verschlüsselten Speicher abgelegt werden.

   Den Konfigurator startet man unter **Anwendungen → TAILS → Persistenten Speicher**. Es ist ein Passwort für die Verschlüsselung anzugeben und auf den Button **Erstellen**

zu klicken. Dann wird der freie Platz auf dem TAILS-Boot-Medium für einen verschlüsselten Container zum Speichern der Daten genutzt.

2. Anschließend ist die Live-DVD neu zu starten und im Boot-Greeter ist der persistente Speicher einzubinden. Dafür ist die Eingabe des Passwortes nötig.
3. Danach kann man Thunderbird starten und den E-Mail-Account einrichten.
4. Als E-Mail-Provider sind jene zu bevorzugen, die Tor-Onion-Services für IMAP, POP3 und SMTP anbieten, um die Gefahr durch bösartige Tor-Exit-Nodes zu minimieren.

Thunderbird und Tor Onion Router???

Thunderbird ist nicht für anonyme E-Mails geeignet. Das Add-on TorBirdy ist seit Version 68 nicht mehr kompatibel mit Thunderbird und niemand hat die Gefahren der neuen Features in aktuellen Thunderbird-Versionen bei Kombination mit Tor analysiert.

> *Alas, I think it might be a while until torbirdy gets an update – it involves somebody looking at Thunderbird 68 to see what new privacy invasive problems they put into it.*

Man kann in Thunderbird einen Proxy verwenden und die nötigen Einstellungen für Tor Onion Router eintragen, aber das reicht nicht. Eine Sicherheitsanalyse der Features von Thunderbird von 2011 zeigte noch einige Gefahren auf, die zur Deanonymisierung führen können. Mit dem Add-on TorBirdy, das maßgeblich von Jacob Appelbaum initiiert wurde, konnten diese Risiken gebannt werden. Für Thunderbird wäre eine neue Analyse und eine neue, angepasste Version des Add-on TorBirdy nötig, die es nicht gibt.

Spam-Blacklisten

Viele große E-Mail-Provider sperren Tor-Nodes bei der Versendung von E-Mails via SMTP aus. Sie nutzen Spam-Blacklisten, in denen Tor-Relays häufig als „potentiell mit Bots infiziert“ eingestuft sind. Wenn der E-Mail-Provider eine dieser DNSBL nutzt, sieht man als Anwender von Tor nur eine Fehlermeldung beim Senden von Mails. Der Empfang funktioniert in der Regel reibungslos.

Um diese Probleme zu vermeiden, sollte man einen datenschutzfreundlichen E-Mail-Provider nutzen, der Sender-IPs aus dem Header der versendeten E-Mails entfernt.

GoogleMail und Anonymisierungsdienste

GoogleMail (oder GMail) mag eine anonyme Nutzung der kostenfreien Accounts nicht. Kurz zusammengefasst kann man sagen, dass Google entweder eine IP-Adresse der Nutzer haben möchte oder die Telefonnummer. Stellungnahme des *Google account security team* zu einer Anfrage der Tor Community:

> *Hello,*
>
> *I work for Google as TL of the account security system that is blocking your access.*
>
> *Access to Google accounts via Tor (or any anonymizing proxy service) is not allowed unless you have established a track record of using those services beforehand. You have several ways to do that:*

> *1) With Tor active, log in via the web and answer a security quiz, if any is presented. You may need to receive a code on your phone. If you don't have a phone number on the account the access may be denied.*
>
> *2) Log in via the web without Tor, then activate Tor and log in again WITHOUT clearing cookies. The GAPS cookie on your browser is a large random number that acts as a second factor and will whitelist your access.*
>
> *Once we see that your account has a track record of being successfully accessed via Tor the security checks are relaxed and you should be able to use TorBirdy.*
>
> *Hope that helps, Google account security team*

Außerdem werden nach einem Bericht von Wired[31] zukünftig alle E-Mails der GMail-Accounts in das NSA-Datacenter in Bluffdale kopiert.

12.3.8 Anonym Bloggen

Es gibt viele Gründe, um anonym zu bloggen. Auf die möglichen Gründe möchte ich nicht weiter eingehen, sondern mich auf einige technische Hinweise für die Umsetzung beschränken.

Die einfachste Variante:

- Man braucht einen anonymen Browser, am besten das TorBrowserBundle. Gut geeignet ist beispielsweise TAILS, da dies neben einem fertig konfigurierten Browser für anonymes Surfen auch die nötigen Tools zur Anonymisierung von Bildern und Dokumenten enthält und keine Spuren auf dem PC hinterlässt.
- Man braucht eine anonyme E-Mail-Adresse, die nur in Zusammenhang mit dem Blog verwendet wird (für die Registrierung und als Kontaktadresse). Dabei ist es nicht nötig, einen E-Mail-Client zu konfigurieren. Man kann die E-Mails im Webinterface des Providers mit dem TorBrowser lesen.
- Man braucht einen Bloghoster, der anonyme Registrierung oder Registrierung mit Fake-Daten ermöglicht. Auf kostenpflichtige Premiumfeatures kann man verzichten, um Spuren durch Finanztransaktionen zu vermeiden.

  Wordpress.com, die kostenfreie Variante von *Twoday.net* oder *Substack.com*...
- Registrierung und Verwaltung des Blogs sowie das Schreiben von Artikeln können komplett im Browser durchgeführt werden. Dabei ist stets der Anonymisierungsdienst zu nutzen. Man sollte darauf achten, dass man nicht hektisch unter Zeitdruck schnell mal einen Beitrag verfasst. Dabei können Fehler passieren.
- Im Blog veröffentlichte Bilder und Dokumente sind stets vor dem Upload zu anonymisieren. Vor allem Bilder von Digitalkameras enthalten eine Vielzahl von Informationen, die zur Deanonymisierung führen können. Fotos von Freunden oder Bekannten sollte man nicht veröffentlichen, da durch Freundschaftsbeziehungen eine Deanonymisierung möglich ist.
- Jede Blog-Software bietet die Möglichkeit, den Zeitpunkt der Veröffentlichung von neuen Artikeln festzulegen. Das sollte man nutzen und neue Artikel nicht sofort veröffentlichen, sondern einige Stunden später freigeben, wenn man nicht online ist.

[31] http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

- Stilometrie (Deanonymisierung anhand des Schreibstils) ist inzwischen fester Bestandteil geheimdienstlicher Arbeit. Es ist mit (teil-) automatisierten Verfahren möglich, anonyme Texte einem Autor zuzuordnen, wenn der Kreis der Verdächtigen eingeschränkt ist und genügend Textproben der Verdächtigen vorliegen. Mit Ruhe und Konzentration beim Verfassen von Blog-Artikeln ist es möglich, seinen individuellen Schreibstil zu verstellen und stilometrische Angriffe zu erschweren.

12.3.9 Anonymes Instant-Messaging

Verschlüsselte Chats und Instant-Messaging in Kombination mit Anonymisierungsdiensten wie Tor sind auch für potente Geheimdienste wie die NSA ein Alptraum. Es gibt keine Metadaten, die OTR-Verschlüsselung kann noch nicht gebrochen werden und eine Zuordnung von Traffic zu IP-Adressen wird durch die Anonymisierungsdienste verhindert.

Leider gibt es nur wenige Messenger, die für die Kombination mit Tor geeignet sind:

- Populäre Messenger, die eine Telefonnummer und ein Smartphone für den Hauptaccount erfordern, sind natürlich ungeeignet (trivial).
- Messenger, die Interactive Connection Establishment (ICE) für Audio- und Videochats verwenden, sind auf PCs/Laptops ebenfalls ungeeignet. ICE versucht nämlich aggressiv, eine Peer-2-Peer Verbindung mit oder ohne Proxy herzustellen, teilt dabei die eigene IP-Adresse dem Kommunikationspartner mit und versucht, via UPnP ein Loch in den Router zu bohren. Somit kann ein Anruf zur Deanonymisierung führen.

  ICE ist Bestandteil von WebRTC und der libjingle (XMPP, WhatsApp).
- DNS-Leaks sind ein häufiges Problem bei Messengern, die nicht ausdrücklich für die Nutzung mit Tor Onion Router vorbereitet wurden.

Folgende Anwendungen können für Instant-Messaging via Tor genutzt werden:

Briar (nur Android) bringt Tor bereits mit und ist für anonyme Nutzung optimiert.

qTox (PCs/Laptops) bzw. der **TRIfA**-Tox-Client für Android können mit Tor genutzt werden, weil das Protokoll keine verräterischen Informationen überträgt.

Dabei ist darauf zu achten, dass der anonym genutzte Account erst dann angelegt wird, wenn der Proxy via Tor konfiguriert wurde. Um die Einstellungen modifizieren zu können, muss man evtl. zuerst einen Dummy-Account erstellen, und danach den richtigen Account.

UDP- und IPv6-Support sind bei der Konfiguration von Tor als Proxy entgegen der Empfehlung zu deaktivieren, da beides von Tor nicht unterstützt wird (Abb. 12.11).

Jabber/XMPP mit Tor zu verwenden, war vor einigen Jahren populär. Der XMPP-Client muss dabei folgende Anforderungen erfüllen:

1. Es muss ein SOCKS5-Proxy mit Remote DNS Resolving (ohne DNS-Leaks) konfigurierbar sein, um die Daten durch den Anonymisierungsdienst zu schicken.
2. Die Tor-Hidden-Service-Adresse des Jabber-Servers muss als *Verbindungsserver* konfigurierbar sein. Wenn Tor Onion Router genutzt wird, empfehlen wir nachdrücklich die Jabber/XMPP-Server, die eine Tor-Hidden-Service-Adresse anbieten. Damit vermeidet man Gefahren durch bösartige Tor-Exit-Nodes. Angriffe von bösartigen Tor-Exit-Nodes auf Jabber/XMPP wurden bereits nachgewiesen.

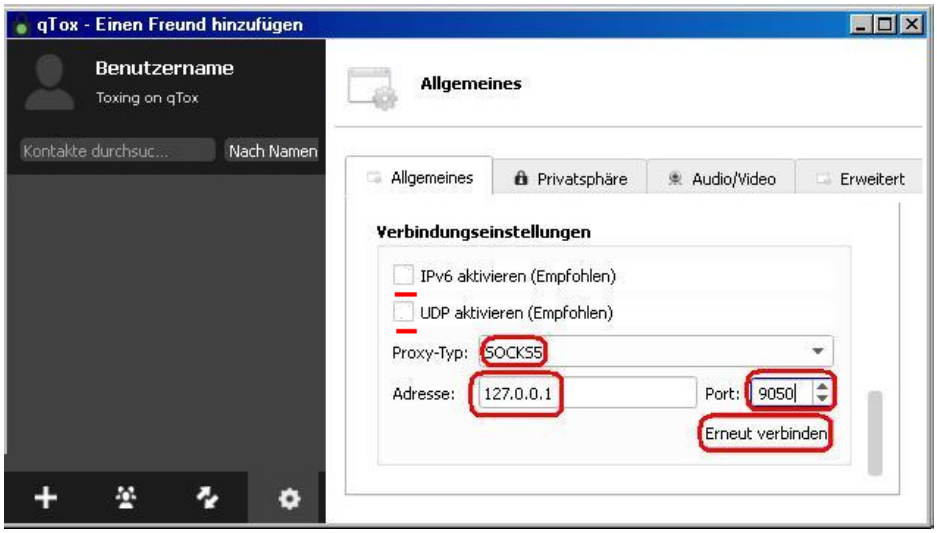


Abbildung 12.11: qTox-Proxy-Konfiguration für Tor Onion Router

3. Audio- und Video-Chats mit der *libjingle* dürfen nicht verfügbar bzw. müssen deaktivierbar sein. Audio- und Video-Chats sind via Anonymisierungsdienst nicht möglich. Bei Einladung zu einem Video-Chat versucht das integrierte *Interactive Connectivity Establishment* (ICE) der *libjingle* nämlich automatisch, eine Verbindung mit oder ohne Proxy herzustellen. Das ist kein Bug, sondern ein Feature der ICE-Spezifikation. Nutzer können damit deanonymisiert werden.
4. Auch weitere XMPP-Erweiterungen wie z. B. der Jingle-Dateitransfer können unter Umständen von einem Angreifer zur Deanonymisierung genutzt werden.

TorProject.org empfiehlt *CoyIM* für Jabber/XMPP. Dieser Client bietet nur Textchats mit OTR-Verschlüsselung und vermeidet durch Reduktion der Features Probleme bei der Anonymisierung, wie sie mit anderen Jabber/XMPP-Clients auftreten.

Allerdings ist OTR als Ende-zu-Ende-Verschlüsselung nicht kompatibel mit den meisten anderen Jabber/XMPP-Clients, die OMEMO bevorzugen.

12.3.10 Dateien anonym tauschen via Tor

OnionShare[32] ist ein kleines Tool, um in Kombination mit dem TorBrowserBundle Dateien zu tauschen. Es ist eine ideale Ergänzung zu TorMessenger oder Ricochet, denen die Möglichkeit zum Tauschen von Dateien (noch) fehlt.

1. Der Absender benötigt OnionShare und den Tor-Daemon des TorBrowserBundles, um die Dateien zum Download bereitzustellen. OnionShare stellt einen Tor-Hidden-Service bereit, unter dem die Dateien abgerufen werden können.
2. Der oder die Empfänger benötigen nur den TorBrowser, um die bereitgestellten Dateien herunterzuladen. Den Link zum Download bekommen die Empfänger über einen anderen sicheren Kanal, z. B. via TorMessenger oder Ricochet.

Installation von OnionShare:

[32] https://onionshare.org/

- Für Windows und MacOS stehen auf der Download-Website Setup-Dateien zur Installation bereit.
- In den Linux-Distributionen Unbuntu und Fedora ist Onionshare enthalten und kann mit dem bevorzugten Tool zur Softwareverwaltung installiert werden.
- Für alle anderen Linux-Distributionen muss man OnionShare selbst compilieren. Eine Anleitung findet man auf der Webseite.

Nach dem Start von OnionShare kann man im Hauptfenster Dateien zur Liste der gesharten Dateien hinzufügen und den Service starten. Der Tor-Daemon des TorBrowserBundle wird genutzt, um den Hidden-Service bereitzustellen. Das TorBrowserBundle muss also gestartet werden, bevor man die Dateien zum Download freigeben kann.

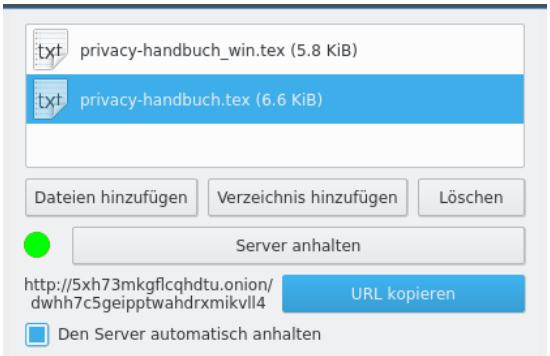


Abbildung 12.12: OnionShare-Hauptfenster

Wenn die Option *Den Server automatisch anhalten* aktiviert ist, dann wird der Tor-Hidden-Service nach dem ersten erfolgreichen Download sofort wieder beendet. Das ist ein Sicherheitsfeature, da es im Tor-Netz auch bösartige Nodes gibt, die neue Tor-Hidden-Services testen und teilweise auch angreifen.[33]

Wenn der Service erfolgreich gestartet ist, kann man die Tor-Onion-URL in die Zwischenablage kopieren und an den oder die Empfänger schicken, am besten via Instant-Messenger. Der oder die Empfänger können die Adresse dann im TorBrowser aufrufen und die bereitgestellten Dateien als ZIP-Archiv herunterladen.

1-Click-Hoster

1-Click-Hoster sind eine weitere mögliche Alternative. Mit dem TorBrowserBundle kann man anonym Dateien bei einem 1-Click-Hoster hochladen und dann den Download-Link verteilen.

- Auf diesen Hostern sind die Uploads nur eine für begrenzte Zeit verfügbar:
  - https://send.tresorit.com (bis zu 5 GB, Ende-zu-Ende-verschlüsselt, Passwortschutz möglich, benötigt eine E-Mail-Adresse, aber Wegwerf-Adressen funktionieren, Uploads werden nach 7 Tagen oder 10 Downloads gelöscht);
  - https://upload.disroot.org/ (bis zu 2 GB, Ende-zu-Ende-verschlüsselt, Schlüssel in Download-URL, Passwortschutz möglich, Uploads können bis zu 30 Tage verfügbar sein);

[33] https://www.schneier.com/blog/archives/2016/07/researchers_dis.html

  - https://upload.adminforge.de/ (bis zu 2 GB, Ende-zu-Ende-verschlüsselt, Schlüssel in Download-URL, Passwortschutz möglich, Uploads können bis zu 30 Tage verfügbar sein);
  - https://1fichier.com/ (bis zu 300 GB, Passwortschutz für Downloads möglich, Uploads werden nach 15 Tagen gelöscht);
  - https://nowtransfer.de/ (Uploads bis zu 8 Wochen verfügbar).

- Für Langzeit-Hosting kann man folgende Dienste verwenden:
  - https://www.mediafire.com (Registrierung für Uploads nötig).

BitTorrent über einen Anonymisierungsdienst ???

Die naheliegende Variante ist, BitTorrent über einen Anonymisierungsdienst wie Tor zu nutzen, um die eigene IP-Adresse zu verstecken. Das funktioniert nur begrenzt. Das BitTorrent-Protokoll überträgt die IP-Adresse des Clients auch im Header der Daten und es ist relativ einfach möglich, die Teilnehmer zu deanonymisieren. Im Moment hat die Abmahn-Industrie den Weg noch nicht gefunden. Im Blog von TorProjekt.org findet man eine ausführliche Erläuterung, warum BitTorrent via Tor NICHT anonym ist.[34]

Anonyme Peer-2-Peer-Netze

Einige Projekte für anonymes, unbeobachtetes Filesharing:

- **I2P Snark:** Das Invisible Internet Project bietet anonymes Filesharing innerhalb des Netzes.
- **GNUnet:** bietet anonymes, zensurresistentes Filesharing ohne zentrale Server. Alle Teilnehmer leiten Daten für andere Teilnehmer weiter und stellen selbst Dateien bereit. Da weitergeleitete Daten nicht von Daten unterscheidbar sind, die von einem Teilnehmer selbst stammen, ergibt sich eine hohe Anonymität. Es ist ein echtes GNU-Projekt (bitte nicht mit *Gnutella* verwechseln). Weitere Informationen findet man auf der Projektwebsite https://gnunet.org/?xlang=German.

12.3.11 Tor-Onion-Services

Das Tor-Netzwerk ermöglicht nicht nur den anonymen Zugriff auf herkömmliche Angebote im Web, sondern auch die Bereitstellung anonymer, zensurresistenter und schwer lokalisierbarer Angebote auf den Tor-Nodes.

Der Zugriff auf die Tor-Hidden-Services (Neu: Tor-Onion-Services) ist nur über das Tor-Netzwerk möglich. Eine kryptische Adresse mit der Top-Level-Domain .onion dient gleichzeitig als Hashwert für ein System von Schlüsseln, welches sicherstellt, dass der Nutzer auch wirklich mit dem gewünschten Dienst verbunden wird. Die vollständige Anonymisierung des Datenverkehrs stellt sicher, dass auch die Betreiber von Onion-Sites technisch anonym bleiben und nur sehr schwer ermittelt werden können.

Es gibt zwei Versionen für Tor-Onion-Services:

[34] https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea

Onion-Services v2 sind veraltet und werden seit Oktober 2021 nicht mehr unterstützt. Diese Onion-Services verwenden kryptografische Funktionen, die teilweise veraltet sind. Es wird SHA1 verwendet, DH-Schlüsseltausch und Public-Key-Kryptografie auf der Basis von RSA mit 1024-Bit-langen Schlüsseln. Die Onion-Adressen waren 16 Zeichen lang:

```
vwakviie2ienjx6t.onion
```

Onion-Services v3 stehen ab Tor-Version 3.2 zur Verfügung (Stable Release v3.2.9 Januar 2018). Sie verwenden aktuelle kryptografische Funktionen (SHA3, ECDHE mit ed25519 und Public-Key-Kryptografie auf der Basis elliptischer Kurven mit curve25519). Die Onion-Adressen sind mit 56 Zeichen wesentlich länger:

```
4acth47i6kxnvkewtm6q7ib2s3ufpo5sqbsnzjpbi7utijcltosqemad.onion
```

Stealth Onion-Services erfordern einen zusätzlichen Schlüssel für den Aufbau einer Verbindung. Die Informationen in den Hidden Service Directories über mögliche Zugangspunkte zu diesen Onion-Services sind verschlüsselt, sodass bösartige Dritte diese Onion-Services nicht ausspionieren oder angreifen können. Wer sich mit diesen Onion-Sites verbinden möchte, braucht einen zusätzlichen Key, um die Informationen über die Zugangspunkte zu dechiffrieren.

Autorisierte Nutzer erhalten den Key zum Entschlüsseln der Informationen vom Betreiber über einen unabhängigen, sicheren Kanal. Der Betreiber kann dabei bis zu 50 unterschiedliche Schlüssel für verschiedene Personen generieren. Die Nutzer können diesen Key in der Konfigurationsdatei *torrc* des Tor-Daemon eintragen:

```
HidServAuth <OnionAdresse> <Key>
```

Alternativ kann man den Schlüssel auch bei Aufruf einer Stealth-Onion-Adresse im Tor-Browser eingeben und dort dauerhaft speichern, wenn die Abfrage erscheint.

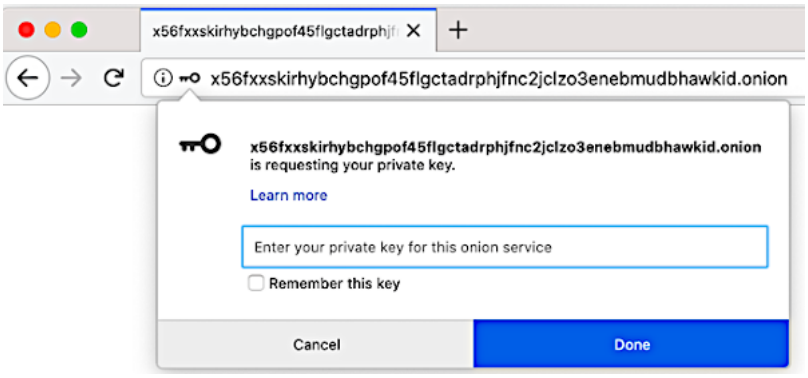


Abbildung 12.13: Abfrage des Schlüssels für eine Stealth-Onion-Site im TorBrowser

Tor-Onion-Webservices als sichere Alternative

Es gibt mehrere Angebote im normalen Web, die zusätzlich als Tor-Hidden-Service bzw. als Tor-Onion-Site anonym und unbeobachtet erreichbar sind. Wenn man Tor nutzt, sollte man diese

Onion-Services den normalen Webadressen vorziehen, da dann keine Gefahr durch Bad-Tor-Exit-Nodes besteht.

Die **Suchmaschine** Metager (deutsche Suchmaschine) ist erreichbar unter
http://metagerv65pwclop2rsfzg4jwowpavpwd6grhhlvdgsswvo6ii4akgyd.onion

Die folgenden Webseiten können als Tor-Onion-Sites aufgerufen werden:

- Die Webseite von TorProject.org ist unter folgender Adresse zu finden:
  http://2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion
- Weitere Onion-Sites findet man unter https://onion.torproject.org bzw.
  http://xao2lxsmia2edq2n5zxg6uahx6xox2t7bfjw6b5vdzsxi7ezmqob6qid.onion
- Die Onion-Sites des Debian-Projekts findet man unter https://onion.debian.org
- Heise.de bietet einen sicheren Briefkasten auf Basis von Secure-Drop für Tippgeber (sogenannte Whistleblower) unter der Adresse:
  http://ayznmonmewb2tjvgf7ym4t2726muprjvwckzx2vhf2hbarbbzydm7oad.onion
- Die CIA bietet einen ähnlichen Briefkasten als Onion-Service für Informanten. Wer sich bei der CIA anbiedern will, um sein Taschengeld ein bisschen aufzubessern, findet ihn hier:
  http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/
- Reddit.com ist als Tor-Onion-v3-Site erreichbar:
  http://kphht2jcflojtqte4b4kyx7p2ahagv4debjj32nre67dxz7y57seqwyd.onion/
- u. v. a. m.

Wenn der Betreiber einer Webseite es mit dem Onion-Service wirklich ernst meint, kann er den HTTP-Header *Onion Location* in die Webseite einbauen, der beim Aufruf der Clearnet-Webseite auf den Onion-Service hinweist. Der TorBrowser zeigt dann rechts von der URL einen lila Button an:

Mit einem Klick auf den lila Button *.onion available* wird die Seite vom Onion-Service aufgerufen. Da die Nutzung des Onion-Service grundsätzlich sicherer ist, als eine Clearnet-Webseite über einen Exit-Node aufzurufen, sollte man diese Möglichkeit nutzen. Mit einer kleinen Einstellung im TorBrowser kann man diesen Schritt auch automatisieren und immer zum Onion-Service wechseln (Abb. 12.14).

Tor-Onion-Services für E-Mail und XMPP

Die folgenden **E-Mail-Provider** bieten POP3, IMAP und SMTP als Tor-Onion-Service:

- mailbox.org: xy5d2mmnh6zjnroce4yk7njlkyafi7tkrameybxu43rgsg5ywhnelmad.onion
- Riseup.net: 5gdvpfoh6kb2iqbizb37lzk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion
- Die ProtonMail-Webseite ist als Onion-v3-Service unter folgender Adresse erreichbar:
  https://account.protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion/login

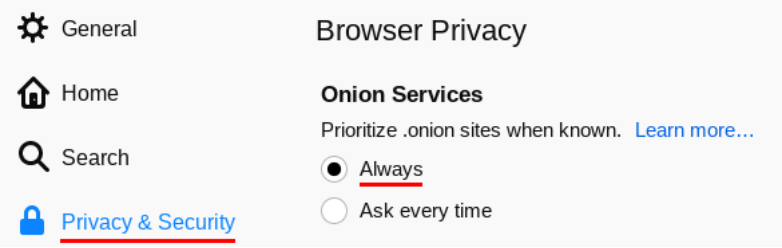


Abbildung 12.14: Einstellung im TorBrowser, um automatisch zum Onion-Service zu wechseln, wenn ein Onion-Service für die Webseite bekannt ist.

Die folgenden **Jabber-Server** sind als Tor-Onion-Service erreichbar:

- Mailbox: xy5d2mmnh6zjnroce4yk7njlkyafi7tkrameybxu43rgsg5ywhnelmad.onion
- Systemli: razpihro3mgydaiykvxwa44l57opvktqeqfrsg3vvwtmvr2srbkcihyd.onion
- Riseup: jukrlvyhgguiedqswc5lehrag2fjunfktouuhi4wozxhb6heyzvshuyd.onion
- Securejabber: sidignlwz2odjhgcfhbueinmr23v5bubq2x43dskcebh5sbd2qrxtkid.onion
- Jabber.otr.im: ynnuxkbbiy5gicdydekpihmpbqd4frruax2mqhpc35xqjxp5ayvrjuqd.onion
- Jabber.so36: yxkc2uu3rlwzzhxf2thtnzd7obsdd76vtv7n34zwald76g5ogbvjbbqd.onion
- Jabber.cat: 7drfpncjeom3svqkyjitif26ezb3xvmtgyhgplcvqa7wwbb4qdbsjead.onion
- Dismail: 4colmnerbjz3xtsjmqogehtpbt5upjzef57huilibbq3wfgpsylub7yd.onion

HKP-Keyserver für OpenPGP-Schlüssel sind unter folgender Adresse erreichbar:
hkp://zkaan2xfbuxia2wpf7ofnkbz6r5zdbbvxbunvp5g2iebopbfc4iqmbad.onion

Für unbeobachtete Kommunikation gibt es folgende Dienste, die ausschließlich als Tor-Hidden-Service genutzt werden können:

- *Mail2Tor* (kostenfrei, Gateway ins normale Web ist vorhanden)
  http://mail2torjgmxgexntbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion
- *TorBox* (kostenfreier Hidden-only E-Mail-Service)
  http://torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.onion

Hinweis: Einige Tor-Onion-E-Mail-Provider bieten ein Gateway ins normale Web, um E-Mails auch mit Nutzern aus dem normalen Internet austauschen zu können. Diese Gateways bieten aber nur eine schlechte TLS-Konfiguration, die Transportverschlüsselung zu den Mailservern der normalen E-Mail-Provider ist also durchgehend sehr schlecht. Deshalb würde ich Tor-Hidden-Mail-Provider nur für die Kommunikation mit Onion-Adressen empfehlen, für den Kontakt mit normalen E-Mail-Adressen aber ein sicheren Provider aus dem normalen Netz nutzen.

Sonstiges

Ansonsten kenne ich kaum etwas, dass ich weiterempfehlen möchte. Meine „Sammlung“ an reinen Tor-Hidden-Services enthält:

- 34x Angebote, die kinderpornografischen Schmutz zum Download anbieten (ausschließlich und teilweise zusätzlich zu anderen Inhalten). Das BKA hat eine etwas umfangreichere Liste mit 545 Seiten (Stand: 2012).[35]
- 3x Angebote zum Thema *Rent a Killer*. Ein Auftragsmord kostet offenbar nur 20.000 Dollar (wenn diese Angebote echt sind).
- Ein Angebot für gefakte Ausweisdokumente (aufgrund der mit Photoshop o. Ä. bearbeiteten Screenshots der Beispieldokumente auf der Webseite halte ich das Angebot selbst für einen Fake).
- Mehrere Handelsplattformen für Drogen. (Das FBI kannte über 400 Plattformen zu diesem Thema.)
- Einige gähnend langweilige Foren & Blogs mit 2–3 Beiträgen pro Monat.
- Einige Index-Seiten mit Listen für verfügbare Hidden-Services wie das legendäre *HiddenWiki* oder das neuere *TorDirectory*. In diesen Index-Listen findet man massenweise Verweise auf Angebote mit Bezeichnungen wie *TorPedo*, *PedoVideoUpload*, *PedoImages*. Nach Beobachtung von ANONYMOUS sollen 70 % der Besucher des *HiddenWiki* die Adult Section aufsuchen, wo dieses Schmutzzeug verlinkt ist.

In dem Paper *Cryptopolitik and the Darknet* (2016) haben sich die Autoren D. Moore und T. Rid empirisch mit den Tor-Onion-Sites beschäftigt. Von den 2723 besuchten Onion-Sites waren 1547 Onion-Sites auf kriminelle, illegale Aktivitäten ausgerichtet.[36]

Fake-Onion-Sites

Für Tor-Onion-Sites gibt es kein Vertrauens- oder Reputationsmodell. Es ist unbekannt, wer einen Tor-Hidden-Service betreibt und es ist damit sehr einfach, Honeypots aufzusetzen. Die kryptischen Adressen sind nur schwer verifizierbar. Das Problem von *Anonymität und Reputation* ist im Kapitel Nachdenken ausführlicher beschrieben.

Juha Nurmi (Betreiber der Hidden-Service-Suchmaschine Ahmia.fi) veröffentlichte bereits zwei Warnungen im Juni 2015[37] und Januar 2016[38] mit 300 Fake-Onion-Sites, die den originalen Onion-Sites täuschend ähnlich sehen. Diese Fake-Sites leiten den Traffic der originalen Sites durch, modifizieren die Daten geringfügig oder erschnüffeln Login-Credentials.

Auch Suchmaschinen mit Hidden-Service-Adressen wie DuckDuckGo (Tor) und Ahmia.fi waren betroffen, wie die Screenshots in Abb. 12.15 zeigen. Die Fake-Site sieht dem Original täuschend ähnlich, die Besucher werden mit den Suchergebnissen aber auf andere Fake-Onion-Sites gelenkt.

Teilweise waren auch die Onion-v2-Adressen der Fake-Sites den Originalen ähnlich:

[35] http://heise.de/-2124930
[36] http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085
[37] https://lists.torproject.org/pipermail/tor-talk/2015-June/038295.html
[38] https://lists.torproject.org/pipermail/tor-talk/2016-January/040038.html

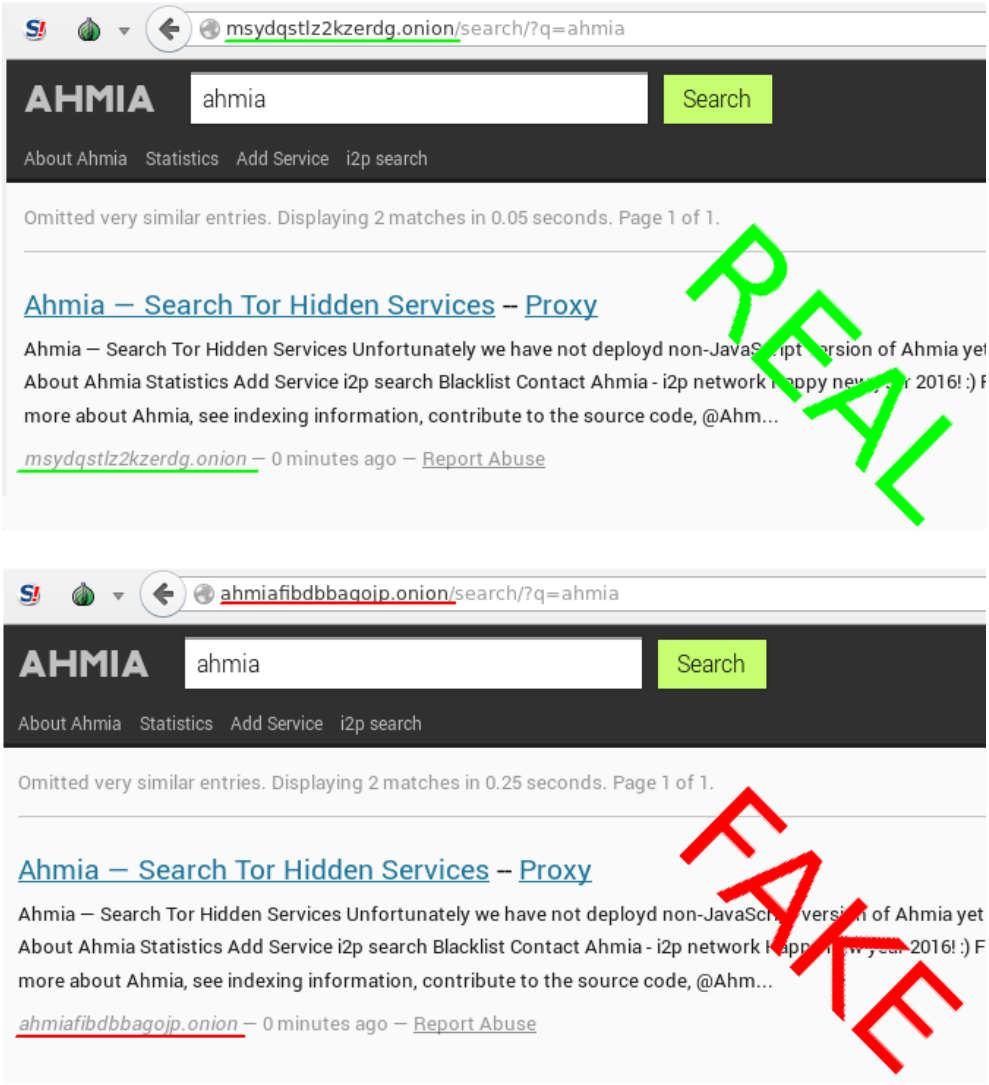


Abbildung 12.15: Original und Fake-Onion-Site der Suchmaschine Ahmia.fi

```
REAL: http://torlinkbgs6aabns.onion
FAKE: http://torlinksb7apugxr.onion

REAL: http://valhallaxmn3fydu.onion
FAKE: http://valhalla4qb6qccm.onion

REAL: http://vendor7zqdpty4oo.onion
FAKE: http://vendor7eewu66mcc.onion
```

Schlussfolgerung: Man sollte den kryptischen Hidden-Service-Adressen nur vertrauen, wenn man sie aus einer vertrauenswürdigen, verifizierten Quelle bekommt. Die Ergebnisse einer Suchmaschine für Onion-Sites sind nur begrenzt zuverlässig, da die Betreiber der Fake-Onion-Sites auch SEO-Techniken nutzen, um *vor* den Originalen platziert zu werden.

12.3.12 Anti-Zensur-Features von Tor Onion Router

Da Tor Onion Router die Möglichkeit bietet, die repressive Informationspolitik einiger Staaten zu umgehen und Zugang zu zensierten Inhalten und Diensten ermöglicht, ist Tor gleichfalls in einigen Ländern von Sperrungen und Zensur betroffen. Einige Beispiele:

- In China ist die Führung der regierenden KPCh der Auffassung, das Meinungs- und Pressefreiheit absolut überflüssig sind. Diskussionen verunsichern die Bevölkerung nur und stören den Marsch in die goldene Zukunft. Ein großer Teil der Bevölkerung hat diese Doktrin akzeptiert.

  Parallel zur Indoktrinierung korrekten Verhaltens setzt China mit der *Great Firewall* auch technische Mittel ein und blockiert damit seit 2008 Verbindungen zum Tor-Netz.

- Iran hat ein landesweites, geschlossenes *Halal*-Netz aufgebaut, das den IP-Adressbereich 10.0.0.0/8 verwendet und nur über wenige, staatlich kontrollierte Knoten mit dem echten Internet verbunden ist. Auf diesen Knoten wird DPI (Deep Packet Inspection) eingesetzt, um Verbindungen zum Tor-Netz nicht nur anhand von IP-Adressen zu blockieren, sondern auch anhand von Merkmalen im Traffic. Es wird bspw. der TLS-Handshake zwischen Tor-Client und Entry-Node anhand der Tor-typischen X509v3-Zertifikate erkannt und die Verbindung unterbrochen.

- In der Türkei wurde Tor 2014 mit der Sperrung von Twitter populär. In kurzer Zeit verdoppelten sich die Nutzerzahlen (ein unzensierter DNS-Server hätte aber auch gereicht). Seit 2017 wird das Tor-Netzwerk bei vielen Internetprovidern in der Türkei blockiert. Die Sperre wird aber nicht weiterentwickelt oder angepasst und kann mit Bridges umgangen werden.

- Belarus hat 2018 einige Millionen Dollar in neue Zensurinfrastruktur investiert und die Technik war 2020 rechtzeitig vor der Wahl und den darauffolgenden Protesten einsatzbereit. Die Zensur des Tor-Netzwerkes wurde mit dem Beginn der Proteste im August 2020 aktiviert. Verbindungen zu den öffentlich bekannten Tor-Nodes werden beim TLS-Handshake zum Aufbau einer Verbindung anhand von Ziel-IP-Adresse und -Port blockiert. Außerdem werden die einfach nutzbaren Built-in-obfs4-Proxys blockiert. Es gibt (bisher) keine Anzeichen für DPI.

- Russland hatte bis 2021 die zweitgrößte Community von Tor Nutzern (mehr als 300.000 Nutzer täglich). Durch schrittweise Einführung von Zensurmaßnahmen (Sperrung der

Webseiten von Torproject.org und der Download-Mirrors, Sperrung der IP-Adressen von Tor-Nodes und Bridges) sank die Zahl der täglichen Nutzer innerhalb eines halben Jahres auf 100.000.

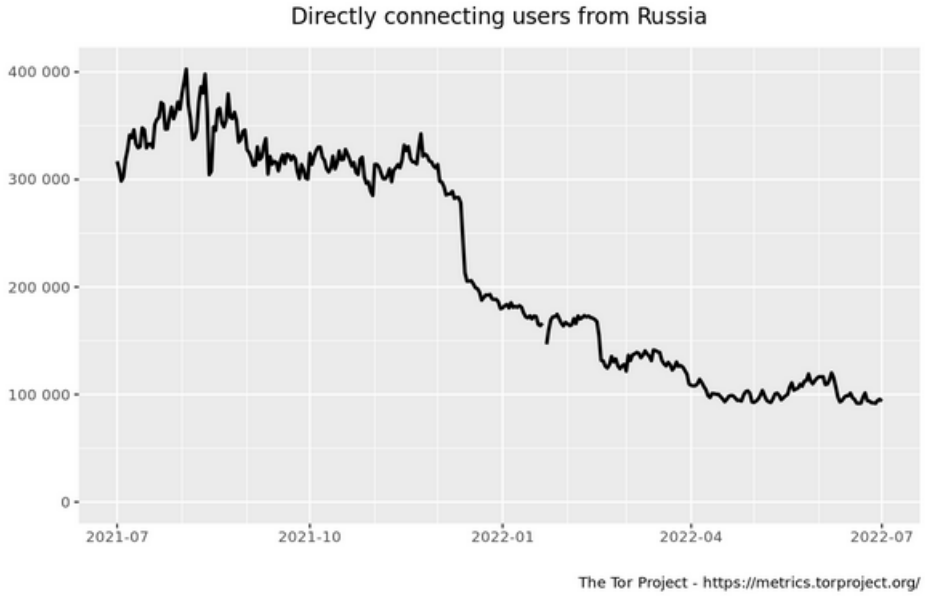


Abbildung 12.16: Tor-Nutzer aus Russland von 07/2021 bis 07/2022

Technisch basiert die Zensur in Russland auf den TCPU-Boxen, die bei den großen Internetzugangsprovidern installiert sind. Die Provider haben keinen Zugriff auf diese Boxen. Die Konfiguration der Zensurmaßnahmen erfolgt zentral durch Roskomnadzor. Es können IP-Adressen und URLs gesperrt oder gezielt gedrosselt werden.

Roskomnadzor baut die Blockade von Tor schrittweise aus. Zuerst wurde die Webseite von TorProject.org gesperrt, dann die Downoload-Mirrors, dann die öffentlich bekannten Adressen regulärer Tor-Nodes. Daraufhin nahm die Nutzung von Bridges in Russland deutlich zu (fast 50 % der Tor-Bridge-Nutzer weltweit kommen aktuell aus Russland). Roskomnadzor reagierte darauf und seit Mai/Juni 2022 werden immer mehr Obfuscation-Bridges in Russland unbrauchbar.

Die Zensurmaßnahmen werden von Roskomnadzor nicht sofort landesweit aktiviert, sondern erst mal in einigen Regionen ausprobiert und dann immer breiter aktiviert.

Die Tor-Community hat Methoden entwickelt, um Blockaden von Tor zu umgehen:

Bridges waren ursprünglich Tor-Entry-Nodes, deren IP-Adressen nicht veröffentlicht wurden. Nachdem der Iran mittels DPI die typischen Merkmale einer Tor-Verbindung erkannte und diese blockierte, wurden die Obfuscation-Bridges entwickelt, die ein anderes Übertragungsprotokoll simulieren. Aktuell sind die *obfs4 proxys* die empfohlenen, performantesten Bridges. Bei Verwendung von *obfs4 proxys* kann ein Provider nicht erkennen, dass Tor genutzt wird.

meek azure nutzt Domain-Fronting. Die meek-Bridges werden in der Microsoft-Azure-Cloud installiert und sind via DNS-Namen mit wechselnden IP-Adressen erreichbar. Eine Blockade der meek-Bridges hätte einen großen Kollateralschaden zur Folge. meek-Bridges sind die empfohlene Methode, um die *Great Firewall* von China zu durchtunneln.

Snowflakes kapseln die Verbindungen zum Tor-Netz in einer WebRTC-Verbindung zu einem Browser irgendwo auf der Welt (Firefox, Google Chrome), der das Snowflakes-Add-on installiert hat. Das Snowflakes-Add-on leitet die Zwiebel-verschlüsselten Daten zum Entry-Node weiter.

Wenn es mit dem TorBrowserBundle nicht möglich ist, eine Verbindung zum Tor-Netzwerk herzustellen, kann man in den *Settings* in der Sektion *Tor* die Option *Use a bridge* aktivieren.

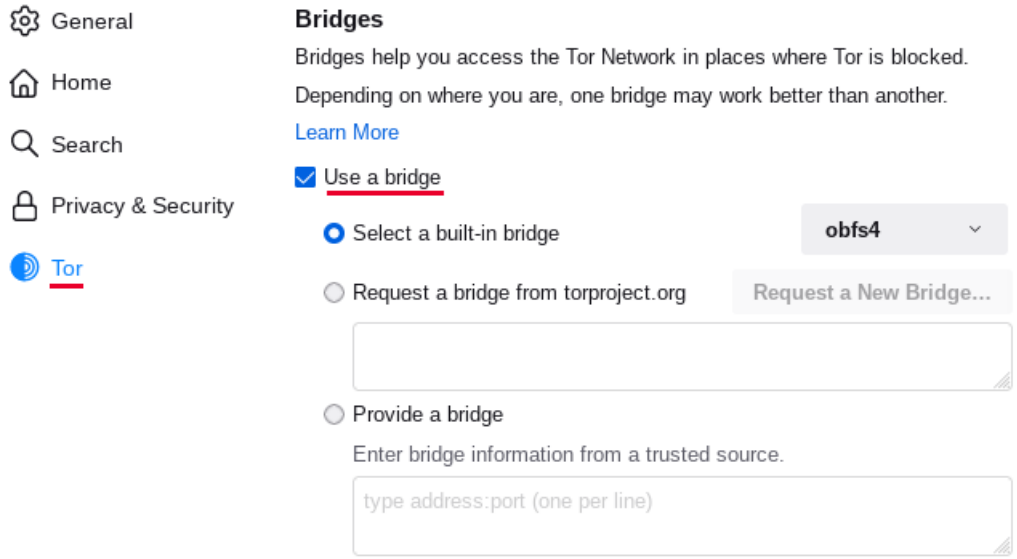


Abbildung 12.17: Anti-Zensur-Methoden im TorBrowserBundle aktivieren

Am besten funktionieren *obfs4*-Bridges. Wenn die Built-in-Bridges blockiert sind, kann man direkt im TorBrowser via Moat-API mit *Request a New Bridge...* eine neue Bridge anfordern. Wenn auch die Moat-API vom Zensor blockiert wird, kann man auf der Webseite TorBridges eine neue Bridge abrufen oder eine E-Mail von einem GMail-Account(!) an bridges@torproject.org schicken und bekommt drei neue obfs4-Bridges, die man unter *Provide a bridge* eintragen kann.

Inoffiziell gibt es (speziell für Russland?) auch den Telegram-Bot @GetBridgesBot, dem man das Kommando /bridges schicken kann und die gewünschte Antwort bekommt.

Wenn man die Whonix-VMs verwendet, werden Bridges nicht im TorBrowser konfiguriert sondern in der Gateway-VM. Man kann die Bridges im Tor Control Panel aktivieren.

12.3.13 Tor-Bad-Exit-Nodes

Ein sogenannter *Bad-Exit-Node* im Tor-Netz versucht, den Traffic zu beschnüffeln oder zusätzliche Inhalte in eine (nicht SSL-gesicherte) Website einzuschmuggeln. Bedingt durch das Prinzip des Onion-Routings holt der letzte Node einer Kette die gewünschten Inhalte. Diese Inhalte liegen dem Tor-Exit-Node im Klartext vor, wenn die Verbindungen zum Server nicht mit TLS verschlüsselt wurden.

Durch einfaches Beschnüffeln wird die Anonymität des Nutzers nicht zwangsläufig kompromittiert, sondern es werden meist Inhalte mitgelesen, die im Web schon verfügbar sind. Erst wenn Login-Daten unverschlüsselt übertragen werden oder Man-in-the-Middle-Angriffe erfolgreich sind, können die Bad-Exit-Nodes an persönliche Informationen gelangen. Persönliche Daten, bspw.

Abbildung 12.18: Anti-Zensur-Methoden in der Whonix-Gateway-VM aktivieren

Login-Daten für einen Mail- oder Bank-Account, sollten nur über SSL- oder TLS-gesicherte Verbindungen übertragen werden. Bei SSL-Fehlern sollte die Verbindung abgebrochen werden. Das gilt für Surfen via Tor wie auch im normalen Web.

Einige Beispiele für Bad-Exits:

1. Die folgenden Nodes wurden dabei erwischt, den Exit-Traffic zu modifizieren und JavaScript in abgerufene Websites einzuschmuggeln. Dabei handelte es sich zumeist um Werbung oder Redirects auf andere Seiten. Diese Bad-Exit-Nodes sind schon lange nicht mehr online, die Liste ist nur als Beispiel gedacht.

apple	$232986CD960556CD8053CBEC47C189082B34EF09
CorryL	$3163a22dc3849042f2416a785eaeebfeea10cc48
tortila	$acc9d3a6f5ffcda67ff96efc579a001339422687
whistlersmother	$e413c4ed688de25a4b69edf9be743f88a2d083be
BlueMoon	$d51cf2e4e65fd58f2381c53ce3df67795df86fca
TRHCourtney1..10	$F7D6E31D8AF52FA0E7BB330BB5BBA15F30BC8D48
	$AA254D3E276178DB8D955AD93602097AD802B986
	$F650611B117B575E0CF55B5EFBB065B170CBE0F1
	$ECA7112A29A0880392689A4A1B890E8692890E62
	$47AB3A1C3A262C3FE8D745BBF95E79D1C7C6DE77
	$0F07C4FFE25673EF6C94C1B11E88F138793FEA56
	$0FE669B59C602C37D874CF74AFEA42E3AA8B62C6
	$E0C518A71F4ED5AEE92E980256CD2FAB4D9EEC59
	$77DF35BBCDC2CD7DB17026FB60724A83A5D05827
	$BC75DFAC9E807FE9B0A43B8D11F46DB97964AC11
Unnamed	$05842ce44d5d12cc9d9598f5583b12537dd7158a
	$f36a9830dcf35944b8abb235da29a9bbded541bc
	$9ee320d0844b6563bef4ae7f715fe633f5ffdba5
	$c59538ea8a4c053b82746a3920aa4f1916865756

```
$0326d8412f874256536730e15f9bbda54c93738d
$86b73eef87f3bf6e02193c6f502d68db7cd58128
```

2. Die folgenden Nodes wurden bei dem Versuch erwischt, SSL-Zertifikate zu fälschen, um den verschlüsselten Traffic mitlesen zu können:

   (a) *LateNightZ* war ein deutscher Tor-Node, der 2007 beim Man-in-the-Middle-Angriff auf die SSL-Verschlüsselung erwischt wurde.[39]

   (b) *ling* war ein chinesischer Tor-Node, der im Frühjahr 2008 versuchte, mit gefälschten SSL-Zertifikaten die Daten von Nutzern zu ermitteln. Gleichzeitig wurde in China eine modifizierte Version von Tor in Umlauf gebracht, die bevorzugt diesen Node nutzte. Die zeitliche Korrelation mit den Unruhen in Tibet ist sicher kein Zufall.[40]

   (c) Im September 2012 wurden zwei russische Tor-Nodes mit den IP-Adressen 46.30.42.153 und 46.30.42.154 beim SSL-Man-in-the-Middle-Angriff erwischt.

   (d) Im April 2013 wurde der russische Tor-Node mit der IP-Adresse 176.99.10.92 beim SSL-Man-in-the-Middle-Angriff auf Wikipedia und auf IMAPS erwischt.[41]

   Beide russische Tor-Nodes gingen kurz nach ihrer Entdeckung offline. Inzwischen können die Geheimdienste durch Zusammenarbeit mit kompromittierten Certification Authorithies gültige SSL-Zertifikate fälschen. Diese Man-in-the-Middle-Angriffe sind sehr schwer erkennbar.

3. Im Februar/März 2012 haben mehrere Exit-Nodes in einer konzertierten Aktion die HTTPS-Links in Webseiten durch HTTP-Links ersetzt. Wie man damit erfolgreich die SSL-Verschlüsselung aushebeln kann, wurde auf der Black Hack 2009 beschrieben. Die Software für diesen Angriff heißt *ssl-stripe* und ist als Open-Source verfügbar.

```
Bradiex             bcc93397b50c1ac75c94452954a5bcda01f47215
                    IP: 89.208.192.83
TorRelay3A2FL       ee25656d71db9a82c8efd8c4a99ddbec89f24a67
                    IP: 92.48.93.237
lolling             1f9803d6ade967718912622ac876feef1088cfaa
                    IP: 178.76.250.194
Unnamed             486efad8aef3360c07877dbe7ba96bf22d304256
                    IP: 219.90.126.61
ididedittheconfig   0450b15ffac9e310ab2a222adecfef35f4a65c23
                    IP: 94.185.81.130
UnFilTerD           ffd2075cc29852c322e1984555cddfbc6fb1ee80
                    IP: 82.95.57.4
```

4. Im Oktober 2014 wurde ein Tor-Exit-Node aufgespürt, der Windows-Binaries (z. B. DLLs oder EXE-Dateien) beim Download on-the-fly mit dem Trojaner OnionDuke infizierte, einer Variation der russischen Cyberwaffe MiniDuke. Der Trojaner sammelte Login-Daten und spionierte die Netzwerkstruktur der Opfer aus. F-Secure konnten die ersten Infektionen mit OnionDuke auf Oktober 2013 datieren. Der Bad-Exit-Node wurde gefunden, weil ein Sicherheitsforscher gezielt nach diesem Angriff gesucht hatte.[42]

[39] http://www.teamfurry.com/wordpress/2007/11/20/tor-exit-node-doing-mitm-attacks/
[40] http://archives.seul.org/or/talk/Mar-2008/msg00213.html
[41] https://trac.torproject.org/projects/tor/ticket/8657
[42] http://heise.de/-2457271

5. Im April 2015 wurden 70 Bad-Tor-Nodes identifiziert, die den Hidden-E-Mail-Service angegriffen hatten. Die Betreiber von SIGAINT warnten, dass es den Angreifern gelungen sei, den Hidden-Service mit einem Man-in-the-Middle-Angriff zu kompromittieren und möglicherweise Daten inklusive Login-Credentials mitzulesen.[43]

   > *I think we are being targeted by some agency here. That's a lot of exit nodes.*
   > SIGAINT Admin

   Diese 70 Nodes meldeten sich innerhalb eines Monats kurz vor dem Angriff als neue Tor-Nodes im Netzwerk an. Weitere 31 Nodes standen noch im Verdacht, ebenfalls zu dieser Gruppe zu gehören, aber noch nicht aktiv angegriffen zu haben.

6. Um passiv schnüffelnde Tor-Exit-Nodes in eine Falle tappen zu lassen, stellte Chloe im Juni 2015 einen Honigtopf auf und spürte 11 passiv schnüffelnde Exit-Nodes auf. Zwei der elf Nodes hatten Guard-Status.[44]

7. Im März 2016 versuchten 14 Bad Exit Nodes in einer konzertierten Aktion, sich als Man-in-the-Middle in die STARTTLS-Verschlüsselung einiger Jabber/XMPP-Server einzuschleichen.[45] Folgende Jabber-Server waren von dem Angriff betroffen:

   - freifunk.im
   - jabber.ccc.de
   - jabber.systemli.org
   - jappix.org
   - jodo.im
   - pad7.de
   - swissjabber.ch
   - tigase.me

8. Im Mai 2020 wurde eine relativ große Gruppe von Tor Exit Nodes dabei erwischt, mit sslstripe Angriffen die Markplätze von Kryptowährungen anzugreifen. Diese Gruppe von Bad Exits Nodes kontrollierte 23% des gesamten Exit Traffics des Tor Netzwerkes.[46]

   Nachdem diese Bad Exits entfernt wurden, wiederholte im Juni 2020 eine zweite Gruppe von Tor Exit Nodes den sslstripe Angriff auf die Marktplätze. Diese zweite Gruppe kontrolliert 19% des gesamten Exit Traffics des Tor Netzwerkes.

   Im Oktober 2020 hat Roder Dingledine eine dritte große Gruppe von Tor Exit Nodes aus dem Netz entfernt, die man-in-the-middle Angriffe auf TLS-Verbindungen ausführte.[47]

9. Tor-Exit-Nodes aus dem Iran sind generell als Bad-Exits markiert. Diese Nodes unterliegen der iranischen Zensur. Außerdem wird beim Aufruf von Webseiten über diese Nodes von der staatlichen Firewall ein unsichtbarer iFrame aus dem Hidden Internet of Iran[48] eingefügt.

[43] https://lists.torproject.org/pipermail/tor-talk/2015-April/037549.html
[44] https://chloe.re/2015/06/20/a-month-with-badonions/
[45] https://tech.immerda.ch/2016/03/xmpp-man-in-the-middle-via-tor/
[46] https://blog.torproject.org/bad-exit-relays-may-june-2020
[47] https://lists.torproject.org/pipermail/tor-relays/2020-October/019045.html
[48] http://arxiv.org/abs/1209.6398

```
<iframe src="http://10.10.34.34" style="width: 100%;
   height: 100%" scrolling="no" marginwidth="0"
   marginheight="0" frameborder="0" vspace="0" hspace="0">
</iframe>
```

10. Die Unterlagen des Whistleblowers E. Snowden bestätigten, dass NSA und GCHQ passiv schnüffelnde Exit-Nodes betreiben. Die NSA soll damals 10–12 leistungsfähige Tor-Server genutzt haben (aktuelle Angriffe zeigen, dass es inzwischen deutlich mehr sind). Zum Engagement des GSHQ wurden keine Zahlen bekannt.

11. Europol betreibt seit Jahren ein Projekt mit dem Ziel *to provide operational intelligence related to TOR*. Die Formulierung lässt vermuten, dass ebenfalls passiv schnüffelnde Exit-Nodes genutzt werden.

12.4 Finger weg von unseriösen Angeboten

Neben Projekten, die sich wirklich um eine anonyme Lösung für Surfer bemühen, gibt es immer wieder Angebote, die unbedarfte Anwender ködern wollen.

Tor-Boxen

Sogenannte Tor-Boxen wie *Anonabox*[49] oder *SafePlug*[50] leiten als Router den gesamten Traffic eines Computers oder Heimnetzwerkes oder als Proxy nur den HTTP-Traffic durch Tor. Die Anbieter versprechen eine einfachste Installation und gleichzeitig die Anonymität des Tor-Netzwerkes. Aber manchmal ist „einfach“ das *Gegenteil* von „anonym“.

Anonymes Surfen erfordert in erster Linie eine sichere Browserkonfiguration. Wer mit einem beliebigen Browser (z. B. Internet Explorer, Google Chrome oder Safari) ohne datenschutzfreundliche Konfiguration im Internet surft, der kann sich die Nutzung von Tor sparen, denn damit surft man nicht anonym. Die einzige von den Tor-Entwicklern empfohlene Variante zum anonymen Surfen ist die Nutzung des TorBrowserBundle.

> *The most crucial problem with a torifying proxy is that it uses a bring-your-own-browser system, as opposed to a hardened browser, and therefore is susceptible to browser-based privacy leaks. This is why it's better to use the Tor Browser Bundle.*
> (Quelle: Blog TorProject.org)

Web-Proxys

Web-Proxys mit HTTPS-Verschlüsselung sind ein probates Mittel, um Zensur im Internet zu umgehen. Sie sind aber als Anonymisierungsdienste unbrauchbar. Mit kruden HTML-Elementen oder JavaScript ist es möglich, die meisten Web-Proxys auszutricksen und die reale IP-Adresse des Nutzers zu ermitteln.

Die folgende Tabelle zeigt eine Liste bekannter Web-Proxys, die den Anonymitätstest der JonDos GmbH nicht bestehen:

Betreiber	HTML/CSS	JavaScript	Java
Anonymouse	gebrochen	gebrochen	gebrochen
Cyberghost Web		gebrochen	gebrochen
Hide My Ass!		gebrochen	gebrochen
WebProxy.ca		gebrochen	gebrochen
KProxy		gebrochen	gebrochen
Guardster		gebrochen	gebrochen
Megaproxy	gebrochen	nicht verfügbar	nicht verfügbar
Proxify		gebrochen	gebrochen
Ebumna	gebrochen	gebrochen	gebrochen

Free Hide IP

Free Hide IP wird von *Computerbild* als Anonymisierungsdienst angepriesen:

[49] http://anonabox.com/home.php
[50] https://freedom-to-tinker.com/blog/annee/security-audit-of-safeplug-tor-in-a-box/

> *Mit Free Hide IP bleiben Sie beim Surfen im Internet anonym. So sind Sie vor Datensammlern und anderen Gefahren geschützt. Die Free-Version der Software verbindet Sie nach einem Klick auf die Schaltfläche Hide IP mit einem amerikanischen Proxy-Server und vergibt eine neue IP-Adresse für Ihren Rechner.*

Der Dienst erfüllt nicht einmal einfachste Anforderungen. Nutzer können in mehreren Varianten deanonymisiert werden – bspw. ganz einfach mit (verborgenen) HTTPS-Links.

ZenMate

ZenMate will ein VPN-artiger Anonymisierungsdienst sein, der eine einfach zu installierende Lösung für anonymes Surfen verspricht. Man muss auf der Webseite nur einmal kurz klicken, um ein Browser-Add-on zu installieren. Es gibt eine kostenlose Version, die nur die IP-Adresse versteckt. Außerdem steht eine Premium-Version zur Verfügung, die auch Tracking-Elemente blockieren können soll, was aber nicht funktioniert (Abb. 12.19).

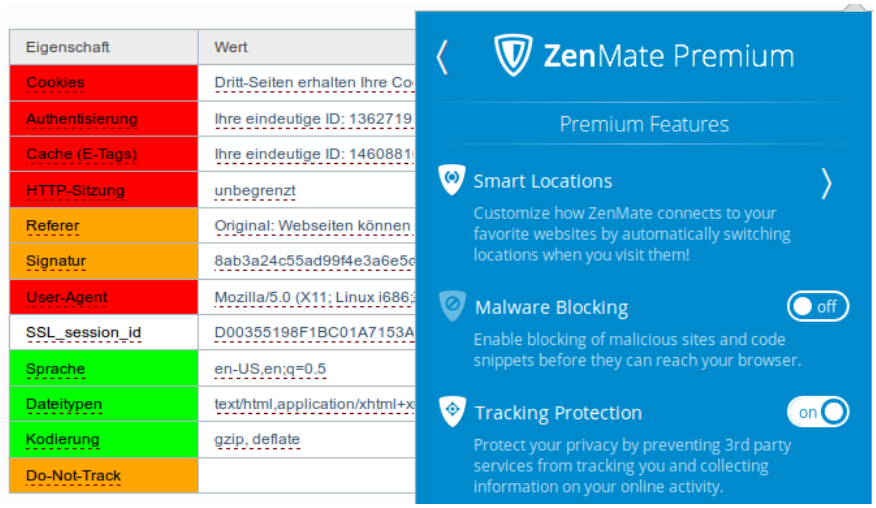


Abbildung 12.19: Tracking-Protection in ZenMate funktioniert nicht

Schlussfolgerung: Das ist nu

Kapitel 13

Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) wurden entwickelt, um vertrauenswürdige Endpunkte über unsichere Netzwerke zu verbinden. Ein VPN schützt gegen folgende Angriffe:

- Ein VPN schützt gegen Angreifer, die nur den verschlüsselten VPN-Traffic beschnüffeln könnten. Dieses Angreifermodell ist die Grundlage für das Konzept.
- Außerdem ändern VPNs die eigene IP-Adresse, die ein Internetdienst sehen kann. Deshalb kann ein VPN gegen Tracking anhand der IP-Adresse schützen und Geo-IP-Sperren umgehen.
- Ein VPN schützt NICHT gegen Angreifer, die neben dem verschlüsselten VPN-Traffic auch den unverschlüsselten Traffic beobachten können, der hinter dem Server rauskommt. Als billige Anonymisierungsdienste sind VPNs daher NICHT geeignet.

Sinnvolle Anwendungen für VPNs sind:

- Im beruflichen Umfeld kann man Außendienstlern (Road Warriors) oder Mitarbeitern im Homeoffice den Zugang ins interne Netz der Firma ermöglichen oder zwei bzw. mehrere Firmenstandorte transparent über das Internet miteinander verbinden.
- Im privaten Bereich kann mit VPNs verwenden, um die Verfolgung der Reisetätigkeit durch Geo-Lokalisierung der IP-Adresse und in nicht vertrauenswürdigen Wi-Fi-Netzwerken (Hotel, Flughafen, U-Bahn o. Ä.) Angriffe durch bösartige Nutzer des Hotspots zu verhindern.

  Ähnlich wie im Beruf ermöglicht ein VPN den Zugriff auf das Heimnetz von unterwegs. Das hat den Vorteil, dass man private Server (NextCloud, Netzwerkspeicher o. Ä.) nicht ins Internet exponieren und damit Hackerangriffen aussetzen muss, um von unterwegs darauf zuzugreifen.

  Außerdem kann man mit einem VPN die Geo-IP-Sperren einiger Medien umgehen. Wenn man einen VPN-Server mit deutscher IP-Adresse verwendet, kann man bspw. auf Mallorca ein bisschen in der ZDF-Mediathek stöbern o. Ä.

  (Das funktioniert aber nicht immer. Die Geo-IP-Sperre von BBC lässt sich bspw. nicht so einfach mit VPNs austricksen, weil die BBC bekannte VPN-Dienste blockiert.)

  Mit einer Verbindung zu einem VPN-Server in einem anderen Land kann man viele nationale oder EU-weite Zensurmaßnahmen umgehen (falls unzensierte DNS-Server nicht ausreichen).

VPN-Technologien

Die für ein VPN notwendige Software steht für unterschiedliche Standards als Open-Source-Software zur Verfügung:

OpenVPN ist ein Klassiker. Die Software arbeitet auf OSI Layer 4 (TCP oder UDP) und nutzt TLS, um den Datenverkehr zwischen zwei Endpunkten zu verschlüsseln. Es funktioniert ähnlich wie HTTPS im Browser. Nachdem ein verschlüsselter TLS-Tunnel aufgebaut wurde, werden Daten durch diesen verschlüsselten Tunnel geschickt. Bei HTTPS im Browser wird HTTP-Traffic durch diesen Tunnel transportiert, bei OpenVPN werden alle Daten durch den TLS-Tunnel gejagt.

Es werden Client-2-Server- und Server-2-Server-Verbindungen unterstützt.

IPsec arbeitet einen Level tiefer auf IP-Ebene und bietet daher eine höhere Robustheit gegen Lauscher, da auch die TCP-Header verschlüsselt werden. Es wird von Regierungsbehörden und Militär bis zur Geheimhaltungsstufe VS-GEHEIM verwendet.

IPsec ist ein komplexes Protokoll und besteht aus mehreren, eigenständigen Teilen:

- Internet Key Exchange (IKE v1/v2) für Schlüsseltausch und -verwaltung;
- Authenticated Header (AH) für die Authentifizierung von Servern und Nutzern;
- Encapsulating Security Payload (ESP) für die Verschlüsselung der Daten.

IPsec kann nicht nur Punkt-zu-Punkt Verbindungen absichern sondern auch komplexe Multi-Side-Topologien realisieren.

WireGuard ist ein relativ junges Projekt, das wie IPsec auf OSI Layer 3 arbeitet. Ziel von WireGuard ist eine VPN-Lösung mit geringer Komplexität in der Protokoll-Spezifikation und Implementierung sowie einer einfachen Anwendung. Der Quellcode umfasst derzeit nur 4.000 Zeilen Code (OpenVPN: 292.000 Zeilen).

Wireguard ist ein Peer-2-Peer-VPN. Jeder Peer stellt einen IP-Adressbereich zur Verfügung, der transparent mit den Netzen der anderen Peers über eine verschlüsselte Verbindung gekoppelt wird. Die Peers authentifizieren sich mit Schlüsseln, die zuvor irgendwie ausgetauscht werden müssen. Eine zusätzliche Authentifizierung von Nutzern wie bei OpenVPN und IPsec gibt es nicht.

Einige VPN-Provider vergewaltigen das Konzept und bauen damit individuelle Client-Server-ähnliche Infrastrukturen, indem die Client-Peers nur eine eigene IP-Adresse für das VPN bereitstellen und auf der Seite des Server das gesamte Internet.

OpenConnect wurde ursprünglich von Cisco entwickelt. Es arbeitet mit UDP (OSI Layer 4) und nutzt DTLS, um den Datenverkehr zwischen einem Client und einem Server zu verschlüsseln. Es ist nicht für Server-2-Server-Verbindungen geeignet.

Iodine versteckt den VPN-Traffic im DNS-Datenverkehr, um VPN-Sperren zu umgehen. Der Datendurchsatz ist viel geringer als bei anderen VPNs.

PPTP Microsofts Point-to-Point-Tunneling-Protocol (PPTP) ist konzeptuell kaputt und sollte nicht mehr verwendet werden.

Daneben gibt es kommerzielle Anbieter für hoch-sichere, zertifizierte VPN-Lösungen. Beispiele dafür sind die Produktlinien genucrypt (von Genua.de) oder SINA (von Secunet.com), die aus Hardware-Software-Kombinationen bestehen und überwiegend (nicht ausschließlich) in kritischen Infrastrukturen wie Energie- und Wasserversorgung sowie bei Behörden eingesetzt werden.

Stealth-VPN-Techniken

Stealth-VPN-Techniken sollen verhindern, dass ein Beobachter erkennt, dass man VPNs verwendet. Damit kann man z. B. einige Firewalls durchtunneln, die VPNs blockieren.

- Die einfachste Stealth-VPN-Technik ist die Verwendung von OpenVPN im TCP-Mode mit Port 443 auf dem Server als Endpunkt. Für einen oberflächlichen Beobachter, der keine Deep-Packet-Inspektion (DPI) einsetzt, sieht es wie die harmlose TLS-verschlüsselte Verbindung eines Webbrowser zu einem Webserver aus (HTTPS).
- Diesen Trick kann man auch für andere VPN-Protokolle wie Wireguard oder IPsec verwenden. Es wird zuerst ein TLS-verschlüsselter Tunnel zum Port 443 zu einem Server aufgebaut und durch diesen Tunnel wird die eigentliche VPN-Verbindung zum VPN-Server initiiert.

  Den TLS-Tunnel könnte man sich mit *stunnel* auf beiden Seiten zusammenbasteln. Einige VPN-Provider haben diese Technik auch in ihre Apps integriert.

Advanced Firewalls mit DPI lassen sich nicht so einfach austricksen. Die staatliche iranische Firewall erkennt zum Beispiel die typischen TLS-Zertifikate von VPN-Providern (und Tor Onion Router) beim Handshake zum Aufbau eines TLS-verschlüsselten Tunnels und blockiert die Verbindung.

- Das SSH-Protokoll verwendet nur nackte Keys und arbeitet nicht mit signierten Zertifikaten wie TLS. Es bietet weniger Merkmale für die Traffic-Analyse via DPI. Man kann auch mit SSH einen verschlüsselten Tunnel zu einem Server aufbauen und durch diesen die VPN Verbindung initiieren. Für einen Beobachter sieht es wie eine Serveradministration aus.
- Obfproxy (Obfuscation Proxy) wurde von TorProject.org entwickelt, um die Erkennung von Tor-Traffic zu verhindern. Man kann diese Technik auch für VPN-Traffic nutzen. Einige VPN-Provider wie IVPN habe es in ihre Apps integriert, wo man es mit einem Klick aktivieren kann.

Einsatzempfehlungen für VPN-Technologien

Ein paar Gedanken zu Einsatzempfehlungen für die unterschiedlichen Technologien:

- OpenVPN ist robust gegen Einschränkungen des Datenverkehrs, wenn man das TCP-Protokoll statt UDP verwendet und den VPN-Server auf Port 443 erreichen kann.

  Manchmal ist man bei Bekannten zu Gast und möchte kurz mal das WLAN nutzen. Der Gast-Zugang ist aber restriktiv konfiguriert und lässt nur HTTPS und HTTP durch (facist firewall). Wenn man auf solche Situationen vorbereitet ist und eine geeignete OpenVPN-Konfiguration mit einem Klick aktivieren kann, sind solche Beschränkungen kein Problem.

- Wireguard ist ein kryptografisch modernes Protokoll mit hoher Performance.

  Nachteilig ist der Schlüsseltausch und die fehlenden Möglichkeiten einer zentralen Nutzerverwaltung. Daher ist es ohne selbstgestrickte Erweiterungen eher für kleine VPNs (weniger als 10 Road Warriors oder Standorte) geeignet, bei denen man die Schlüssel per Hand verteilen kann.

  Das Sicherheitskonzept von Wireguard geht davon aus, dass private Schlüssel lokal auf den Clients erzeugt und nur die Public-Keys ausgetauscht werden. Eine zentrale Erzeugung/Verwaltung privater Schlüssel ist nicht empfehlenswert.

- IPsec/IKEv2 ist ein komplexes Gebäude mit vielen Optionen, dass höchste Sicherheitsansprüche erfüllen kann (military grade security). Aufgrund der Möglichkeiten zur zentralen Verwaltung von Zugriffsrechten ist es für größere VPNs geeignet.

  Da man prinzipiell eine Kompromittierung des VPN-Servers nicht ausschließen kann, ist in größeren, kommerziellen Umgebungen die Verwendung von Smartcards oder Hardware-Security-Modulen (z. B. Nitrokey HSM) für Serverzertifikate sinnvoll. Wenn die Serverzertifikate kompromittiert werden und hundert oder mehr Road Warriors die Zertifikate tauschen müssen, dann hat der Admin ein Problem. Einen kompromittierten Server könnte ein IT-Admin aber schnell ersetzen, HSM-Stick mit dem Serverzertifikat anschließen – fertig.

Sicherheitsempfehlungen von BSI und NSA für VPNs

Das BSI und die NSA geben in ihren Empfehlungen für VPNs mit hohen Sicherheitsanforderungen (für Regierungen, Militär u. Ä.) einige allgemeine Hinweise, die man teilweise auch umsetzen kann, wenn man keine extremen Sicherheitsanforderungen hat.

Kurze Zusammenfassung der BSI- und NSA-Empfehlungen für sichere VPNs:

- Die Verwendung von irgendwelchen TLS-Tunneln auf OSI Layer 4 für VPN-Verbindungen sollte vermieden werden (also kein OpenVPN). Die Verschlüsselung muss auf Layer 3 erfolgen, damit auch die TCP-Header verschlüsselt sind.
- Als VPN-Protokoll wird IPsec/IKE mit aktuellen Ciphern empfohlen.
- IP-Adressen der Endpunkte sind fest zu konfigurieren und sollten nicht von der DNS-Namensauflösung von DNS-Servern abhängen, über die man keine Kontrolle hat.
- Die Authentifizierung von Nutzern sollte nicht mit Passwörtern erfolgen, sondern mit Zertifikaten, die in einem externen Hardware-Security-Modul gespeichert sind (also z. B. Nitrokey). Die PKI zur Verwaltung der Zertifikate für die Nutzer darf nicht ins Internet exponiert werden.
- Funktionen für die Remote-Administration der VPN-Server dürfen nur via VPN zugänglich sein und dürfen nicht in das Internet exponiert werden.

Wenn man konkrete Angebote von VPN-Anbietern mit dieser Liste vergleicht, dann löst sich das PR-Geblubber von *military grade security* ganz schnell wieder in Luft auf.

13.1 VPN Dienste als Billig-Anonymisierer

Aus der Werbung eines VPN-Providers:

> *Verbergen Sie Ihre Online-Identität und surfen Sie anonym im Netz!*

Bullshit! VPNs wurden NICHT als Anonymisierungsdienste konzipiert, sondern für die Verbindung von vertrauenswürdigen Endpunkten über unsichere Netze.

Das Angreifermodell, gegen das VPNs schützen sollen, geht davon aus, dass ein Angreifer nur den verschlüsselten Datenverkehr beobachten oder angreifen kann und nicht den unverschlüsselten Datenverkehr hinter einem der beiden Endpunkte.

Ein VPN als Anonymisierungsdienst zu nutzen, ist wie Suppe mit der Gabel löffeln. Für eine Aufgabe wird das falsche Tool genutzt, das nur einen Teil der Probleme löst.

Für den Einsatz als Billig-Anonymisierer sind VPNs konzeptuell nicht geeignet, weil:

- VPNs verändern lediglich die IP-Adresse eines Internetnutzers. Für Trackingdienste ist die IP-Adresse aber nur ein geringwertiges Trackingfeature. Durch die Verbreitung mobiler Internetnutzung ist der Wert dieses Merkmals weiter gesunken. Modernes Tracking verwendet Fingerprinting und EverCookies, gegen die VPNs nicht schützen. Somit ist durch VPNs keine Anonymität bei Surfen gegeben.

  (Richtige Anonymisierungsdienste wie Tor Onion Router adressieren dieses Problem durch eine einheitliche Browserkonfiguration (TorBrowserBundle), die eine Anonymitätsgruppe schafft, in der einzelne Surfer nicht unterscheidbar sind.)

- Die IP-Anonymisierung von VPNs kann relativ einfach durch Traffic-Korrelation oder Traffic-Fingerprinting ausgehebelt werden. Die mathematischen Grundlagen dafür lernt jeder Informatikstudent im ersten Jahr im Mathe Grundkurs.

  Hermann/Wendolsky/Federrath haben bereits 2009 in dem Paper *Popular Privacy Enhancing Technologies with the Multinomial Naïve-Bayes Classifier*[1] gezeigt, dass man die Nutzer eines OpenVPN-Servers zu 95% durch Beobachtung und Korrelation des Eingangs- und Ausgangstraffics des VPN-Servers deanonymisieren kann ohne die Krypto zu knacken.

  In der Praxis werden vergleichbare Techniken beispielsweise von der Firma Team Cymru eingesetzt, um sogenannte *Bad Actors* im Internet zu identifizieren, die der Meinung sind, sie könnten sich hinter einem VPN-Server verstecken und seien dann anonym. Man muss dabei nicht unbedingt alle VPN-Server weltweit selbst beobachten, sondern kann die benötigten Daten von den Internet-Backbone-Providern kaufen und dann zur Deanonymisierung von VPN-Nutzern auswerten.[2]

  US-Behörden wie die Spionageabwehrbehörde Defense Security Service (DSS) sollten die Netflow Daten zur Deanonymisierung von VPN Nutzern eigentlich bei der NSA abrufen und selbst auswerten. Routine für die Auswertung ist vorhanden. Weil die NSA aber langsam reagiert und oft einige Tage für eine Antwort braucht, kauft beispielsweise das DSS häufig die akkumulierten Netflow Daten von der Firma Team Cymru.[3]

- Ein VPN-Betreiber hat wie ein Internet-Zugangsprovider Zugriff auf das gesamte Nutzungsverhalten. Das erfordert ein hohes Maß an Vertrauen in den VPN-Betreiber, das bei vielen Betreibern nicht gerechtfertigt ist.

  - Der von Facebook betriebene VPN-Dienst Onavo spioniert seine Nutzer aus und speichert, welche Apps und Internetdienste sie verwenden. Damit kann Facebook frühzeitig Konkurrenten erkennen und Maßnahmen zur Sicherung der Marktes ergreifen.
  - Der VPN-Dienst AnchorFree verwendet für das Angebot Hotspot Shield Free JavaScript, um IFrames mit personalisierten Werbeanzeigen zu injizieren und außerdem den Standort des Nutzers zu tracken. Eindeutige Identifikationsmerkmale wie MAC-Adressen und IMEI-Nummern von Smartphones werden an Werbenetzwerke weitergegeben, was die Nutzer gegenüber den Trackingdiensten natürlich deanonymisiert.[4]

[1] https://epub.uni-regensburg.de/11919/
[2] https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru
[3] https://www.golem.de/news/dss-us-behoerde-verfolgt-vpn-traffic-mit-gekauften-netflow-daten-2309-178009.html
[4] https://heise.de/-3795523

Statt einen Gewinn an Privatsphäre zu erhalten, wird man als Nutzer solcher VPN-Dienste noch mehr ausgespäht.

- Bei vertrauenswürdigen VPN-Providern ist zu beachten, dass sie den Gesetzen des jeweiligen Landes folgen müssen. Da diese Dienste wie Zugangsprovider zum Internet arbeiten, kann sich daraus eine deutliche Absenkung der Sicherheit und Privatsphäre ergeben, wenn die Gesetze des Heimatlandes des VPN-Anbieters eine Vorratsdatenspeicherung oder Zugriff auf den Datenverkehr für Geheimdienste fordern.

  Der britische VPN-Dienst HideMyAss (Testsieger beim VPN Magazine[5]) hat z. B. 2011 den LuzSec-Hacker Cody Kretsin, der dem Anonymitätsversprechen von HideMyAss vertraute, an das FBI verraten. Dabei hat HideMyAss nur im Rahmen der gesetzlichen Vorgaben kooperiert. In einem Blog-Artikel verteidigt HideMyAss die Deanonymisierung von Kretsin gegenüber dem FBI.[6]

  Es gibt keinen Grund, einem VPN-Anonymisierer mehr zu vertrauen als einem Internet-Zugangsanbieter wie Telekom, Vodafone o. Ä.

13.2 Empfehlenswerte VPN-Provider

Einige VPN-Provider haben Tracker in ihren Apps integriert, was man für Android-Apps bei Exodus Privacy erfragen kann. Andere werben mit Anonymität beim Surfen oder mit *military grade security*, weil AES256-GCM für die Verschlüsselung der Daten verwendet wird. Um solche VPN-Provider mit irreführender Werbung sollte man einen Bogen machen.

(Für *military grade security* braucht man nicht nur sichere Cipher, sondern auch sichere Speicherung der Schlüssel außerhalb der Arbeitsumgebung auf einem Hardware-Security-Modul. Die VPN-Verschlüsselung muss ebenfalls außerhalb der Arbeitsumgebung erfolgen. Diese Anforderungen erfüllt kein bekannter VPN-Provider.)

Folgende VPN-Provider kann man für die Umgehung geo-spezifischer IP-Sperren, zur Vermeidung von Gefahren in öffentlichen WLANs (Hotel, ICE, Flughafen usw.) oder zur Verhinderung des Trackings von Reisetätigkeiten anhand der IP-Adressen empfehlen:

Mullvad VPN hebt sich durch seriöse Aussagen vom Großteil der VPN-Anbieter ab.[7]

- Mullvad VPN bietet weltweit verteilte OpenVPN- und Wireguard-Server für 5,- Euro pro Monat. Man sollte *owned* Server bevorzugen, bei denen der Anbieter die volle Kontrolle hat.
- Die Smartphone-Apps von Mullvad VPN enthalten keine Tracker und fordern nur die minimal nötigen Berechtigungen.
- Auf PCs kann man die Standardsoftware für OpenVPN oder Wireguard nutzen.
- Um die Probleme beim anonymen Surfen via VPNs zu addressieren, bietet Mullvad den **Mullvad Browser** zum Download an, der auf dem TorBrowserBundle basiert.[8]
  Für die Installation muss man wie beim TorBrowser nur das heruntergelandene Archiv entpacken und kann dann den Browser starten (siehe: Kapitel 12.3.2).

[5] https://www.vpnmagazin.de/hidemyass-test/
[6] http://t3n.de/news/lulzsec-hacker-anonymizer-hidemyass-strafverfolgung-332537/
[7] https://mullvad.net/de/
[8] https://mullvad.net/de/download/browser/

Der Mullvad Browser verwendet selbst keine VPN Server. Das VPN muss man auf Systemebene aktivieren. Es werden die DNS-Server von Mullvad via DNS-over-HTTPS verwendet. Im Gegensatz zum TorBrowser ist das Add-on uBlock Origin standardmäßig eingebaut und es können wie beim TorBrowser drei verschiedene Sicherheitslevel aktiviert werden, wobei der mittlere Level ein guter Kompromiss ist.

Mit dem Browser möchte Mullvad für die Nutzer seines VPN Dienstes ähnlich wie beim TorBrowserBundle eine Anonymitätsgruppe definieren. Deshalb sollte man die Konfiguration des Browsers nicht verändern (auch nicht die Filterlisten uBlock Origin).

Standardmäßig wird DuckDuckGo als Suchmaschine genutzt. Man kann nach eigenen Vorlieben weitere Such-Plugins hinzufügen und als Standardsuche konfigurieren.

Den Mullvad Browser kann man auch ohne VPN Server zum Surfen verwenden oder mit anderen VPN Diensten nutzen - es könnte ein Standardbrowser für VPNs werden.

ProtonVPN hebt sich durch einige Sicherheitsfeatures von anderen Anbietern ab.[9]

- ProtonVPN bietet Wireguard-, OpenVPN- und IPsec/IKEv2-Server mit starker Krypto. Es gibt ein kostenloses Angebot mit wenigen, stark ausgelasteten Servern sowie Premium-Angebote.
- Es ist empfehlenswert, auf Smartphones die Apps von ProtonVPN zu nutzen. Die Apps erfordern nur notwendige Freigaben und enthalten keine Tracker, aber dafür zusätzliche Sicherheitsfeatures wie den *Netzwerk Kill Switch* für Android oder *Always-on-VPN* für iPhones.
- Windows 10, MacOS und Linux unterstützen Wireguard, IPsec/IKEv2 oder OpenVPN mit nativen Clients. Für diese Clients kann man fertige Konfigurationen von der ProtonVPN-Webseite herunterladen.

IVPN.net ist auf Gibraltar registriert. Der Hauptteil des Teams sitzt in Berlin.

- IVPN.net betreibt in 32 Ländern Wireguard-, OpenVPN- und IPsec/IKEv2-Server, die eine sichere Verschlüsselung nach dem aktuellen Stand der Technik bieten.
- Die Apps für Windows, MacOS, Linux und Smartphones sind Open Source und wurden 2021 von Cure53 auditiert. Sie enthalten keine Tracker, dafür zusätzliche Sicherheitsfeatures wie *Netzwerk-Kill-Switch* bzw. *Always-on-VPN* (iOS) und eine Firewall. Für Smartphones kann man die VPN-Apps gegenüber den integrierten Lösungen bevorzugen.
- Bei der Registrierung werden keine Daten erfasst, kein Name, keine Telefonnummer oder E-Mail-Adresse. Es wird eine Account-ID generiert, die man kopieren muss.
- Für die Bezahlung bietet IVPN.net flexible Laufzeiten mit opt-in für eine automatische Verlängerung sowie anonyme Zahlung per Cash-Brief. Beim Test gab es ein paar Probleme. Bezahlung mit einer Kreditkarte war nicht möglich.

  Der Support von IVPN kommentierte:

  > *We occasionally see the bank or financial institution associated with the credit or debit card block payments because it looks suspicious to them. We are located in Gibraltar, so this is not entirely unexpected.*

  Die Bezahlung mit Bitcoin schied wegen der hohen Mining-Gebühren von 100-800 % für die Zahlung aus. Bei In-App-Bezahlung mit iPhones zahlt man 15 % Aufschlag für die Provision an Apple.

[9] https://protonvpn.com/de/

Bei den VPN-Bewertungen bei VPNmentor oder Wizecase belegen in der Regel die VPN-Anbieter **CyberGost**, **Expressvpn** und **Privat Internet Access** die vordersten Plätze.

Die Webseiten VPNmentor und Wizecase gehören der Firma *Kape* (früher unter dem Namen *Crossrider* bekannt) und dieser Firma gehören auch die VPN Dienste CyberGost (seit 2017), Expressvpn (seit 2021) und Privat Internet Access (Ohhh!). Kape setzt ein erhebliches PR-Budget für SEO-Optimierung sowie dafür ein, die eigenen VPN-Dienste auf anderen Webseiten schönschreiben zu lassen. Gründer der Firma Crossrider, die jetzt Kape heißt, hatten gute Beziehungen zu Unit 8200 (israelisches Äquivalent zu NSA und GCHQ).[10]

Warnung für iPhone-Nutzer

Auf iPhones ist es nicht möglich, den Datenverkehr ins Internet vollständig durch ein VPN zu jagen. Apple-Dienste wie Push-Services telefonieren am VPN vorbei, die GMail-App kontaktiert IMAP-Server am VPN vorbei und andere Probleme bestehen seit Jahren.

Mullvad[11] und ProtonVPN[12] empfehlen folgendes Vorgehen, um die Probleme mit bestehenden Verbindungen zu reduzieren, die beim Starten eines VPNs nicht getunnelt werden:

1. VPN-App starten und eine Verbindung zum VPN-Server herstellen.
2. Flugmodus aktivieren, damit alle bestehen Verbindungen unterbrochen werden.
3. WLAN deaktivieren (falls aktiviert) und wieder aktivieren (falls benötigt).
4. Flugmodus wieder deaktivieren. Die Verbindung zum VPN-Server wird aufgebaut und alle neuen Verbindungen (außer Systemkommunikation) geht durch das VPN.

GrapheneOS: DNS-Leaks in Non-Owner-Profilen bei VPN + Private DNS

Wenn man in GrapheneOS mit mehreren Nutzerprofilen arbeitet, in einem Non-Owner-Profile ein VPN für den gesamten Netzwerk-Traffic aktiviert hat und dabei aber nicht den DNS-Server des VPN-Providers verwendet, sondern einen DNS-over-TLS- bzw. DNS-over-HTTPS-Server (Private DNS), dann geht der DNS-Datenverkehr am VPN vorbei.

Die Dokumentation von GrapheneOS empfiehlt, die DNS-Server des VPN-Providers zu nutzen.

ProtonVPN empfiehlt in den FAQ generell für alle Android-Versionen, bei der Nutzung der VPN-Apps die DNS-over-TLS- bzw. DNS-over-HTTPS-Server (Private DNS) zu deaktivieren.

13.3 VPNs für kleine Firmen oder für das Heimnetz

Unabhängig von der eingesetzten VPN-Technologie gibt es ein paar allgemeine Tipps für die Einrichtung eines VPN-Zugangs zum Heimnetz oder in ein kleines Firmennetzwerk.

[10] https://www.michaelhorowitz.com/VPNs.on.iOS.are.scam.php
[11] https://mullvad.net/en/blog/2020/5/4/ios-vulnerability-puts-vpn-traffic-risk/
[12] https://protonvpn.com/blog/apple-ios-vulnerability-disclosure/

Einfaches Konzept (für Einsteiger)

Wenn man nicht in finstere Abgründe der IT abtauchen will, könnte man die VPN-Funktionalitäten von modernen Routern der mittleren oder höheren Preiskategorie verwenden. Wenn man sich via VPN aus dem Internet mit dem eigenen Router verbindet, hat man praktisch die gleichen Möglichkeiten wie bei einer Verbindung via WLAN zuhause auf der Couch. So kann man von unterwegs auf alle heimischen Ressourcen zugreifen, ohne die privaten Server ins Internet exponieren zu müssen (Abb. 13.1).

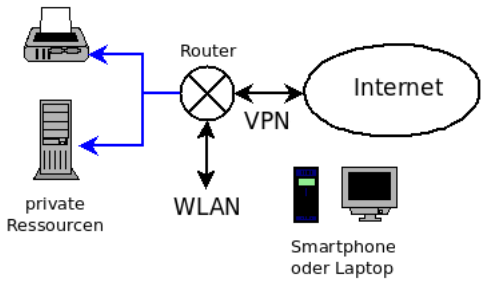


Abbildung 13.1: VPN mit dem eigenen Internetrouter

- Fritz!Boxen mit Fritz!OS ab Version 7.50 können ein Wireguard-VPN bereitstellen, das den aktuellen Sicherheitsanforderungen an VPNs entspricht.

  Ältere Version von Fritz!OS beherrschen nur IPsec/IKEv1 mit schwachen Krypto-Parametern, das man mit aktuellen Smartphones nicht mehr verwenden kann.

- Telekom Router ab der Baureihe Speedport Smart 3/4 enthalten ebenfalls Wireguard.

  Bei den Speedport Smart 3 kann eine VPN Verbindung für einen einzelnen Nutzer erstellt werden. Bei den Speedport Smart 4 kann man mehrere VPN Zugänge konfigurieren.

Sicheres Konzept (für Professionals)

Der Netzwerkplan für die Platzierung eines VPN-Serves als Zugangsschutz vor einem privaten Heim- oder Firmennetz könnte grob gezeichnet wie in Abb. 13.2 aussehen.

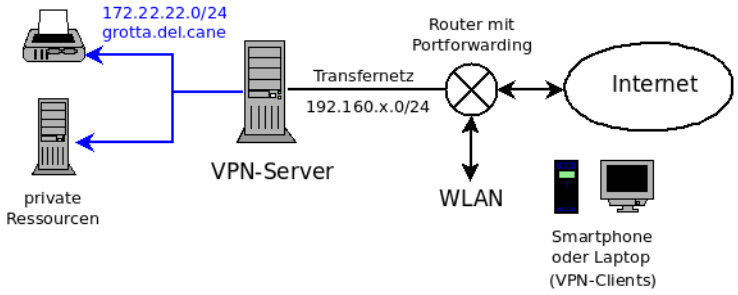


Abbildung 13.2: Netzwerkplan für ein privates VPN oder für eine kleine Firma

- Das private, geschützte Netz hat im Beispiel den DNS-Suffix *grotta.del.cane*. Einzelne Server können via DNS z. B. als *cloud.grotta.del.cane* oder via IP-Adresse angesprochen werden. Der Zugriff auf diese Ressourcen ist von überall auf der Welt nur via VPN möglich.

- Der VPN-Server kann gleichzeitig die Aufgaben einer Firewall übernehmen. Es gibt wartungsarme Appliances für diese Aufgabe wie NitroWall von der Nitrokey GmbH. Man muss sich keinen Server zusammenbasteln.
- Über das Transfernetz ist der VPN-Server mit dem Router verbunden.
- Der Router ist über einen dynamischen DNS-Namen (DynDNS-Adresse, s. u.) oder eine feste IP-Adresse aus dem Internet erreichbar. Diese öffentliche Adresse des Routers wird auf den VPN-Clients (Road Warriors) als Endpunkt für die VPN-Verbindungen konfiguriert.
- Eingehender VPN-Traffic von den VPN-Clients aus dem Internet wird via Port-Forwarding an den VPN-Server weitergeleitet und nicht auf dem Router verarbeitet.

Auch bei der Nutzung des WLAN kann man nur per VPN auf die privaten Ressourcen zugreifen. (So kann man Gästen einen WLAN-Zugang geben, ohne die privaten Ressourcen zu gefährden.)

13.3.1 DynDNS-Adresse einrichten

Wenn der Internet-Provider keine feste IP-Adresse für den Anschluss bereitstellt, benötigt man einen DynDNS-Account. Dieser Account stellt einen dynamischen DNS-Namen zur Verfügung, unter dem der eigene Router bei wechselnden IP-Adressen aus dem Internet erreichbar ist.

1. Voraussetzung ist, dass dem Router auf der externen Seite eine öffentliche IP-Adresse zugewiesen wird. Bei DS-Lite Tunneln (IP: 192.0.0.0 - 192.0.0.7) oder Carrier-Grade-NAT Adressen (IP: 100.64.0.0 - 100.127.255.255) ist der Router nicht aus dem Internet erreichbar.

   Die externe IP-Adresse findet man im *Online Monitor* in der Sektion *Internet*. Sollte es eine Adresse aus den oben genannten Bereichen sein, muss man sich an den Provider wenden und um die Zuweisung einer öffentlichen IP-Adresse bitten (möglicherweise kostenpflichtig).

2. Bei Fritz!Boxen bekommt man mit der Registrierung bei MyFritz! auch eine DynDNS Adresse zugeteilt. Wer seinen Router bei MyFritz! registriert hat, muss nichts weiter tun.

3. Der Anbieter deSEC bietet kostenlose (spendenfinanzierte!) DynDNS-Accounts, die DNSSEC-signiert werden und die man sehr einfach und anonym anlegen kann.

4. Auf der Webseite zur Registrierung wählt man den Namen für die Subdomain und gibt eine E-Mail-Adresse an. Es wird eine E-Mail mit Verifikationslink geschickt. Wenn man auf den Link klickt, werden die benötigten Daten angezeigt.

   Es ist empfehlenswert, die Daten in einem Passwortmanager wie KeepassXC zu speichern, falls man mal einen neuen Router konfigurieren muss. ;-)

5. Diese Daten gibt man im Router bei der DynDNS-Konfiguration ein. Abb. 13.3 zeigt die Konfiguration in der Fritz!Box.

6. Der DynDNS-Name wird auf den VPN-Clients (Road Warriors) als Endpunkt für den VPN-Server verwendet.

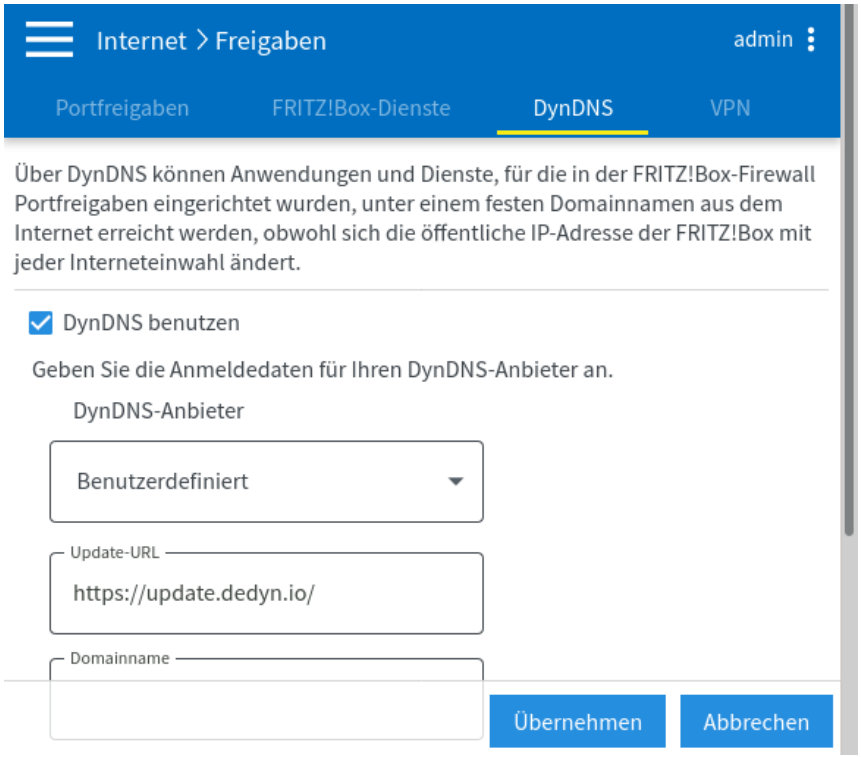


Abbildung 13.3: DnyDNS bei der Fritz!Box einrichten

13.3.2 WireGuard VPN mit Speedport Smart 3/4 Routern

Die Speedport Smart 3/4 Router der Telekom bieten einen einfach bedienbaren Assistenten, um WireGuard VPN Verbindungen in das heimische LAN zu konfigurieren. Auf den älteren Speedport Smart 3 kann man nur eine VPN Verbindung konfigurieren, die man aber auf mehreren Geräten nutzen kann. Bei den Speedport Smart 4 Routern kann man mehrere Verbindungen anlegen.

1. Als erstes benötigt man einen DynDNS Account, der einen DNS Namen bereitstellt, unter dem der eigene Router bei wechselnden IP-Adressen aus dem Internet erreichbar ist.

2. Auf den Clients ist die WireGuard App (Smartphones) bzw. die Wireguard Software (Windows, Linux, MacOS) zu installieren, unter Linux wie folgt:

   ```
   Ubuntu: > sudo apt install wireguard
   Fedora: > sudo dnf install wireguard-tools
   ```

3. Die VPN Konfiguration findet man unter *Netzwerk → Virtuelles Netz (VPN)*. Für eine neue Wireguard Verbindung legt man einen Namen fest und klickt auf *Aktivieren*.

4. Im nächsten Schritt kann man mit WireGuard App auf dem Smartphone den QR-Code scannen oder die Konfiguration für Laptops herunterladen und dort importieren.

   HINWEIS: Man muss WireGuard auf dem Smartphone jetzt(!) konfigurieren oder die Konfiguration herunterladen. Später hat man keinen Zugriff mehr auf die Konfigurationsdaten, weil der Router die privaten Schlüssel für die Clients nicht speichert.

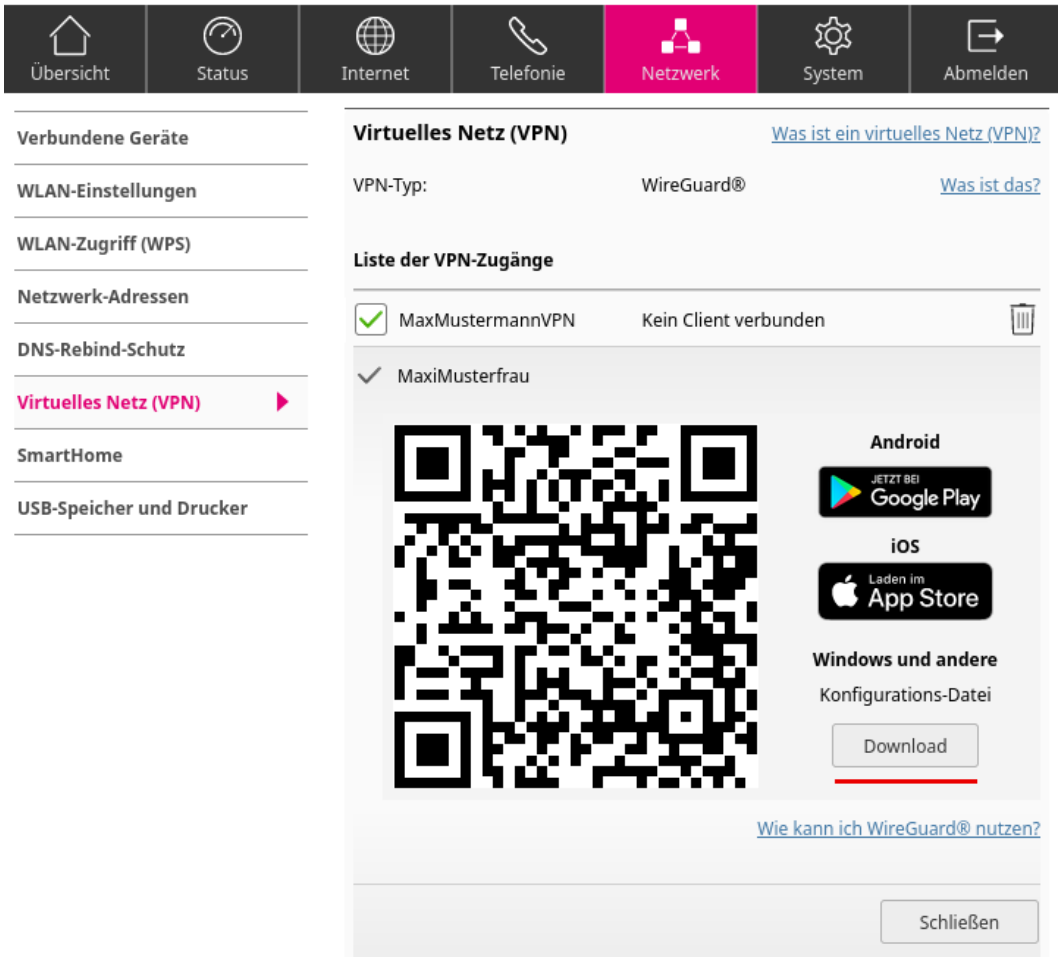


Abbildung 13.4: WireGuard VPN Verbindung im Speedport Smart Router erstellen

5. Wenn man die WireGuard Verbindung auf dem Smartphone oder Laptop aktiviert, hat man Zugriff auf die internen Ressourcen im privaten Heim- oder Firmennetz.

   Mit dem Parameter *Allowed IPs* in der WireGuard Konfiguration auf den Clients kann man das Verhalten steuern, ob der gesamte Datenverkehr des Smartphone/Laptops über die Fritz!Box geroutet werden soll oder ob nur der Zugriff auf private Ressourcen via VPN erfolgen soll.

   - Den gesamten Datenverkehr schickt man wie folgt zur Fritz!Box:

     ```
     AllowedIPs = 0.0.0.0/0,::/0
     ```

   - Wenn man nur Zugriff auf private Ressourcen via VPN haben will, trägt man das private Netzwerk dort ein. (xxx ist durch die konkrete Netzwerkkonfiguration im Heimnetz zu ersetzen.)

     ```
     AllowedIPs = 192.168.xxx.0/24
     ```

6. Damit alles reibungslos funktioniert und man sich so richtig *wie zuhause* fühlt, sollte auf den Smartphones/Laptops der heimische DNS Server genutzt werden, der in der Wireguard Konfiguration steht und zusammen mit dem Einschalten des VPN aktiviert wird.

In Kombination mit VPNs sollte man verschlüsseltes DNS (DNS-over-TLS oder DNS-over-HTTPS) auf den Smartphones/PC deaktivieren(!) und statt dessen den heimischen DNS Server auf dem Router oder Pi-hole richtig konfigurieren. Dann kann man auch via VPN auf die privaten Ressourcen im heimischen Netzwerk problemlos via DNS Namen zugreifen.

13.3.3 Fritz!VPN mit der Fritz!Box

AVM hat in Fritz!OS folgende Möglichkeiten für VPN Verbindungen implementiert:

1. Fritz!OS ab Version 7.39 bietet als VPNs Wireguard und IPsec/IKEv2 mit preshared Keys, die aktuellen Sicherheitsanforderungen an VPN Verbindungen entsprechen.

   - WireGuard ist auf der Fritz!Box Seite am einfachsten konfigurierbar. Auf der Clientseite benötigt man zusätzlich die Wireguard Software, die man zusätzlich installieren muss.
   - IPsec/IKEv2 kann auf Smartphones (Android, iPhones) mit der Systemsoftware genutzt werden und erfordert keine zusätzliche Softwareinstallationen.

   Beide Optionen kann man im Mischbetrieb verwenden.

2. Ältere Versionen von Fritz!OS bieten für VPNs nur IPsec/IKEv1 mit preshared Keys. Es werden schwache DH Parameter verwendet (DH Group 2 mit 1024 Bit für den initialen Schlüsseltausch). Diese VPN-Verbindungen können von potenten Angreifern seit Jahren on-the-fly aufgebrochen werden und sind mit aktuellen Smartphones nicht nutzbar.

Man kann das Fritz!VPN verwenden, um sich von unterwegs ins heimische Netz einzuwählen (um die eigenen Server zu nutzen oder um die Gefahren durch unsichere Hotspots zu minimieren). Außerdem könnte man in kleineren Firmen Außenstellen mit der zentralen IT verbinden.

Fritz!VPN ist aber zur Anonymisierung des gesamten ausgehenden Traffics ungeeignet. Es ist zwar prinzipiell möglich, den ausgehenden Datenverkehr zu einem VPN Server (ProtonVPN o.ä.) weiterzuleiten, aber die Nutzer haben keine Kontrolle, ob diese Upstream VPN Verbindung wirklich besteht. Es gibt keinen Kill Switch, der Datenverkehr ohne VPN blockieren würde, und die VPN Verbindung kann beim Routerneustart (z.B. bei Updates) oder Eingriffen des ISP via Wartungsinterface verloren gehen, ohne das die Nutzer es bemerken würden.

Eine VPN Verbindung zu Upstream VPN Servern (ProtonVPN, Mullvad...) ist immer auf den Endgeräten einzurichten, wo man die volle Kontrolle über den Zustand der Verbindung hat.

Anleitung für WireGuard (Fritz!OS ab Version 7.39)

1. Als erstes benötigt man einen DynDNS Account, der einen DNS Namen bereitstellt, unter dem die eigene Fritz!Box bei wechselnden IP-Adressen aus dem Internet erreichbar ist.

2. Auf den Clients ist die WireGuard App (Smartphones) bzw. die Wireguard Software (Windows, Linux, MacOS) zu installieren.

3. Auf der Fritz!Box muss man unter *Internet* → *Freigaben* auf dem Reiter *VPN (WireGuard)* für jeden Client (Smartphone oder Laptop) eine eigene VPN Verbindung erstellen.

   Im Assistenten wählt man die *Vereinfachte Einrichtung* für die Anbindung von Clients.

   Dann gibt man der Wireguard Verbindung noch einen wiedererkennbaren Namen.

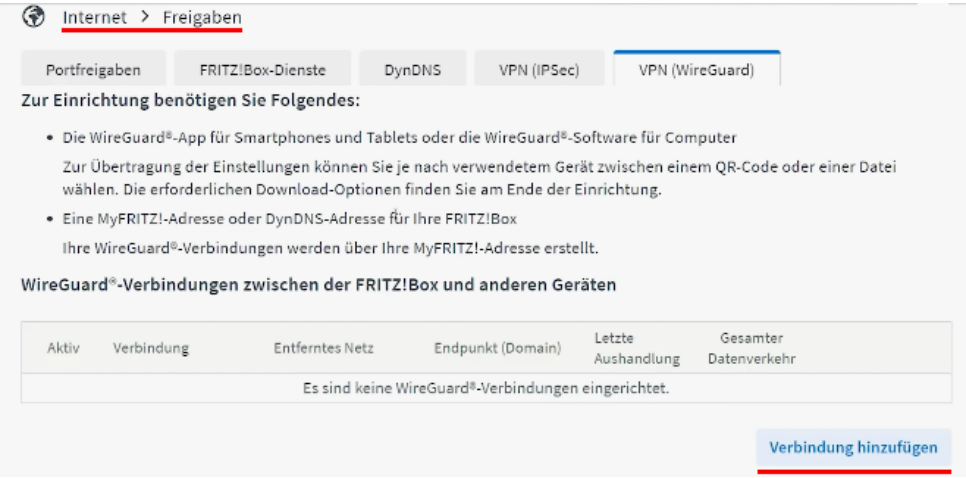


Abbildung 13.5: Fritz!Box: WireGuard VPN Verbindung erstellen

Im nächsten Schritt kann man mit WireGuard App auf dem Smartphone den QR-Code scannen oder die Konfiguration für Laptops herunterladen und dort importieren.

HINWEIS: Man muss WireGuard auf dem Smartphone jetzt(!) konfigurieren oder die Konfiguration herunterladen. Später hat man keinen Zugriff mehr auf die Daten, weil die privaten Schlüssel für die Clients nicht auf der Fritz!Box gespeichert werden.

4. Wenn man die WireGuard Verbindung auf dem Smartphone oder Laptop aktiviert, hat man Zugriff auf die internen Ressourcen im privaten Heim- oder Firmennetz.

   Mit dem Parameter *Allowed IPs* in der WireGuard Konfiguration auf den Clients kann man das Verhalten steuern, ob der gesamte Datenverkehr des Smartphone/Laptops über die Fritz!Box geroutet werden soll oder ob nur der Zugriff auf private Ressourcen via VPN erfolgen soll.

   - Den gesamten Datenverkehr schickt man wie folgt zur Fritz!Box:

     ```
     AllowedIPs = 0.0.0.0/0,::/0
     ```

   - Wenn man nur Zugriff auf private Ressourcen via VPN haben will, trägt man das private Netzwerk dort ein. (xxx ist durch die konkrete Netzwerkkonfiguration im Heimnetz zu ersetzen.)

     ```
     AllowedIPs = 192.168.xxx.0/24
     ```

Anleitung für IPsec/IKEv1 (ältere Fritz!OS-Versionen)

1. Als erstes benötigt man auch wieder einen DyDNS Account, der einen DNS Namen bereitstellt, unter dem die eigene Fritz!Box bei wechselnden IP-Adressen aus dem Internet erreichbar ist.

2. Die Daten für den DynDNS Account gibt man in der Fritz!Box bei der DynDNS Konfiguration ein unter *Internet - Freigaben - DynDNS*.

3. Danach erstellt man unter *System -> Fritz!Box-Benutzer* einen oder mehrere Accounts und gibt diesen Nutzern das Recht, VPN-Verbindungen zur Fritz!Box aufzubauen.

Weitere Zugriffsrechte sollten VPN-Nutzern nicht eingeräumt werden. Für Zugriffe auf Daten (NAS-Inhalte usw.) können separate Accounts eingerichtet werden.

Es ist empfehlenswert, für jedes Gerät einen eigenen Account zu erstellen, damit man den Account bei Bedarf sperren kann, ohne andere Geräte zu beeinträchtigen.

4. Abschließend konfiguriert man die VPN-Verbindung auf den Clients. Die notwendigen Daten sowie eine Anleitung für Smartphones werden mit Klick auf den Link *VPN-Einstellungen anzeigen* für den Fritz!Box Nutzer angezeigt.

   Android 12 kann ein Fritz!VPN nicht mehr verwenden (zu unsicher).

   iPhones könnten das Fritz!VPN nutzen und das Protokoll *IPsec* wählen.

   Aber es ist kein *Always-on-VPN* realisierbar. Die VPN-Verbindung wird geschlossen, wenn kein mehr Datenverkehr fließt. Da es außerdem keine Anzeige für eine bestehende VPN-Verbindung mehr gibt, weiß man beim Starten einer App nicht, ob vielleicht noch eine VPN-Verbindung besteht oder nicht mehr. Das ist sehr unpraktisch und auch unbrauchbar.

   Linuxer können auf ihrem Laptop mit einem Klick auf das NetworkManager Applet ein VPN hinzufügen und wählen *Cisco compatible VPN (vpnc)* aus. Falls diese Option nicht zur Verfügung steht sind folgende Pakete zu installieren:

   ```
   Ubuntu: > sudo apt install networkmanager-vpnc
   ↪ networkmanager-vpnc-gnome
   Fedora: > sudo dnf install NetworkManager-vpnc
   ↪ NetworkManager-vpnc-gnome
   ```

   In den Einstellungen für das VPN ist der DynDNS Name als Gateway einzugeben, der Account auf der Fritz!Box als Username und Gruppenname, das Passwort des Nutzers sowie als Gruppenpasswort das IPsec Shared Secret.

   Um die Sicherheit ein bisschen zu verbessern, kann man mit Klick auf den Button *Erweitert...* die Krypto Parameter anpassen und die IKE DH Group 5 auswählen (1536 Bit), die von Fritz!VPN ebenfalls unterstützt wird.

13.4 IPsec/IKEv2 VPN Client mit Windows 10

Windows 10 enthält eine vollständige Implementierung von IPsec. Man könnte sich einen IPsec Client in Einstellungen für *Netzwerk und Internet* zusammenklicken. Vollständigen Zugriff auf alle Parameter hat man nur mit der Powershell. Eine Übersicht über alle VPN Client Cmdlets der Powershell findet man in der Dokumentation von Microsoft.

1. Eine IPsec VPN-Verbindung wird mit folgendem Cmdlet erstellt:

   ```
   PS C:\> Add-VPNConnection -AllUserConnection -Name "meinVPN"
   -ServerAddress 1.2.3.4 -TunnelType "Ikev2"
   -AuthenticationMthod "EAP" -RememberCredential
   ```

   - Es wird eine IPsec VPN Verbindung für alle Anwender erstellt.
   - Der Name kann frei gewählt werden. Er dient nur der Anzeige und wird in den folgenden Kommandos verwendet, im die VPN-Verbindung auszuwählen.

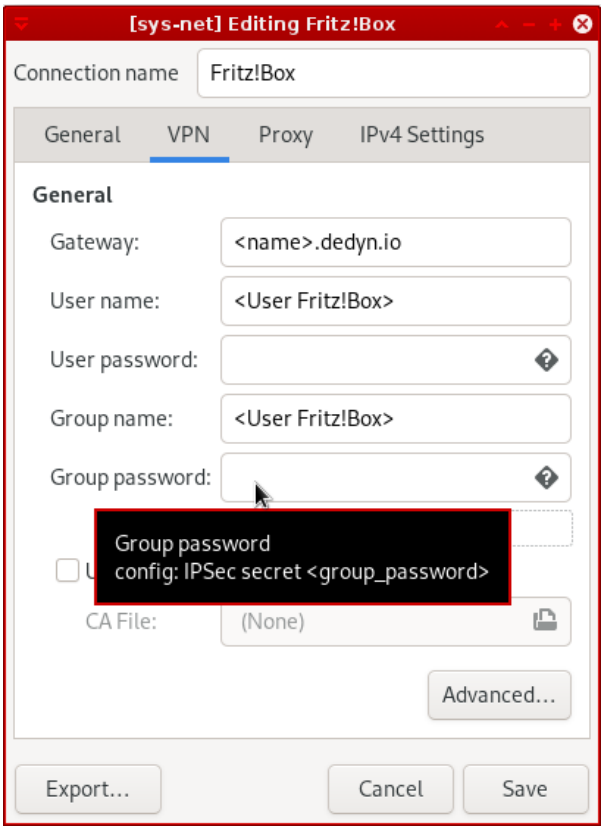


Abbildung 13.6: Fritz!VPN im NetzworkManager konfigurieren

- Der VPN-Server hat im Beispiel die IP-Adresse 1.2.3.4. Man kann auch einen DNS Namen angeben. Die DNS Namen der VPN Server findet man auf der Webseite des VPN-Providers.
- Die Authentifizierung beim Server erfolgt mit Username/Passwort (EAP).
- Die Login Credentials werden beim ersten Login abgefragt und dauerhaft gespeichert. Wenn man die Credentials nicht speichern möchte, kann man den letzten Parameter weglassen.

2. Standardmäßig vertraut Windows 10 den Certification Authorities (CAs) im Store, um die Identität des VPN-Servers anhand seines X509v3 Zertifikates zu bestätigen.

   Unter Umständen kann es nötig sein, das Root Zertifikat von der Webseite des VPN Providers herunter zu laden, wenn der VPN Provider aus Sicherheitsgründen eine eigene CA verwendet statt der bekannten Certification Authorities. Bei ProtonVPN muss man z. B. das Zertifikat der ProtonVPN Root CA[13] herunterladen und dann mit folgendem Befehl in den Store importieren:

   ```
   PS C:\> Import-Certificate -CertStoreLocation Cert:\LocalMachine\Root
   -FilePath "C:\Users\XYZ\Download\ProtonVPN_ike_root.der"
   ```

   Um Man-in-the-Middle-Angriffe zu erschweren, kann man das CA Root Zertifikat festlegen, mit dem das Zertifikat des VPN Server signiert sein muss (CA Pinning).

[13] https://protonvpn.com/download/ProtonVPN_ike_root.der

Wenn man ProtonVPN verwendet, könnte man nach dem Import des Root Zertifikat mit folgenden Powershell Kommandos die CA für diese VPN Verbindung festlegen:

```
PS C:\> $ca = Get-ChildItem Cert:\LocalMachine\Root | ? Subject
↪  -EQ 'CN=ProtonVPN Root CA'
PS C:\> Set-VpnConnection -ConnectionName "meinVPN"
↪  -MachineCertificateIssuerFilter $ca
```

Der erste Befehl filtert das CA Root Zertifikat der Liste der vertrauenswürdigen CAs. Der zweite Befehl legt fest, dass dieses Root Zertifikat die Identität des VPN-Servers bestätigen muss.

3. Ein guter VPN Provider wird seine Server so konfigurieren, das nur sichere Cipher für die Verschlüsselung verwendet werden. Wenn man den Admins des VPN-Servers diesbezüglich nicht vertraut, kann man mit folgendem Cmdlet die VPN Verbindung anpassen, um sichere Ciphersuiten gemäß NSA Suite-B-128 zu erzwingen:

   ```
   PS C:\> Set-VpnConnectionIPsecConfiguration -ConnectionName "meinVPN"
   -CipherTransformConstants GCMAES128 -EncryptionMethod AES128
   -PfsGroup ECP256 -DHGroup ECP256 -IntegrityCheckMethod SHA256
   -AuthenticationTransformConstants SHA256128
   ```

4. Man kann festlegen, dass bestimmte Anwendungen nur via VPN genutzt werden. Es wird automatisch das VPN gestartet, wenn eine der definierten Anwendungen gestartet wird. Man definiert VPN-only Anwendungen mit folgendem Cmdlet:

   ```
   PS C:\> Add-VpnConnectionTriggerApplication -ConnectionName "meinVPN"
   -ApplicationID <Path> | <Package Family Name>
   ```

   Legacy Anwendungen werde dabei über den Path der EXE-Datei spezifiziert, moderne Anwendungen werden über den Package Family Name referenziert.

13.5 Verschiedene VPN Lösungen für Linux

1. Linuxer können die Apps der VPN-Provider nutzen, wenn sie den gesamten Datenverkehr über einen VPN-Server leiten wollen. Das ist die einfachste Variante, bei der man Konfigurationsfehler vermeidet. Außerdem hat man in dem GUI einfachen Zugriff auf alle Server des Providers und kann mit einem Klick wechseln, um ein Land als Exit zu wählen und Geo-IP Sperren zu umgehen.

   Die VPN Apps der VPN-Provider leiten rigoros den gesamten Traffic durch das VPN und verhindern (in der Regel) zuverlässig DNS- oder IPv6 Leaks.

2. Linux bietet für Interessierte auch die Möglichkeit, mit Boardmitteln ein VPN oder mehrere VPNS zu konfigurieren (IPsec/IKEv2, Wireguard, OpenVPN). Damit ist man flexibler und kann sich viele interessante Konfigurationen bauen. Ein paar Beispielanwendungen:

   - Man könnte unterwegs normal surfen und gleichzeitig Zugriff auf das interne Netz der Firma oder Ressourcen im privaten Heimnetz haben (Road Warrior).

- Man könnte zuhause den Internet Datenverkehr über einen VPN-Server leiten, um Zensur oder Geo-IP Sperren zu umgehen, und gleichzeitig die Ressourcen im eigenen Heimnetz nutzen.
- Man könnte beides kombinieren und als Road Warrior den normalen Internet Traffic über einen VPN-Provider schicken und gleichzeitig ein zweites VPN für den Zugriff auf die heimischen Ressourcen oder Server der Firma verwenden.

Wenn der gesamte Datenverkehr zu einem VPN-Provider gehen soll, muss man sich auch selbst um DNS- oder IPv6-Leaks kümmern, wenn man die VPN-Verbinung mit Boardmitteln konfiguriert. Dabei handelt es sich nicht um Bugs (im Sinne einer Fehlfunktion des VPN) sondern um Features im Routing, die man durch geeigente Konfiguration vermeiden kann.

13.5.1 OpenVPN mit Linux

OpenVPN hat den Vorteil, dass es unter Linux auf Client Seite sehr einfach zu konfigurieren ist. Die nötige Software ist in Regel standardmäßig installiert oder wird nachinstalliert:

```
Ubuntu: > sudo apt install openvpn network-manager-openvpn-gnome
Fedora: > sudo dnf install openvpn NetworkManager-openvpn-gnome
```

Die VPN-Provider oder die Administratoren der IT-Abteilung einer Firma können eine OpenVPN Konfigurationsdatei zum Download bereitstellen, die man importiert. Beispiel:

```
client
proto tcp
port 443

auth-user-pass

remote-random
remote 37.120.217.162
remote 37.120.217.82
remote 194.126.177.6
remote 89.36.76.130
remote 194.126.177.14

dev tun
tun-mtu 1500
tun-mtu-extra 32
mssfix 1450
persist-key
persist-tun

comp-lzo no
reneg-sec 0
remote-cert-tls server
pull
fast-io
verb 3
```

```
<ca>
-----BEGIN CERTIFICATE-----
MIIFozCCA4ugAwIBAgIBATANBgkqhkiG9w0BAQ0FADBAMQswCQYDVQQGEwJDSDEV
MBMGA1UEChMMUHJvdG9uVlBOIEFHMRowGAYDVQQDExFQcm90b25WUE4gUm9vdCBD
...
-----END CERTIFICATE-----
</ca>
key-direction 1
```

Das Beispiel zeigt eine OpenVPN Client Konfiguration, die TCP statt UDP verwendet. Es wird ein zufällig ausgewählter Server aus der Liste auf Port 443 (HTTPS) kontaktiert, um problemlos durch alle Firewalls zu kommen. Die Authentifizierung des Nutzers erfolgt mit einer Username/Passwort Kombination ohne Zertifikat. Der Server muss sich mit einem Zertifikat authentifizieren, dass von der CA signiert wurde. Die IP-Adressen der Server kann man per Hand mit den Kommandos *dig* oder *resolvectl* ermitteln, wenn der VPN-Provider nur DNS Namen der Server bereitstellt, z B. für deutsche Server von ProtonVPN:

```
> resolvectl query de.protonvpn.com
```

Üblicherweise überlässt man es dem professionellen Admin der/des Server(s), die Cipher für die Verschlüsselung festzulegen. Unter Umständen möchte man die Cipher aber selbst festlegen, wenn man dem Admin die Kompetenz für eine sichere Konfiguration nicht zutraut oder wenn man zur Verbesserung der Performance lieber AES-128 statt AES-256 verwendet (was normalerweise völlig ausreicht).

Die verfügbaren Cipher kann man sich mit folgendem Kommando anzeigen lassen:

```
> openvpn --show-ciphers
```

In der Konfiguration könnte man z. B. folgenden Parameter ergänzen:

```
# Cipher für die Verschlüsselung der Daten
cipher AES-128-GCM
```

Unter Linux fügt man ein VPN im NetworkManager hinzu, der auch LAN- und WLAN-Verbindungen verwaltet. Nachdem man die OpenVPN Konfiguration von der Webseite des VPN-Providers herunter geladen und evtl. etwas angepasst hat, wählt man *VPN hinzufügen* und im ersten Dialog die Option *Aus Datei importieren...*.

Im folgenden Dialog muss man dem VPN noch einen Namen für die Anzeige geben und die Login Credentials für die Anmeldung angeben (Abb. 13.7).

Bei der Speicherung des Passworts für die Anmeldung gibt es mehrere Möglichkeiten:

1. Wenn man das Passwort nur für den aktuellen Nutzer speichert, wird es verschlüsselt im GNOME Keyring oder KWallet (KDE Desktop) gespeichert.
2. Wenn man es für alle Nutzer speichert, liegt es unverschlüsselt auf der Festplatte.
3. Wenn man es nicht speichert, muss man es beim Start des VPN eingeben.

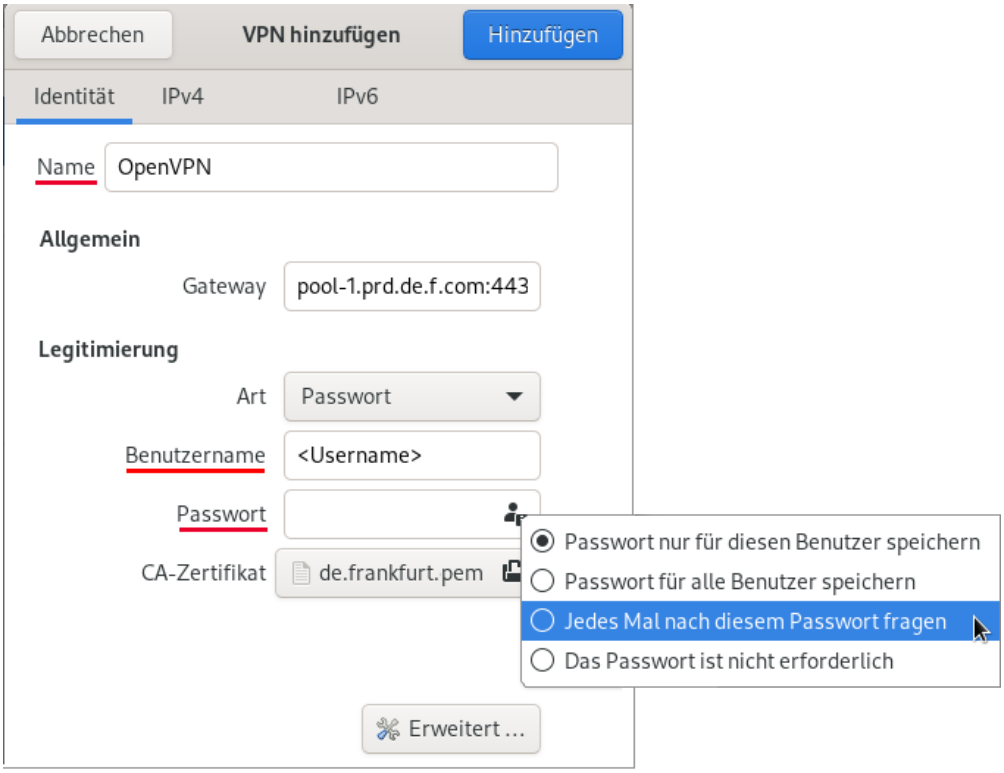


Abbildung 13.7: NetworkManager OpenVPN Import: Login Credentials eingeben

4. Bei einigen VPN Providern wie z. B. IVPN.net ist kein Passwort nötig, weil die zufällige Userkennung nicht zu erraten ist und nur für das VPN verwendet wird.

Man kann das VPN mit einem Klick im NetworkManager Applet aktivieren, sobald man mit einem Netzwerk verbunden ist. Um diesen Vorgang zu automatisieren, könnte man in den Einstellungen für ein WLAN festlegen, dass immer ein bestimmtes VPN automatisch gestartet werden soll, wenn man sich mit diesem Netzwerk verbindet (Abb. 13.8).

HINWEIS: in den Netzwerkeinstellungen im GNOME Kontrollzentrum ist diese Option nicht vorhanden. Wenn die Linux Distribution das GNOME Kontrollzentrum zur Konfiguration der Netzwerke bevorzugt, muss man den Konfigurationseditor des NetworkManagers im Terminal aufrufen:

```
> nm-connection-editor
```

13.5.2 Wireguard mit Linux

Wireguard ist ein Peer-2-Peer VPN, das durchgehend moderne Kryptografie für Verschlüsselung und Authentifizierung verwendet. Im Unterschied zu OpenVPN und IPsec werden Client-Server Architekturen nicht direkt unterstützt, können aber auch (irgendwie) realisiert werden.

- Jeder Wireguard Peer stellt einen IP-Adressbereich zur Verfügung, der transparent mit den Netzen der anderen Peers über eine Internetverbindung gekoppelt wird.

  Einige VPN-Provider vergewaltigen das Konzept und bauen damit individuelle Client-Server ähnliche Infrastrukturen, indem die Client Peers nur die eigene IP-Adresse (ein /32 Netz) verwenden und auf der Seite des VPN-Servers das gesamte Internet bereitgestellt wird.

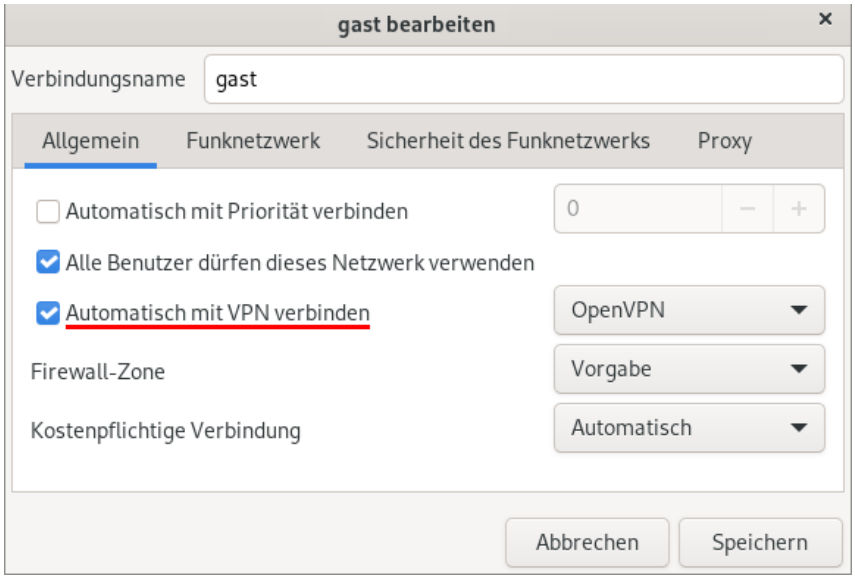


Abbildung 13.8: VPN mit einer Netzwerkverbindung automatisch starten

- Es gibt keine zentral verwalteten Authentifizierungsmechanismen für VPN Endpunkte wie bei OpenVPN oder IPsec, wo die VPN-Server sich mit X509v3 Zertifikaten authentifizieren können, die von einer zentralen CA ausgegeben werden.

  Bei Wireguard müssen die public Keys der verbundenen Peers irgendwie per Hand zwischen den Peers ausgetauscht werden.

- Es gibt keine Authentifizierung von Nutzern und keine zentrale Account Datenbank für Nutzer. Der Zugriff via VPN wird mit den public Keys der Peers verwaltet.

- Linux verwaltet Wireguard Verbindungen als Netzwerk Interfaces wie WLAN oder LAN Schnittstellen und nicht als VPN Verbindungen wie bei OpenVPN oder IPsec, die man einfach im NetworkManager als Overlays aktivieren kann.

- Wenn man PostUp- und PostDown-Scripte verwenden möchte, um Firewall oder DNS nach dem Start des VPN anzupassen, kann man die Wireguard Konfiguration nicht im NetworkManager GUI zusammenklicken oder importieren sondern muss Komandozeile zum Starten/Stoppen verwenden. Konfigurationsdateien ohne PostUp- und PostDown-Scripte kann man im NetworkManager importieren.

Installation der WireGuard Software

Als erstes ist die WireGuard Software zu installieren:

```
Ubuntu: > sudo apt install wireguard resolvconf
Fedora: > sudo dnf install wireguard-tools resolvconf
```

WireGuard Client für das private Heimnetz

Wenn man die Fritz!Box oder Speedport Router der Telekom als VPN Endpunkt nutzt, erhält man bei der Konfiguration der Nutzer im Router eine Wireguard Konfiguration für jeden Nutzer.

Man könnte darüber nachdenken, ob man diese VPN Verbindung nur für den Zugriff auf Ressourcen im heimischen Netzwerk nutzen möchte (Roadwarrior Szenario) oder den gesamten Datenverkehr über den heimischen Router ins Internet schicken, um die Reisetätigkeiten zu verbergen. Die vom Router generierte Konfigurationsdatei kann man dafür wie folgt anpassen.

- Standardmäßig wird der gesamte Datenverkehr über den heimischen Router geleitet:

```
AllowedIPs = 0.0.0.0/0,::/0
```

- Wenn man nur Zugriff auf heimische Ressourcen via VPN haben will, trägt man nur das private Netzwerk ein. (xxx ist durch konkrete Konfiguration im Heimnetz zu ersetzen.)

```
AllowedIPs = 192.168.xxx.0/24
```

Die vorbereitete Konfigurationsdatei kann man dann im Networkmanager importieren:

```
> sudo nmcli con import type wireguard file <DATEI>
```

Die importierte WireGuard VPN Verbindung sofort aktiviert. Das kann man in der Konfiguration im NetworkManager nachträglich deaktivieren und außerdem könnte man der VPN Verbindung einen sinnvollen Namen geben (Abb. 13.9).

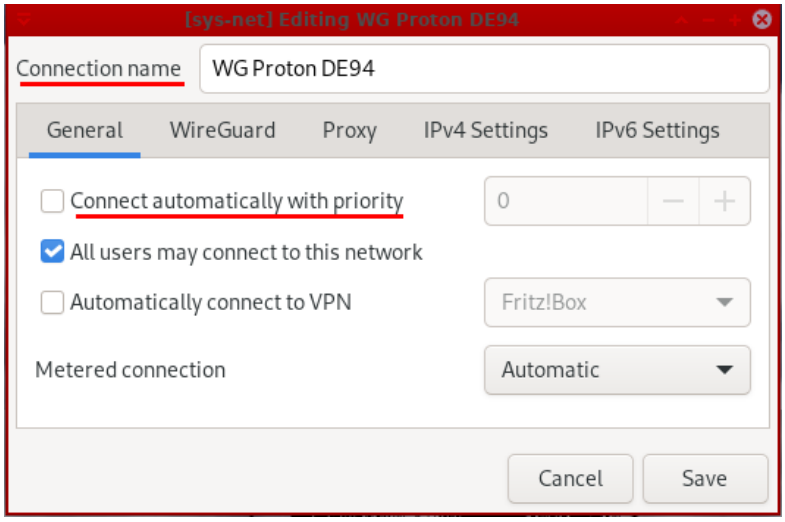


Abbildung 13.9: Editieren einer importierten Wireguard Verbindung

Zukünftig kann man die WireGuard VPN Verbindung mit einem Klick im NetworkManager Applet aktivieren oder sie auch automatisch bei Verbindung mit einem bestimmten Netzwerk aktivieren.

WireGuard Client Konfiguration für VPN-Provider

Viele VPN-Provider haben individuelle Lösungen entwickelt, um WireGuard für ihre Kunden in eine Client-Server ähnliche Infrastruktur zu pressen und Wireguard VPN-Server anbieten zu können.

Einige VPN-Provider (z.B. ProtonVPN) bieten fertige Konfigurationen für WireGuard inklusive der Schlüssel zum Download an. Bei anderen VPN-Providern muss man seinen selbst erstellten

öffentlichen Schlüssel auf der Webseite hochladen, sich den Schlüssel für den Wireguard Server sowie die zugeteilte IP-Adresse für den eigenen Peer und den DNS-Servers von der Webseite holen und die WireGuard Konfiguration selbst erstellen.

1. Man erstellt sich also eine kleine Konfigurationsdatei *wg0.conf* für die Verbindung zum VPN Server oder lädt sie vom Provider herunter. Wenn man zwischen mehreren VPN Servern wechseln möchte, muss man für jeden Wireguard Server eine eigene Konfigurationsdatei *wgX* erstellen.

   ```
   [Interface]
   PrivateKey = <privater Schlüssel>
   Address = <IP-Addr. für den eigenen Peer>/32
   DNS = <IP-Addr. vom DNS Server>

   [Peer]
   PublicKey = <öffentlicher Schlüssel des Servers>
   Endpoint = <IP-Addr. vom Server>:<Port>
   AllowedIPs = 0.0.0.0/0,::/0
   ```

   Mit dieser Beispielkonfiguration wird der gesamt Datenverkehr, der den Rechner verlässt, zum VPN Server geschickt. Mit der Aktivierung des VPNs hat man keinen Zugriff mehr auf Resourcen im lokalen Heimnetz (Netzwerkdrucker, Router, private Nextcloud o.ä.). Wenn man nur den Datenverkehr ins Internet via VPN Server routen möchte und gleichzeitig weiterhin Zugriff auf Ressourcen im heimischen Netz haben möchte, muss man folgenden Wert anpassen:

   ```
   AllowedIPs = ::/0, 1.0.0.0/8, 2.0.0.0/8, 3.0.0.0/8, 4.0.0.0/6,
   ↪ 8.0.0.0/7, 11.0.0.0/8, 12.0.0.0/6, 16.0.0.0/4, 32.0.0.0/3,
   ↪ 64.0.0.0/2, 128.0.0.0/3, 160.0.0.0/5, 168.0.0.0/6, 172.0.0.0/12,
   ↪ 172.32.0.0/11, 172.64.0.0/10, 172.128.0.0/9, 173.0.0.0/8,
   ↪ 174.0.0.0/7, 176.0.0.0/4, 192.0.0.0/9, 192.128.0.0/11,
   ↪ 192.160.0.0/13, 192.169.0.0/16, 192.170.0.0/15, 192.172.0.0/14,
   ↪ 192.176.0.0/12, 192.192.0.0/10, 193.0.0.0/8, 194.0.0.0/7,
   ↪ 196.0.0.0/6, 200.0.0.0/5, 208.0.0.0/4, 10.13.13.1/32
   ```

2. Diese Konfigurationsdatei(en) kann man im NetworkManager importieren:

   ```
   > sudo nmcli con import type wireguard file wg0.conf
   ```

3. Die importierte Wireguard VPN Verbindung wird sofort aktiviert! Das kann man in der Konfiguration im NetworkManager nachträglich deaktivieren und außerdem könnte man der VPN Verbindung einen sinnvollen Namen geben (Abb. 13.9).

4. Zukünftig kann man die WireGuard VPN Verbindung mit einem Klick im NetworkManager Applet aktivieren oder sie auch automatisch bei Verbindung mit einem bestimmten Netzwerk aktivieren.

WireGuard Server für ein kleines Firmennetz oder privates Heimnetz

Wenn man den heimischen Router nicht als Wirguard Server verwenden möchte oder der Router dieses Feature nicht bietet, könnte man einen kleinen Linux Server als VPN Gateway aufsetzen.

Die Konfiguration beginnt mit dem Erzeugen der kryptografischen Schlüssel. Idealerweise erzeugt jeder WireGuard Peer seine Schlüssel selbst. Dann müssen nur die öffentliche Schlüssel ausgetauscht werden, was auch über einen unsicheren Kanal (E-Mail o.ä.) erfolgen kann.

```
> sudo su
# cd /etc/wireguard
# umask 077
# wg genkey | tee privatekey | wg pubkey | tee publickey
bjqCt8IJ20zbfn3kLxvJ3mYGjTF+oe7Dg5vgyKqG4gU=
```

Der am Ende angezeigte öffentliche Schlüssel ist zu kopieren den anderen Peers zur Verfügung zu stellen. Man findet ihn auch in */etc/wireguard/publickey*. Den privaten Schlüssel aus der Datei *privatekey* braucht man im nächsten Schritt in der eigenen Konfigurationsdatei für die WireGuard Verbindung(en).

Wenn man einen WireGuard Server für den Zugang zum privaten Firmen- oder Heimnetz verwenden möchte, braucht man eine Konfigurationsdatei mit allen Peers, die als */etc/wireguard/wg0.conf* zu speichern ist.

(Die IP-Adressen für das Netzwerk und die Peers sind Beispiele - bitte selbst anpassen an das eigene Netzwerk.)

```
[Interface]
PrivateKey = <privater Schlüssel des Servers>
Address = 172.22.22.1/25
ListenPort = 51820
[Peer]
PublicKey = <öffentlicher Schlüssel des ersten Peer>
AllowedIPs = 172.22.22.211/32
[Peer]
PublicKey = <öffentlicher Schlüssel des zweiten Peer>
AllowedIPs = 172.22.22.212/32
[Peer]
PublicKey = <öffentlicher Schlüssel des dritten Peer>
AllowedIPs = 172.22.22.213/32
```

Bei der Firewallkonfiguration des Servers ist darauf zu achten dass Incoming UDP Traffic auf Port 51820 erlaubt ist, damit die Peers eine VPN-Verbindung aufbauen können.

```
Debian: > sudo uwf proto udp allow 51820
Fedora: > sudo firewall-cmd --add-port=51820/udp --permanent --zone=public
```

Wireguard VPN-Server startet und stoppt man mit folgenden Kommando:

```
> sudo wg-quick up wg0
> sudo wg-quick down wg0
```

Systemd kann den Wireguard Server auch beim beim Booten starten:

```
> sudo systemctl enable wg-quick@wg0.service
> sudo systemctl daemon-reload
```

Um den Start beim Booten wieder zu entfernen sind folgende Kommandos nötig:

```
> sudo systemctl stop wg-quick@wg0
> sudo systemctl disable wg-quick@wg0.service
> sudo rm -i /etc/systemd/system/wg-quick@wg0*
> sudo systemctl daemon-reload
> sudo syytemctl reset-failed
```

13.5.3 IPsec/IKEv2 mit Linux

IPsec ist ein komplexes Protokoll, dass viele Optionen bietet und bei hohen Sicherheitsanforderungen bei Militär und Regierungen bevorzugt wird. Unter Linux gibt es mehrere Implementierungen für die IPsec Standard. Im folgenden wird *strongSwan* verwendet.

IPsec/IKEv2 Server von VPN Providern nutzen (Debian/Ubuntu)

Das folgende Beispiel zeigt, wie man die IPsec Server von ProtonVPN mit strongSwan unter Ubuntu verwenden könnte. Als erstes ist die nötige Software zu installieren:

```
> sudo apt install strongswan libstrongswan-extra-plugins
↪  libcharon-extra-plugins
```

Die Konfiguration erfolgt als Full-Text-Adventure, da das NetworkManager GUI nicht alle nötigen Features unterstützt:

1. Für die Authentifizierung der VPN Server benötigt man das CA-Root Zertifikat von ProtonVPN, dass im Verzeichnis */etc/ipsec.d/cacerts/* zu speichern ist.

   Aus Sicherheitsgründen verwendet strongSwan nur die CA-Root Zertifikate, die in diesem Verzeichnis liegen, und nicht die Sammlung von CAs des Betriebssystems.

2. In der Datei /etc/ipsec.conf konfiguriert man einen oder mehrere VPN Server, die man auf der Webseite von ProtonVPN findet. Die IP-Adressen der Server (*right=...*) kann man anhand der Servernamen ermitteln oder man nimmt aus Faulheit den DNS Namen der Server. Die Namen für die Verbindungen können frei gewählt werden:

   ```
   conn proton-de13
     left=%defaultroute
     leftsourceip=%config
     leftauth=eap
     eap_identity=<USERNAME>

     right=37.120.217.163
     rightsubnet=0.0.0.0/0
     rightauth=pubkey
     rightid=%de-13.protonvpn.com
     rightca=/etc/ipsec.d/cacerts/ProtonVPN_ike_root.der

     keyexchange=ikev2
   ```

```
  type=tunnel
  auto=add

conn proton-it01
  left=%defaultroute
  leftsourceip=%config
  leftauth=eap
  eap_identity=<USERNAME>

  right=it-01.protonvpn.com
  rightsubnet=0.0.0.0/0
  rightauth=pubkey
  rightid=%it-01.protonvpn.com
  rightca=/etc/ipsec.d/cacerts/ProtonVPN_ike_root.der

  keyexchange=ikev2
  type=tunnel
  auto=add
```

<USERNAME> (*eap_identity=...*) ist durch den Usernamen für den Login auf OpenVPN/IPsec Servern zu ersetzen, den man ebenfalls auf der ProtonVPN Webseite findet.

3. Die Login Credentials für die VPN Server werden in */etc/ipsec.secrets* gespeichert:

   ```
   <USERNAME> : EAP <PASSWORT>
   ```

   Die Login Credentials für die VPN Server sind nicht identisch mit den Username/Passwort für den Login auf der Webseite. Man findet die richtigen Daten nach dem Login.

   Aus Sicherheitsgründen sollte die Datei */etc/ipsec.secrets* nur für root lesbar sein:

   ```
   > sudo chmod 0600 /etc/ipsec.secrets
   ```

Die Verwaltung der VPN Verbindungen erfolgt ebenfalls auf der Kommandozeile:

- Standardmäßig läuft der strongSwan Daemon unter Debian nach der Installation. Nach dem Anpassen der Konfigurationsdateien muss die Konfiguration neu eingelesen werden:

  ```
  > sudo ipsec reload
  ```

- In der Statusübersicht kann man sich anschauen, welche Verbindungen möglich sind:

  ```
  > sudo ipsec statusall
  ...
  Listening IP addresses:
  192.168.x.y
  Connections:
  proton-de13: %any...37.120.217.163 IKEv2
  proton-de13: local: uses EAP authentication with EAP identity
  ↪  '<USERNAME>'
  ```

```
proton-de13: remote: [de-13.protonvpn.com] uses public key
↪  authentication
proton-de13: child: dynamic === 0.0.0.0/0 TUNNEL
proton-it01: %any...it-01.protonvpn.com IKEv2
proton-it01: local: uses EAP authentication with EAP identity ''
proton-it01: remote: [it-01.protonvpn.com] uses public key
↪  authentication
proton-it01: child: dynamic === 0.0.0.0/0 TUNNEL
Security Associations (0 up, 0 connecting):
none
```

Es sind zwei IPsec/IKEv2 Verbinden konfiguriert: *proton-de13* und *proton-it01*.

- Mit folgendendem Kommando kann man eine Verbindung aufbauen:

  ```
  > sudo ipsec up proton-de13
  ```

  Es wird eine IPsec Verbindung zum VPN Server aufgebaut. Der VPN Server liefert die IP-Adresse des DNS Servers, die mit dem Kommando *resolvconf* systemweit gesetzt wird (bei Proton VPN ist der DNS Server 10.1.0.1) und das Routing wird angepasst. strongSwan hat keine Probleme mit IPv6, so dass keine Nachbearbeitungen per Script nötig sind.

- Mit folgendem Kommando kann man eine Verbindung zum VPN Server trennen:

  ```
  > sudo ipsec down proton-de13
  ```

13.5.4 Firewall Kill-Switch-Konfiguration für VPNs mit UFW

Wenn man eine VPN-Verbindung aktiviert, dann möchte man evtl. auch die Sicherheit haben, dass wirklich der gesamte Datenverkehr, der den Rechner verlässt, durch das VPN geschickt wird. Mit einer sogenannten Netzwerk-Kill-Switch-Konfiguration für die Uncompliceded Firewall (UFW) kann man das erzwingen und verhindert damit WebRTC Leaks und DNS Leaks oder dass Daten ins Internet geroutet werden, wenn die Verbindung zum VPN-Server gestört ist.

1. Falls UFW noch nicht auf dem Rechner vorhanden ist, installiert und aktiviert man die Firewall mit folgenden Kommandos:

   ```
   > sudo apt install ufw
   > sudo ufw enable
   ```

2. Für eine Kill-Switch-Konfiguration der Firewall benötig man die IP-Adresse(n) der VPN-Server, die man unter Linux mit *resolvectl* oder *dig* ermitteln kann.

3. Für eine neue UFW Konfiguration löscht man zuerst alle aktiven Regeln:

   ```
   > sudo ufw reset
   ```

4. Standardmäßig wird der gesamte aus- und eingehende Traffic blockiert:

   ```
   > sudo ufw default reject outgoing
   > sudo ufw default deny incoming
   ```

5. Durch das virtuelle VPN Interface *tun0* (OpenVPN) bzw. *wg0 ... N* (Wireguard) ist ausgehender Datenverkehr erlaubt. (Die folgenden Beispiele sind für OpenVPN. Wenn man Wireguard verwendet, ist *tun0* durch *wg0* zu ersetzen.)

   Alles erlauben, was raus will:

   ```
   > sudo ufw allow out on tun0 from any to any
   ```

   Man könnte es auch restriktiv konfigurierieren und nur bestimmte Daten erlauben:

   ```
   > sudo ufw allow out on tun0 http from any to any
   > sudo ufw allow out on tun0 https from any to any
   ...
   > sudo ufw allow out on tun0 dns from any to <DNS Server IP>
   ```

   Wenn der VPN-Server Port Forwarding anbietet und der eigene Rechner auf bestimmten Ports von außen erreichbar sein soll, könnte man Freigaben definieren:

   ```
   > sudo ufw allow in on tun0 from any port 22
   ```

6. Alle anderen Netzwerkschnittstellen dürfen mit den VPN-Servern kommunizieren:

   ```
   > sudo ufw allow out from any to <VPN Server1 IP>
   > sudo ufw allow out from any to <VPN Server2 IP>
   ...
   ```

Wenn man öfters zwischen dem Betrieb mit und ohne VPN wechselt, könnte man die Befehle zur Firewallkonfiguration in einem Script zusammenfassen, dass der NetworkManager beim Starten und Beenden des VPNs ausführt. Ein einfaches Beispielscript als Vorlage für Anpassungen:

```
#!/bin/sh
 case "$2" in

  vpn-up)
   # UFW Kill-Switch Konfiguration mit VPN
   ufw reset
   ufw default reject outgoing
   ufw default deny incoming
   ufw allow out on tun0 from any to any
   ufw allow out from any to <VPN Server1 IP>
   ;;

  vpn-down)
   # UFW Konfiguration ohne VPN
   ufw reset
   ufw default allow outgoing
   ufw default deny incoming
   ;;
esac
```

Das Script ist in das Verzeichnis */etc/NetworkManager/dispatcher.d/* zu kopieren, Eigentümer und Berechtigungen sind anzupassen. Der NetworkManager-dispatcher wird das Script nur ausführen, wenn es *root* gehört und die Berechtigungen korrekt sind:

```
> sudo cp beispielscript.sh /etc/NetworkManager/dispatcher.d/20-vpn-ufw
> sudo chown root:root /etc/NetworkManager/dispatcher.d/20-vpn-ufw
> sudo chmod 755 /etc/NetworkManager/dispatcher.d/20-vpn-ufw
```

Zukünftig wird der NetworkManager-dispatcher die Firewallregeln automatisch umschreiben, wenn eine VPN-Verbindung aktiviert oder beendet wird. Sollte das nicht funktionieren, muss man evtl. den Dispatcher Service des NetworkManagers bei einigen Distributionen noch aktivieren:

```
> sudo systemctl enable NetworkManager-dispatcher
```

Mit folgendem Kommando kann man prüfen, welche Firewall-Regeln aktiv sind:

```
> sudo ufw status verbose
```

13.6 Das VPN Exploitation Team der NSA

Aus den Dokumenten, die Edward Snowden bei der NSA rausgetragen hat, ist bekannt, dass bei der NSA das *OTP VPN Exploitation Team* für die Angriffe auf VPNs zuständig ist. Es werden einige Angriffsvektoren beschrieben, die ambitionierte Hacker gegen VPNs einsetzen (nicht nur die NSA setzt diese Techniken ein, auch andere Länder wie Frankreich, China oder Russland haben erhebliche Kapazitäten auf dem Gebiet und Kriminelle Hacker jeglicher Art sind auch interessiert).

Angriffe auf die Verschlüsselung: In den Snowden-Dokumenten wird erwähnt, dass der NSA 2010 einen Durchbruch bei Angriffen auf Verschlüsselung gelang und 60 % des weltweiten VPN-Traffics on-the-fly entschlüsselt werden konnte.

2015 wurde die Logjam Attack[14] durch zivile Kryptoforscher publiziert, die die Erfolge der NSA erklären konnte. Dabei handelt es sich um einen pre-computation Angriff auf den Diffie-Hellman Schlüsseltausch.

Dieses Beispiel zeigt, dass staatliche Angreifer mehrere Jahre Informationvorsprung bei der Kryptoanalyse haben. Man sollte deshalb keine Kryptografie einsetzen, die schon ein bisschen schwächelt.

Außerdem werden *Man-in-the-Middle* Angriffe und *TLS-Downgrade* Angriffe eingesetzt. Für beide Angriffe gibt es inzwischen Appliances.

- Bei Man-in-the-Middle-Angriffen lenkt der Angreifer den Datenverkehr des Clients auf seinen Server (z. B. mit DNS Manipulationen). Er gibt sich als der gewünschte VPN-Server aus, entschlüsselt den Datenverkehr und tut gegenüber dem VPN-Serven so, als ob er der Client wäre. Während der Kommunikation sitzt der Angreifer janusköpfig zwischen beiden und kann alles mitlesen.

[14] https://weakdh.org

- Bei TLS-Downgrade Angriffen stört der Angreifer den Aufbau der VPN-Verbindung immer wieder und bringt damit beide Seiten dazu, eine immer schwächere Verschlüsselung zu probieren. Wenn dann eine hinreichend schwache Verschlüsselung ausgewählt wurde, die der Angreifer knacken kann, lässt er den Aufbau der Verbindung zu.

  Appliances für TLS-Downgrade Angriffe sind military-grade Hardware hinsichtlich Geheimhaltung und Exportbeschränkungen. Ich kenne nur eine ältere Appliance, die RC4 Cipher on-the-fly brechen konnten. Auch bei der IETF hat man davon gehört und mit RFC 7465 die Verwendung von RC4 verboten.

  An dieser Stelle ein Dank an Jakob Appelbaum, der als erster darauf hinwies:

  RC4 is broken in real time by #NSA - stop using it. (November 2013)[15]

  (In der zivilen Kryptoanalyse ist kein Ansatz bekannt, um RC4 Cipher on-the-fly zu brechen. RC4 gilt als schwacher Cipher und konnte mit der NOMORE Attack[16] in 75h geknackt werden, um HTTPS Cookies zu entschlüsseln, und in 1h bei WPA Passwörtern. RC4 on-the-fly brechen ist bisher NSA-only Level.)

Angriffe auf die kryptografischen Schlüssel sind die logische Alternative, wenn man die Verschlüsselung nicht brechen kann.

Pre-shared Keys (PSK) können alle VPNs zur Authentifizierung nutzen. Das Programm *HappyDance* der NSA hat die Aufgabe, diese Schlüssel zu knacken um den Datenverkehr als passive Lauscher zu entschlüsseln.

Dabei kommen drei Methoden zum Einsatz:

1. Die E-Mail Überwachung wird genutzt, um in den abgefangenen Mails nach Schlüsseln zu suchen, die als pre-shared Keys für die Authentifizierung bei VPNs geeigent sein könnten. Diese Schlüssel werden gesammelt und automatisiert genutzt. (Es gibt immer Admins, die diese Schlüssel per E-Mail verteilen.)
2. Außerdem werden pre-shared Keys von interessanten VPNs mit Brute-Force-Attack angegriffen. Da diese Keys oft mit zu geringer Entropie von der VPN Software erzeugt werden (Shannon E. < 3.5), sind diese Angriffe erfolgreich.
3. In besonders hartnäckigen Fällen wird das Gruppe *Taylored Access Operations* (TAO) der NSA beauftragt, den VPN-Server oder einen beliebigen VPN-Client aus dem VPN-Netzwerk zu knacken und den pre-shared Key zu kopieren.

Pre-shared Keys sollte man nur für Testzwecke nutzen. Das StrongSwan Team warnt aufgrund der Snowden Dokumente vor dem Einsatz. Statt dessen sollte man X509v3 Zertifikate verwenden, auch wenn die Konfiguration damit komplizierter wird.

Kompromittierung der VPN-Server oder -Clients Das *OTP VPN Exploitation Team* der NSA setzt auch diese Methode gegen High-Value-Targets wie z. B. Banken ein, wenn Admins ihre VPNs professionell konfigurieren.

1. Die Gruppe Taylored Access Operations (TAO) der NSA wird damit beauftragt, den VPN-Server oder einen VPN-Client zu knacken.
2. Anschließend installiert das NSP-Team ein Implantat (Rootkit), dass die VPN-Verschlüsselung des Datenverkehrs so stark schwächt, dass sie on-the-fly gebrochen werden kann, ohne das der Admin es jahrelang bemerkt.

[15] https://twitter.com/ioerror/status/398059565947699200
[16] https://www.rc4nomore.com

Gelegentlich greift das TAO-Team die Server nicht direkt an sondern spielt über die Bande und kompromittiert zuerst die Computer Administratoren, um an Passwörter oder Keys zu gelangen (*Inside the NSA's Secret Efforts to Hunt and Hack System Administrators*[17]).

[17] https://theintercept.com/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/

Kapitel 14

Domain Name Service (DNS)

DNS (Domain Name Service) ist das Telefonbuch des Internet. Eine kurze Erklärung:

1. Der Surfer gibt den Namen einer Website in der Adressleiste des Browsers ein (z. B. https://www.privacy-handbuch.de).
2. Daraufhin fragt der Browser bei einem DNS-Server nach der IP-Adresse des Webservers, der die gewünschte Webseite liefern könnte. Üblicherweise wird der DNS-Server des Zugangsproviders gefragt, also z. B. Telekom, Vodafone usw.
3. Der angefragte DNS-Server erkundigt sich bei den Servern der Root-Zone nach dem DNS-Server, der für die Toplevel-Domain *.de* zuständig ist. Diesen Server fragt er nach dem DNS-Server, der für die Domain *privacy-handbuch.de* zuständig ist, dann jenen DNS-Server nach der IP-Adresse des Webservers für *www.privacy-handbuch.de*.
4. Wenn ein passender Webserver gefunden wurde, dann wird die IP-Adresse zurück an den Browser gesendet (z. B. 81.169.145.78 oder NXDOMAIN, wenn der Surfer sich vertippt hat). Der Prozess dauert nur wenige Millisekunden.
5. Dann sendet der Browser seine Anfrage an die IP-Adresse des entsprechenden Servers und erhält als Antwort die gewünschte Webseite.

DNS-Server werden nicht nur beim Surfen verwendet. Alle Dienste verwenden das DNS-System, um die IP-Adressen der Server zu ermitteln (E-Mail, Chat usw.). Ein DNS-Server kennt also alle Internet-Dienste und Webserver, die man kontaktiert. Außerdem kann der DNS-Server durch Manipulation der Antworten entscheiden, welche Webseiten der Surfer sehen und welche Dienste man nutzen kann.

Möglichkeit zur Zensur

Die Möglichkeit der DNS-Manipulation zur Zensur des Internetzugangs sollte 2009 mit dem Zugangserschwerungsgesetz (ZugErschwG) genutzt werden. Alle deutschen Provider sollten eine geheime, vom BKA gelieferte Sperrliste von Domainnamen sperren und die Surfer beim Aufruf dieser Webseiten durch manipulierte DNS-Antworten auf eine Stopp-Seite umlenken. Durch zumutbare Maßnahmen gemäß dem Stand der Technik sollten Provider die Nutzung alternativer, unzensierter DNS-Server verhindern.

Neben dem damaligen Innenminister Schäuble haben sich besonders Hr. v. Guttenberg und Ursula v. d. Leyen für das Gesetz engagiert. Frau v. d. Leyen wurde dafür mit dem Big Brother

geehrt (was ihre weitere Karriere aber nicht negativ beeinflusst hat). Aufgrund des Widerstandes der Zivilgesellschaft wurde das ZugErschwG wieder aufgehoben.

Aktuell wird die Sperrung von Webseiten im DNS in der EU, im Iran, Türkei, Ukraine. Süd Korea oder Vietnam nach diesem Muster umgesetzt. In Großbritannien gibt es konkrete Pläne für eine Zensurinfrastruktur auf Basis von DNS-Manipulationen. Für die Türkei wurde auch nachgewiesen, dass die Nutzung alternativer DNS Server blockiert wird und DNS Anfragen auf immer an kompromittierte Server umgeleitet werden. Nur verschlüsseltes DNS ermöglicht eine Umgehung dieser Zensur.

14.1 DNSSEC-Validierung

DNSSEC verbreitet sich langsam, aber immer weiter, als Sicherheitskomponente. Ein DNSSEC-validierender DNS-Server kann die Echtheit der DNS-Informationen anhand kryptografischer Signaturen verifizieren, Manipulationen erkennen und verwerfen, wenn der Betreiber der Domain die DNS-Daten signiert hat. Damit wird verhindert, dass Dritte die Daten manipulieren und den Surfer irgendwie umleiten (Zensur? Phishing?). Wie das konkret funktioniert, ist eine Menge Krypto-Voodoo.

DNSSEC ist außerdem eine Voraussetzung, um via DANE/TLSA die X509v3-Zertifikate für die TLS-Verschlüsselung zu verifizieren oder um mit OPENPGPKEY bzw. SMIMEA kryptografische Schlüssel sicher zu verteilen.

Im ersten Schritt ist es also ein Sicherheitsgewinn, wenn man einen DNSSEC-validierenden DNS-Server verwendet. Die Verwendung DNSSEC-validierender Server sichert aber nur die Auflösung der DNS-Anfragen auf dem DNS-Server. Die *letzte Meile* zwischen DNS-Server und Nutzer bleibt ungeschützt.

Um diese Schwäche zu vermeiden, könnte man die DNSSEC-Signaturen auch auf dem eigenen Rechner mit einem lokalen Resolver validieren.

- Windows bietet out-of-the-box noch keine Möglichkeit, DNSSEC zu nutzen.
- Die meisten Linux-Distributionen verwenden inzwischen systemd-resolve für die DNS-Namensauflösung. Um DNSSEC zu aktivieren, ist eine Config-Datei *dnssec.conf* im Verzeichnis */etc/systemd/resolved.conf.d/* mit folgendem Inhalt anzulegen:

```
[Resolve]
DNSSEC=true
```

14.2 Verschlüsselung des DNS-Datenverkehrs

Das DNS-Protokoll enthält keine Authentifizierung, die sicherstellt, dass man wirklich mit dem gewünschten DNS-Server verbunden ist. DNS-Anfragen könnten vom Provider auf eigene, möglicherweise kompromittierte DNS-Server umgeleitet werden. In der Türkei wird dieses Feature seit mehreren Jahren zur Durchsetzung der Zensur eingesetzt.

Um diese Schwächen zu vermeiden, kann man den DNS-Datenverkehr zum Upstream-DNS-Server verschlüsseln. Das stellt kryptografisch sicher, dass man wirklich mit dem gewünschten DNS-Server verbunden ist (Authentifizierung), und verhindert eine Manipulation durch Dritte auf der *letzten Meile*.

Die Verschlüsselung der DNS-Daten in Kombination mit ESNI (Encrypted Server Name Indication) in TLS 1.3 hat das Potential, die staatliche Infrastruktur zur Zensur des Internet in den meisten Länder auszutricksen. Aus diesem Grund versuchen einige Länder, diese technischen Entwicklungen zu blockieren:

- Die *Great Firewall* von China blockiert TLS 1.3, um anhand der unverschlüsselt übertragenen Servernamen im TLS-Handshake unerwünschte Webseiten zu blockieren.
- In Großbritannien wurde auf Druck der Internet-Service-Betreiber ein Deal mit Mozilla geschlossen, dass DNS-over-HTTPS nicht wie geplant standardmäßig aktiviert wird. Man rechnet damit, dass die meisten Nutzer nie etwas davon gehört haben.
- In Russland wurde im September 2020 vom Ministerium für Digitale Entwicklung ein Gesetzentwurf zur Diskussion vorgelegt, der den Einsatz von verschlüsseltem DNS und ESNI im RuNet verbieten soll. Begründet wurde der Entwurf mit der Wirkungslosigkeit von staatlichen Zensurmaßnahmen, wenn sich die Techniken verbreiten. Zur Durchsetzung des Gesetzes sollen IP-Adressen von DNS-Servern mit DNS-over-TLS oder DNS-over-HTTPS blockiert werden.

Um den Datenverkehr kryptografisch zu sichern, gibt es folgende Möglichkeiten:

DNSCrypt ist die älteste Technik für verschlüsseltes DNS und basiert auf DNScurve von D. J. Bernstein. Sie stellt mit kryptografischen Verfahren sicher, dass man wirklich den gewünschten DNS-Server verwendet, und verschlüsselt die DNS-Daten.

Um DNScrypt zu verwenden, muss man den *dnscrypt-proxy* installieren, den es für verschiedene Betriebssysteme und Smartphones gibt. Nach der Installation sollte man die Konfiguration anpassen und die vertrauenswürdigen Server auswählen. Standardmäßig verwendet dnscrypt-proxy auch Google und Cloudflare.

DNS-over-TLS wurde von der IETF im Mai 2016 im RFC 7858 spezifiziert. Die meisten aktuellen Versionen der Linux-DNS-Server beherrschen inzwischen DNS-over-TLS.

Android 9 kann ebenfalls DNS-over-TLS nutzen. Die Option heißt *Privates DNS* und verbirgt sich in den erweiterten Einstellungen für *Netzwerk & Internet*. Hier kann man den Namen des gewünschten DNS-over-TLS-Servers eintragen.

iPhones unterstützen verschlüsseltes DNS-over-TLS seit iOS Version 14.

DNS-over-HTTPS wurde im Sommer 2016 von Google initiiert. Es dient in erster Linie der Umgehung von Zensur durch DNS Manipulation und kommt auch durch *Fascist Firewalls*.

Verglichen mit DNS-over-TLS ist DoH aufgrund des HTTP-Overheads weniger performant. Außerdem ergeben sich durch die Nutzung des HTTP-Protokolls Implikationen für die Privatsphäre. Ein Server könnte HTTP-Auth-Header, E-Tags sowie SSL-Session-ID für das Tracking instrumentalisieren oder HTTP-Header wie User-Agent, Accept-Language usw. für das Fingerprinting des Browsers nutzen. Simples Tracking via Cookies wäre aber zu einfach. Die Cookies soll ein DoH Client ignorieren, wie die IETF in RFC 8484 schreibt.

Es gibt einige Programme, die DNS-over-HTTPS beherrschen und damit die in den Systemeinstellungen konfigurierten DNS-Server umgehen können:

dnscrypt-proxy kann als lokaler DNS-Resolver mit eingebautem Cache genutzt werden und auch DNS-over-HTTPS-Server verwenden.

Firefox kann die DNS-Einstellungen des Systems umgehen und DNS-over-HTTPS-Server als Trusted Recursive Resolver (TRR) verwenden.

Thunderbird kann ebenfalls DNS-over-HTTPS-Server als Trusted Recursive Resolver (TRR) verwenden. Es sind die gleichen Parameter wie bei Firefox in den erweiterten Einstellungen anzupassen.

DNS-over-HTTPS-over-Tor kann man machen, wenn ein sinnvolles Gesamtsicherheitskonzept es erfordert. Man kann beliebigen HTTPS-Traffic durch Tor tunneln, um zu verhindern, dass DNS-Server die eigene IP-Adresse protokollieren können.

Man erreicht das gleiche Ziel aber auch ohne Perfomance-Einbußen, indem man einen vertrauenswürdigen DNS-Server mit No-Logging-Policy verwendet.

Abgesehen von einigen Szenarien mit höchsten Sicherheitsanforderungen, für die es schwerfällt, ein plausibles Beispiel zu konstruieren, ist DoHoT meist Overkill.

Oblivious DNS-over-HTTPS wurde von Cloudflare im Dezember 2020 initiiert, weil es in Europa Vorbehalte gegen die Nutzung von Cloudflare als Defaut-Trust-Recursive-Resolver (DoH) in Firefox gab. Derzeit läuft der Standardisierungsprozess.

Für Cloudflare ist nicht interessant, welche Webseiten Lieschen Müller oder Pitschie Hufnagel aufrufen. Das Unternehmen interessiert sich vielmehr für eine globale Sicht: Welche neuen Ideen gewinnen an Popularität, was ist der neue *heiße Shit* und was ist anderseits auf dem absteigenden Ast. Diese Informationen frühzeitig zu haben ist wertvoll, wie es Google mit seiner Suchmaschine demonstriert. Für Cloudfare besteht die Chance, als Default-DNS-over-HTTPS-Server für alle Firefox-Nutzer millionenfach diese Daten zu sammeln, wenn sie die Bedenken der Privacy-Community ausräumen können.

Aus technischer Sicht verwendet Oblivious-DNS-over-HTTPS einfach Onion-Routing mit nur einem Hop. Wenn die Betreiber der Hops nicht mit Cloudflare kooperieren, bleibt die Privatsphäre der Nutzer ähnlich gut geschützt wie bei DoHoT, mit wesentlich geringeren Einbußen bei der Performance.

Kann sein, dass ich mich täusche und ODoH ein neuer *heißer Trend* wird. Aber man muss nicht unbedingt Cloudflare-DNS-Server nutzen. ;-)

Hinweis für Wi-Fi-Hotspots

Die Anmeldung für viele Wi-Fi-Hotspots (zum Beispiel in Hotels, U-Bahnen usw.) arbeitet in der Regel mit einer Manipulation des DNS für den Aufruf der Captive-Portal-Seite. Validierung mittels DNSSEC und Verschlüsselung mit DNScrypt, DNS-over-HTTPS oder DNS-over-TLS funktionieren daher an Wi-Fi-Hotspots mit Login nicht.

Wer mit seinem Laptop einen Wi-Fi-Hotspot nutzen möchte, muss den DNS-Server des Hotspot-Betreibers verwenden und die lokale DNSSEC-Validierung abschalten.

Bei Android-Smartphones und iPhones besteht dieses Problem nicht. Bei einem Wechsel des Netzwerkes wird erst der Captive-Portal-Check mit dem zugewiesenen DNS-Server ausgeführt und danach auf DNS-over-TLS umgeschaltet (wenn es aktiviert ist).

14.3 Vertrauenswürdige DNS-Server

Die meisten DNS-Server der Zugangsprovider verwenden kein DNSSEC für die Validierung. Das könnte ein Grund (Sicherheit) für einen selbst gewählten DNS-Server sein.

Einige deutsche Kabelnetzprovider betreiben keine eigenen DNS-Server mehr, sondern schicken ihre Kunden einfach zu Google-DNS (8.8.8.8) oder Cloudflare (1.1.1.1). Wenn man mit der Datensch(m)utz-Policy der Default-DNS-Server der Provider nicht einverstanden ist, muss man sich selbst kümmern und die DNS-Server auf dem Router anpassen.

Das Sammeln, Auswerten und Verkaufen von DNS-Daten der Kunden durch den Zugangsprovider ist in angelsächsischen Ländern üblich, aber nicht in Deutschland.

Zensur durch manipulierte DNS-Server spielte nach der Abwehr des ZugErschwG zeitweise keine Rolle in Deutschland, wurde aber 2022 von der EU unter Führung von Ursula v. d. Leyen zur moralischen Reinhaltung und Abwehr russischer Propaganda wieder eingeführt (beispielsweise bei Telekom und T-Mobile). Wer sich bei FEINDSENDERN informieren will, braucht einen unzensierten DNS-Server.

Die Nachdenkseiten berichteten im Dez. 2022, dass sie bei einigen Zugangsprovider zeitweise gesperrt wurden, unter Hinweis auf das Zensurverodnung der EU. Wenn man nicht eines Tages feststellen möchte, dass interessante Seiten im Netz nicht mehr erreichbar sind, sollte man rechtzeitig über unzensierte DNS Alternativen nachdenken. Die Bemühungen zur Einführung von mehr Zensur werden auch in der EU stärker - das ist seit 2022 kein Alleinstellungsmerkmal von Diktaturen.

Hinweis: Ein Trackingdienst könnte ermitteln, welcher DNS-Server vom Browser verwendet wird, und diese Information als Parameter für das Fingerprinting des Browsers verwenden (kurze Erläuterung). Es gibt bisher keine empirischen Studien, ob dieses Verfahren *in the wild* genutzt wird. Aber prinzipiell wäre es möglich. Deshalb sollte man kurz nachdenken, ob es Gründe gibt, einen selbst ausgewählten DNS-Server zu nutzen, also ob der Vorteil an Sicherheit, Privatsphäre gegenüber dem Zugangsprovider und Schutz gegen Zensur evtl. unerwünschte Nebeneffekte kompensiert.

Folgende DNS-Server mit No-Logging-Policy, DNSSEC-Validierung und Anti-Spoofing-Schutz[1] kann man als Alternative zu den Default-DNS-Servern der Provider empfehlen:

- Freifunk München[2] (normales DNS, DNS-over-TLS und DNS-over-HTTPS!)
  - IPv4: 5.1.66.255 / IPv6: 2001:678:e68:f000:: / dot.ffmuc.net
  - IPv4: 185.150.99.255 / IPv6: 2001:678:ed0:f000:: / dot.ffmuc.net
- Digitale Gesellschaft (CH)[3] (Nur DNS-over-TLS und DNS-over-HTTPS!)
  - IPv4: 185.95.218.42 / IPv6: 2a05:fc84::42 / dns.digitale-gesellschaft.ch
  - IPv4: 185.95.218.43 / IPv6: 2a05:fc84::43 / dns.digitale-gesellschaft.ch
- Censurfridns Denmark[4] (aka. UncensoredDNS)
  - IPv4: 91.239.100.100 / IPv6: 2001:67c:28a4::
  - IPv4: 89.233.43.71 / IPv6: 2a01:3a0:53:53:: (mit DNS-over-TLS)

Die folgenden DNS-Server filtern Werbung, Tracking und Malware-Domains. Alle drei Projekte werden von unabhängigen Einzelpersonen betrieben:

[1] https://www.grc.com/dns/dns.htm
[2] https://ffmuc.net/wiki/doku.php?id=knb:dohdot
[3] https://www.digitale-gesellschaft.ch/dns/
[4] http://blog.uncensoreddns.org

- dismail.de[5](mit DNS-over-TLS)
  - IPv4: 116.203.32.217 / IPv6: 2a01:4f8:1c1b:44aa::1 / fdns1.dismail.de
  - IPv4: 159.69.114.157 / IPv6: 2a01:4f8:c17:739a::2 / fdns2.dismail.de
- dnsforge.de[6] (mit DNS-over-TLS, DNS-over-HTTPS)
  - IPv4: 176.9.93.198 / IPv6: 2a01:4f8:151:34aa::198 / dnsforge.de
  - IPv4: 176.9.1.117 / IPv6: 2a01:4f8:141:316d::117 / dnsforge.de
- BlahDNS.com[7] (mit DNS-over-TLS, DNS-over-HTTPS, DNScrypt)
  - Server DE: 78.46.244.143 / 2a01:4f8:c17:ec67::1 / dot-de.blahdns.com
  - Server FI: 45.91.92.121 / 2a0e:dc0:6:23::2 / dot-ch.blahdns.com

Beim Filtern von Trackingdomains ist die Grenze zur Zensur schmal und hängt davon ab, welche Filterlisten eingebunden werden. Die Fake-News-Blackliste von StevenBlack enthält beispielsweise 56.000+ Einträge, die von irgendwem irgendwie als Fake News deklariert wurden. Unabhängig von den Diskussionen um Fake News, die wesentlich vom politischen Weltbild des Betrachters abhängen, ist die Sperrung von Informationsangeboten Zensur. Und ein unzensierter Zugang zu Informationen ist ein wichtiger Grund für die Konfiguration eigener DNS-Server. Bei DNS-Servern mit Filterung muss man prüfen, welche Blocklisten verwendet werden.

14.4 Unzensierte DNS-Server von vertrauenswürdigen VPN-Providern

Der DNS- und VPN-Provider AdGuard stellt seine DNS-Server zur kostenfreien Nutzung bereit und finanziert sich mit Premium-Features. Die Server stehen in Westeuropa.[8]

- AdGuard-DNS-Server MIT Werbe- und Trackingfilter:
  - IPv4: 94.140.14.14 / IPv6: 2a10:50c0::ad1:ff / dns.adguard-dns.com
  - IPv4: 94.140.15.15 / IPv6: 2a10:50c0::ad2:ff / dns.adguard-dns.com
- AdGuard DNS-Server OHNE Werbe- und Trackingfilter:
  - IPv4: 94.140.14.140 / IPv6: 2a10:50c0::1:ff / unfiltered.adguard-dns.com
  - IPv4: 94.140.14.141 / IPv6: 2a10:50c0::2:ff / unfiltered.adguard-dns.com

Njalla ist ein privacy-fokusierter schwedischer Domain-, Hosting- und VPN-Provider, der seinen unzensierten DNS-Server kostenlos zur Verfügung stellt.[9]

- Njalla DoT- und DoH-Server (ohne Werbe- und Trackingfilter):
  - IPv4: 95.215.19.53 / IPv6: 2001:67c:2354:2::53 / dns.njal.la

[5] https://dismail.de/info.html
[6] https://dnsforge.de/
[7] https://blahdns.com
[8] https://adguard-dns.io/de/welcome.html
[9] https://dns.njal.la/

Der schwedische VPN-Provider Mullvad stellt DNS-over-TLS und DNS-over-HTTPS Server ebenfalls kostenlos zur Verfügung (kein Plain-DNS). Die Server stehen in Deutschland, Schweden, Großbritannien, Singapur sowie in den USA und sind unter einheitlichen IP-Adressen erreichbar.[10]

- Mullvad DoT- und DoH-Server mit Werbe- und Trackingfilter:
  - IPv4: 194.242.2.3 / IPv6: 2a07:e340::3 / adblock.dns.mullvad.net
- Mullvad DoT- und DoH-Server mit Werbe-, Tracking- und Malwarefilter:
  - IPv4: 194.242.2.4 / IPv6: 2a07:e340::4 / base.dns.mullvad.net
- Mullvad DoT- und DoH-Server mit Werbe-, Tracking-, Malware- und Social Media Filter:
  - IPv4: 194.242.2.5 / IPv6: 2a07:e340::5 / extended.dns.mullvad.net
- Mullvad DoT- und DoH-Server mit Werbe-, Tracking-, Malware-, Social Media, Porno- und Gambnlingfilter:
  - IPv4: 194.242.2.9 / IPv6: 2a07:e340::9 / all.dns.mullvad.net
- Mullvad DoT und DoH-Server OHNE Filter:
  - IPv4: 194.242.2.2, 193.19.108.2 / IPv6: 2a07:e340::2 / dns.mullvad.net

14.5 DNS-Server der Big-Player der IT-Branche

Daneben gibt es einige kommerzielle DNS-Dienste von den Big-Playern der IT-Branche, die damit werben, die länderspezifische Zensur von Zugangsprovidern, wie sie beispielsweise in der Türkei üblich ist, zu umgehen. Ein paar kleine Kommentare zu diesen Angeboten:

- Der Klassiker ist Google DNS. Google verspricht, dass die DNS-Server unter den IP-Adressen 8.8.8.8 und 8.8.4.4 nicht kompromittiert oder zensiert werden, und bemüht sich erfolgreich um schnelle DNS-Antworten.

  Natürlich werden alle Anfragen gespeichert und ausgewertet. Es gilt die Datensch(m)utz-Policy[11] von Google. Ziel ist es, die besuchten Webdienste zu erfassen und in das Monitoring des Web einzubeziehen. Positiv an dieser Initiative ist, dass es sich kaum jemand leisten kann, die Wirtschaftsmacht Google zu blockieren. Damit wird auch die Sperrung alternativer DNS-Server deutlich erschwert, wie sie in Deutschland im Rahmen des ZugErschwG geplant war.

- Quad9 mit Hauptsitz in der Schweiz ist technisch mit Google-DNS vergleichbar. Unter einheitlichen IP-Adressen stehen 100-200 DNS-Server zur Verfügung:

```
Primary DNS:    9.9.9.9 / 2620:fe::fe / dns.quad9.net
Secondary DNS:  149.112.112.112 / 2620:fe::9 / dns.quad9.net
```

[10] https://mullvad.net/de/help/dns-over-https-and-dns-over-tls
[11] https://policies.google.com/privacy?hl=de&gl=de

Das Projekt verfolgt aber andere Ziele. Quad9 ist für die Anforderungen von Unternehmen optimiert. Im Vordergrund steht IT-Sicherheit. Durch die Verwendung von zeitnah aktualisierten Blocklisten sollen die Auswirkungen von Malware- und Phishing-Kampagnen minimiert werden. Ein (temporäres) Overblocking ist nicht gewünscht, wird aber zugunsten der Sicherheit von Quad9 nicht ausgeschlossen.

Dafür arbeitet Quad9 mit 18+ Cyber-Threat-Intelligence-Providern zusammen. Deren Erkenntnisse über Cyber-Angriffe werden gesammelt, um die Abwehr von kriminellen Angriffen und Wirtschaftsspionage auf DNS-Ebene zu konsolidieren. Bei einem Angriff erhalten die Threat-Intelligence-Provider dafür Zugriff auf den (anonymisierten) DNS-Traffic, um die Analyse zu beschleunigen.

Die Anforderungen privater Anwender an Privatsphäre und Zensurfreiheit spielen nur eine untergeordnete Rolle. Trotzdem sind auch private Anwender eingeladen, den Dienst zu nutzen. DNSSEC ist bei Quad9 Standard, außerdem sind DNS-over-TLS sowie DNS-over-HTTPS und (testweise) DNScrypt nutzbar.

- Am 01. April 2018 hat Cloudflare einen ähnlichen DNS-Dienst gestartet. Unter den IP-Adressen 1.1.1.1 und 1.0.0.1 stehen weltweit sehr schnelle DNS-Server bereit, die hinsichtlich Geschwindigkeit Google DNS und Quad9 übertreffen.[12]

  Privacy ist ein wichtiges Verkaufsargument und deshalb schwört auch Cloudflare, die Privatsphäre der Nutzer zu respektieren. Das Privacy-Statement klingt sehr überspezifisch: Man wird keine Daten verkaufen, die IP-Adressen der Nutzer nicht auf die Festplatte schreiben und Logdaten max. 24h behalten. Cloudflare wird aber auswerten, welche Domains gesucht wurden, und darauf aufbauend Analysen durchführen, die viel Geld wert sind, wenn große Mengen an Daten einfließen, die für die weltweite Internetnutzung repräsentativ sind.

  Cloudflare behauptet nicht, dass der DNS-Service zensurfrei sei. Im Blog-Artikel wird darauf hingewiesen, dass man mit den DNS-Servern via DoT oder DoH länderspezifische Sperren wie jene in der Türkei umgehen kann, aber man kann davon ausgehen, dass Cloudflare die Anforderungen der US-Administration umsetzten wird.

  DNSSEC ist aktiv, außerdem ist DNS-over-TLS und DNS-over-HTTPS nutzbar.

14.6 Konfiguration der DNS-Server

Für die Konfiguration der DNS-Server gibt es mehrere Möglichkeiten mit unterschiedlichen Vor- und Nachteilen.

DNS-Server auf dem Router konfigurieren

Die bevorzugten DNS-Server könnte man im eigenen LAN im Router konfigurieren, indem man auf der Konfigurationsseite für die Verbindung zum Internet-Provider die bevorzugten DNS-Server eingibt.

Vorteil: Via DHCP werden diese DNS-Server automatisch an alle Rechner im LAN und WLAN verteilt, sobald sie sich neu mit dem Router verbinden. Es sind keine weiteren Konfigurationen an Rechnern oder Smartphones nötig.

Nachteil: Die meisten Router unterstützen kein DNS-over-TLS, DNS-over-HTTPS oder DNScrypt, um sicherzustellen, dass man wirklich mit dem gewünschten DNS-Server verbunden ist. Lediglich

[12] https://1.1.1.1/de/

die Fritz!Boxen mit Fritz!OS 7.24 könnten DNS-over-TLS mit Einschränkungen verwenden, wobei man für störungsfreies Arbeiten den Fallback auf unverschlüsseltes DNS in Kauf nehmen muss, so dass unter Last ein Teil der DNS-Anfragen unverschlüsselt rausgeht.

DNS-Server in den Netzwerkeinstellungen konfigurieren

Alternativ kann man die DNS-Server auf jedem Computer einzeln in den Einstellungen für die Netzwerkverbindung im Betriebssystem des PCs oder Laptops konfigurieren.

Unter Linux kann man z. B. mit dem NetworkManager-Applet für jede Verbindung einzeln konfigurieren, welche DNS-Server verwendet werden sollen. Wenn man öfters mit dem Laptop unterwegs ist, kann man also im eigenen LAN zuhause andere Einstellungen nutzen als in bekannten WLANs oder bei Wi-Fi-Hotspots, wo man den DNS-Server des Hotspot-Betreibers nutzen muss, um die Captive-Portal-Seite aufrufen zu können.

In dem Applet in der Taskleiste des Desktops wählt man den Menüpunkt *Verbindungen bearbeiten*. In dem sich öffnenden Fenster kann man für jede Internet-Verbindung (LAN, WLAN usw.) die DNS-Server konfigurieren. Der NetworkManager kümmert sich dann darum, dass die gewünschten Einstellungen beim Herstellen der Internetverbindung aktiviert werden. (Ist ein wenig umständlich bei neuen WLANs, funktioniert aber.)

Die Einstellungen sind auf den Reitern IPv4 UND IPv6 anzupassen! Für IPv6 muss man keine DNS-Server konfigurieren, kann man aber machen. Es reicht, die Methode der Konfiguration auf *Automatisch (DHCP), nur Adressen* zu setzen. Für IPv4 muss man die Methode der Konfiguration auf *Automatisch (DHCP), nur Adressen* setzen und 2–3 DNS-Server eintragen. (Bild 14.1)

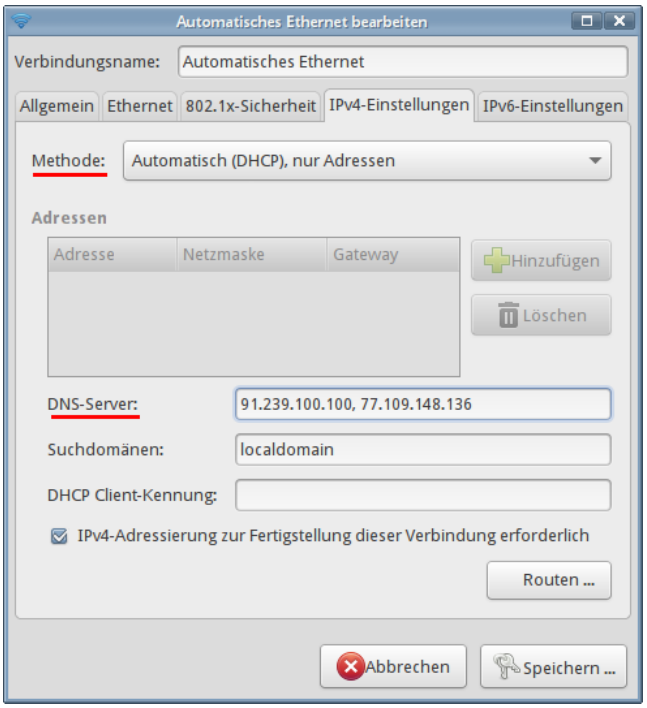


Abbildung 14.1: Konfiguration der DNS-Server im NetworkManager (Linux)

Verschlüsseltes DNS nutzen

Wenn man DNS-over-TLS, DNS-over-HTTPS oder DNScrypt einsetzen möchte, muss man einen DNS-Daemon lokal auf dem Rechner installieren bzw. konfigurieren, der als DNS-Proxy agiert und den DNS-Traffic zum Upstream-Server verschlüsselt.

Windows unterstützt in der Standardinstallation noch kein verschlüsseltes DNS. Interessierte Nutzer können den *SimpleDNScrypt* verwenden.[13]

Nach der Installation des MSI-Paketes kann man im GUI die Auswahl der Server konfigurieren. Man kann Anforderungen definieren und aus einer Liste die gewünschten Server auswählen oder dem Daemon die automatische Auswahl überlassen. Bei automatischer Auswahl werden auch die DNS-Server von Google und Cloudflare verwendet und aufgrund der hohen Performance bevorzugt.

Linux-Distributionen verwenden überwiegend *systemd-resolve* für die DNS-Namensauflösung. Der *systemd* in einer Version > 245.2-1 (Ubuntu 20.04+, Fedora 32+) beherrscht DNS-over-TLS und man kann ihn aktivieren, indem man eine Datei *upstream.conf* im Verzeichnis */etc/systemd/resolved.conf.d/* speichert. Ein Beispiel für die Quad9 Server:

```
[Resolve]
DNS=9.9.9.9#dns.quad9.net
DNS=149.112.112.112#dns.quad9.net
DNSOverTLS=yes
```

Es können mehrere DNS-Server angegeben werden. Die Adresse eines Servers besteht aus der IP-Adresse und dem Namen des Servers für die TLS-Authentifizierung.

Außerdem darf sich der NetworkManager nicht in die Konfiguration der DNS-Server einmischen! Dafür speichert man eine Konfigurationsdatei *nodns.conf* im Verzeichnis */etc/NetworkManager/conf.d/* mit folgendem Inhalt:

```
[main]
dns=none
systemd-resolved=false
```

Hinweis: Diese Konfiguration ist nicht für Road Warriors geeignet, die unterwegs Wi-Fi-Hotspots mit Login-Webseiten in Hotels oder am Flughafen nutzen wollen.

Android Smartphones können DNS-over-TLS out-of-the-box. Die Option heißt *Privates DNS* und verbirgt sich in den erweiterten Einstellungen für *Netzwerk & Internet*. Hier kann man den Namen des gewünschten DoT-Servers eintragen (Abb. 14.2).

Die initiale Ermittlung der IP-Adresse des DNS-over-TLS-Servers erfolgt mit dem Standard-Resolver, danach wird auf DNS-over-TLS umgeschaltet.

Mit dieser Methode lässt sich auch ein Trackingblocker für Android realisieren, indem man einen DNS-Server mit Werbe- und Trackingfilter auswählt.

iPhones unterstützen verschlüsseltes DNS seit iOS Version 14. Die Konfiguration ist ein bisschen umständlicher als bei Android, aber machbar.

[13] https://github.com/instantsc/SimpleDnsCrypt?tab=readme-ov-file

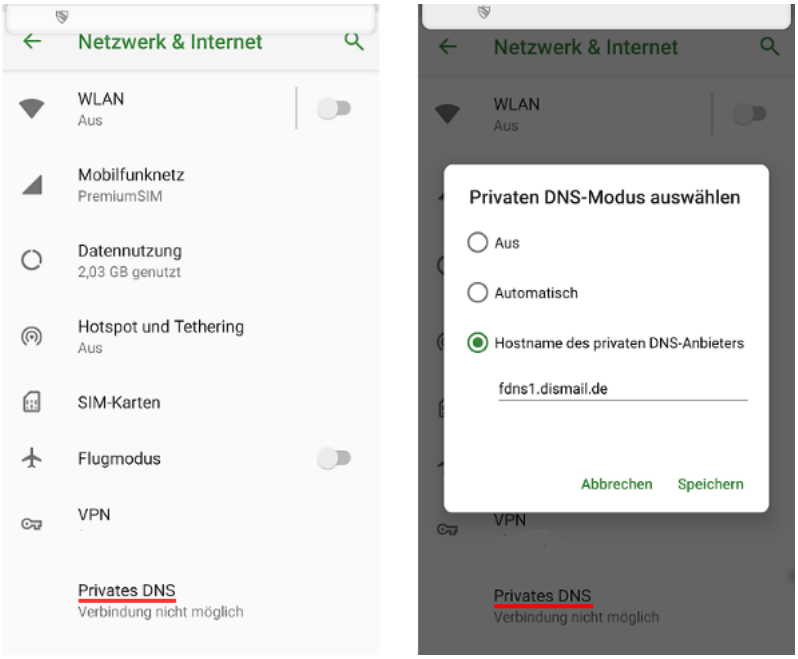


Abbildung 14.2: Android: DNS-over-TLS aktivieren

Man muss sich ein Konfigurationsprofil für den DNS-Server herunterladen. Es gibt mehrere Websites (z. B. encrypted-dns.party), die Profile für einige DNS-Server bereitstellen. Es ist aber empfehlenswert, ein signiertes Profil direkt vom Anbieter herunterzuladen, z. B. vom russischen DNS-Anbieter AdGuard.

Nach dem Download kann man den Browser schließen und das Konfigurationsprofil ist zu installieren: *Einstellungen* → *Profil geladen*.

Standardmäßig ist das zuletzt installierte Profil automatisch aktiv. Wenn man mehrere Profile für DNS-Server installiert hat, kann man in den Einstellungen unter *Allgemein* → *VPN & Netzwerk* → *DNS* das aktive Profil auswählen.

Kapitel 15

Daten verteilen

Der moderne Mensch ist digital vernetzt. Man verwendet mehrere Geräte, auf denen man die gleichen Daten nutzen möchten (z. B. Adressbücher, Passwortdatenbanken usw.) oder möchte irgendwelchen Daten oder Bilder mit Bekannten austauschen.

15.1 Wenige Dateien verteilen (an Bekannte und zwischen den eigenen Geräten)

- Dateien **per E-Mail verschicken** ist nicht wirklich orginell. Manche Leute verschicken E-Mails mit Dateianhängen auch an sich selbst, um Daten zwischen PC und Smartphone auszutauschen.

  Echte Profis schaffen es sogar, ihre E-Mails zu verschlüsseln, damit sie nicht vom E-Mail Provider beschnüffelt werden. Das notwendige Wissen dazu ist aber nicht sehr verbreitet.

- Man kann Dateien **per Messenger austauschen** und profitiert dann bei guten Messengern von der sicheren Ende-zu-Ende Verschlüsselung, was ein Vorteil gegenüber E-Mail ist.

  Um Daten zwischen den eigenen Geräten auszutauschen, kann man den Multi-Device Support der Messenger nutzen. Man installiert den Messenger Client auf allen Geräten und erstellt eine geschlossene Chatgruppe nur für sich allein (Selbstgespräch). Dort kann man alle Daten speichern, die man auf mehreren Geräten braucht. Einige Messenger haben dafür vorbereitete Chats wie z. B. Signal App (*Notiz an mich*) oder Telegram (*Gespeichertes*).

- Innerhalb des gleichen LAN/WLAN kann man einzelne Dateien serverlos direkt zwischen den Geräten (PC, Laptop, Smartphone) austauschen. Die Geräte müssen dabei direkt miteinander kommunizieren können (was bei Gäste-WLANs aus Sicherheitsgründen oft nicht möglich ist) und die Firewalls auf den Geräten müssen die Kommunikation erlauben.

  Alternativen zu proprietären Tools wie AirDrop von Apple sind *LocalSend* oder *KDE Connect / GSConnect*, die es für Androids, iPhones, Windows, MacOS und Linux gibt.

- Große Dateien bis zu einigen TeraByte kann man **via 1-Klick-Hoster versenden**. Nach dem Upload schickt man den Empfängern den Download Link und evtl. das Passwort für den Download via Messenger oder E-Mail. Einige (spendenfinanzierte) Angebote:

  – Send - adminForge[1] (bis zu 8 GB, Dateien sind Ende-zu-Ende verschlüsselt, Schlüssel in Download-URL, Passwortschutz möglich, Uploads bis zu 7 Tage verfügbar)

[1] https://send.adminforge.de

  - Lufi - adminForge[2] (bis zu 2 GB, Dateien sind Ende-zu-Ende verschlüsselt, Schlüssel in Download-URL, Passwortschutz möglich, Uploads bis zu 30 Tage verfügbar)
  - Lufi - Disroot[3] (bis zu 2 GB, Dateien sind Ende-zu-Ende verschlüsselt, Schlüssel in Download-URL, Passwortschutz möglich, Uploads bis zu 30 Tage verfügbar)

Mit diesen Methoden kann man einzelne Dateien zwischen seinen Geräten austauschen oder an Freunde schicken. Für die Synchronistaion von Daten, Online Backups oder das Verteilen größerer Mengen von Daten (Urlaubsbilder o. ä.) braucht man eine Cloud Lösung.

15.2 Private, eigene Cloud

- Wer eine **Fritz!Box** als Router verwendet, kann mit Fritz!NAS eine eingebaute Mini-Cloud zum Speichern und Verteilen von Dateien nutzen und via USB den Speicherplatz erweitern.

  Anleitungen zur Nutzung des Fritz!NAS stellt AVM als Video oder Text zur Verfügung.

- Ein **eigener Nextcloud Server** zuhause bietet mehr Möglichkeiten zur Synchronistation und Backup von Daten. Neben Dateien kann man auch Adressbücher via CardDAV zwischen mehreren Geräten/Programmen synchronisieren, Kalender und Aufgaben via CalDAV...

  Die NextBox[4] von der Nitrokey GmbH ist ein fertig eingerichteter Nextcloud Server für zuhause und ohne großen Installations- und Pflegeaufwand lauffähig.

- Eine Nummer größer sind **NAS** (Network Attached Storage) wie die Diskstations von Synology oder QNAP, die mit mehreren Festplatten ausgerüstet werden können und in variablen RAID Konfigurationen eine besser Ausfallsicherheit bieten. Ein NAS bietet viele Möglichkeiten, um auf die Daten zuzugreifen: Neben WebDAV, CardDAV, CalDAV auch SMB, SSH, FTP usw.

Um auch von unterwegs auf die private Daten zuhause lesend und schreibend zugreifen zu können, kann man ein VPN verwenden (Kapitel 13.3). Das ist sicherer, als den privaten Server ins Internet zu exponieren, wo er für jeden mittelmäßig begabten Hacker mehr oder wenigen angreifbar sind.

Empfehlung: Es ist sinnvoll, für jede Personen (Papa, Mama, Thronfolger, Prinzessin... usw.) einen Account auf dem Datenspeicher einzurichten (mit spezifischen Schreib- und Leserechten für eigene und gemeinsam genutzte Verzeichnisse) aber die VPN Accounts spezifisch für jedes Gerät auf dem Router oder VPN Server einzurichten, damit man bei der Entsorgung eines Gerätes einfach den VPN Account löschen kann ohne Passwörter auf anderen Geräten ändern zu müssen.

Man könnte auf der privaten Cloud einen Gastaccount mit Nur-Leserechten für ein freigegebenes Verzeichnis einrichten, der (temoprär) direkt aus dem Internet erreichbar sein könnte (um der Verwandschaft Urlaubs- oder Hochzeitsbilder o. ä. zu präsentieren) Dafür braucht man nur einen DynDNS Namen, unter welchem der eigene Router aus dem Internet erreichbar ist und eine Portweiterleitung auf dem Router zur eigenen Cloud - kann man machen.

15.3 Cloudserver von Dritten (also die sogenannte Klaut)

- Viele E-Mail Provider bieten Cloud Funktionalitäten zusammen mit dem E-Mail Account.

[2] https://upload.adminforge.de
[3] https://upload.disroot.org
[4] https://shop.nitrokey.com/de_DE/shop/product/nextbox-116

  - Zu einem ProtonMail Account gehört der Ende-zu-Ende verschlüsselter Datenspeicher ProtonDrive. Auf dem PC/Laptop kann man via Browser darauf zugreifen und für Smartphones gibt es Apps von Proton für das Drive. Bisher nur für Windows gibt es eine Anwendung, um Verzeichniss auf dem PC mit dem ProtonDrive zu synchronisieren.

    Für Verzeichnisse oder Dateien kann man einen Freigabenlink erstellen und diesen Link an Dritte senden, denen man die Daten zur Verfügung stellen oder zeigen möchte.
  - mailbox.org (ab dem 3,- Euro Tarif) oder Mailfence bieten Cloud Funktionalitäten wie Dateispeicher, WebDAV, CardDAV oder CalDAV.

    Um die Verschlüsselung der Dateien im Cloudspeicher muss man sich selbst kümmern und die Freigabe für Dritte ist möglich.

Man muss nicht gleich alle Daten in der Klaut speichern. Bei Adressbüchern könnte man z. B. ein Adressbuch für die Familie pflegen und für alle Familienmitglieder freigeben oder ein Adressbuch für Vereinsmitglieder an zentraler Stelle durch einen Beauftragten verwalten lassen. E-Mail Programme wie Thunderbird können diese Adressbücher via CardDAV importieren und für Smartphones gibt es Apps wie DAVx[5] für Android...

Hinweis: Wenn man Daten von Dritte verteilt, braucht man die Zustimmung der Betroffenen!

Man kann auch Verzeichnisse (mit den Urlaubs- oder Hochzeitsbildern o. ä.) oder einzelne Dateien via WebDAV sehr einfach für Dritte freigeben. Der Freigabelink kann zeitlich befristet und mit Passwort geschützt werden, dass man per Messenger oder E-Mail verteilt.

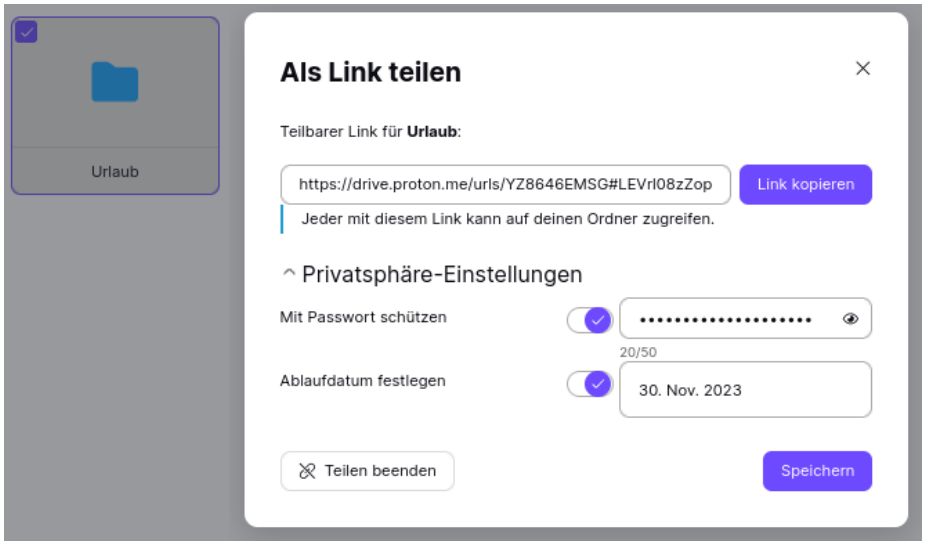


Abbildung 15.1: Freigabelink für ein Verzeichnis im ProtonDrive erstellen

- Einen Nextcloud Account mit allen Möglichkeiten zum Datenaustausch, die eine Nextcloud bietet, gibt es (spendenfinanziert) beispielsweise bei adminForge mit bis zu 3 GB Speicher.
- Außerdem gibt es **kommerzielle Datenspeicher** mit preisgestaffeltem Datenvolumen im Terabyte Bereich inklusive Verschlüsselung wie Strato HiDrive[5], Tresorit[6] oder filen.io[7] mit Apps für (fast) alle System und der Möglichkeit, Freigaben für Dritte zu verwalten.

[5] https://www.strato.de/cloud-speicher
[6] https://tresorit.com/de
[7] https://filen.io

- **CryptPad** ist eine Open Source Software für collaboratives Bearbeiten von Office Dokumenten im Browser (Text, Tabellen, Diagramme), also eine Alternative zu Google Docs. Im Gegensatz zu Google Docs werden die Dokumente im Browser Ende-zu-Ende verschlüsselt bevor sie auf dem Server gespeichert werden, so dass der Betreiber der Plattform keinen Zugriff hat. Es gibt mehrere CryptPad Instanzen, die man mit oder ohne Account nutzen kann. Die Instanz der Entwickler ist Cryptpad.fr, deutsche Server gibt es bei adminForge[8] oder Digitalcourage[9].

  Wenn man ein Dokument erstellt und eine erste Version gespeichert hat, kann man mit dem *Teilen* Button einen Freigabelink erstellen, den man im Team verteilen kann. Dabei kann man Rechte zum Bearbeiten des Dokumentes erteilen oder nur zum Betrachten.

  Der Link enthält die notwendigen Schlüssel zum Entschlüsseln der Daten und sollte über einen sicheren(!) Kanal verteilt werden. Wer den Link per unverschlüsselter E-Mail an einen GMail Account schickt, sollte sich nicht wundern, wenn die NSA irgendwann den Inhalt kennt.

  Eine Registrierung mit E-Mail Adresse ist bei einer CryptPad Instanz nicht unbedingt notwendig, man kann als Gast arbeiten. Dafür sollte man der CryptPad Instanz das dauerhafte Speichern von Cookies im Browser erlauben, damit die Schlüssel beim Schließen des Browser nicht verloren gehen. Die Dokumente von Gästen werden nach 90 Tagen automatisch gelöscht.

  Als registrierter Nutzer bleiben die Dokumente unbgrenzt erhalten (bis zur Löschung durch den Nutzer) und man kann detailliertere Rechte für Dokumente vergeben. Außerdem kann man das CryptPad Drive als kleinen Cloudspeicher zum Verteilen von Dateien verwenden. Auf der adminForge Instanz steht registrierten Benutzern bis zu 1 GB Speicher zur Verfügung.

  Bei Cryptpad.fr gibt es kostenpflichtige Premiumaccounts mit mehr Speicher und Support.

[8] https://cryptpad.adminforge.de
[9] https://cryptpad.digitalcourage.de

Kapitel 16

Daten verschlüsseln

Dass die Verschlüsselung von Daten der Erhaltung der Privatsphäre dient, bemerkt man spätestens, wenn ein USB-Stick verloren geht. Wird ein Laptop gestohlen, möchte man die Fotosammlung sicher nicht im Internet sehen.

Journalisten, Rechtsanwälte und auch Priester haben das Recht und die Pflicht, Daten über ihre Informanten bzw. Klienten zu schützen. Sie sollten sich frühzeitig Gedanken über ein Konzept zur Verschlüsselung machen. Es ist wirklich ärgerlich, wenn die Rote Hilfe einen unverschlüsselten Datenträger mit Mitgliederdaten verliert. Das kann ernste Konsequenzen haben.

Als Whistleblower sind besondere Anforderungen an die Datensicherheit zu stellen. Neben der sicheren Aufbewahrung kommt es auch darauf an, keine Spuren auf den Rechnern zu hinterlassen. Im Fall Bradley Mannings konnten Forensiker viele Daten wiederherstellen.

Die Beispiele zeigen, dass unterschiedliche Anforderungen an eine Verschlüsselung bestehen können. Bevor man wild anfängt, alles irgendwie zu verschlüsseln, sollte man sich deshalb Gedanken über die Bedrohung machen, gegen die man sich schützen will:

1. **Schutz sensibler Daten** wie z. B. Passwortlisten, Revocation Certificates o. Ä. erfordert die Speicherung in einem Container oder verschlüsselten Archiv, welches auch im normalen Betrieb geschlossen ist.

2. **Schutz aller persönlichen Daten** bei Verlust oder Diebstahl von Laptop oder USB-Stick erfordert eine Software, die transparent arbeitet, ohne den Nutzer zu behindern und bei korrekter Anmeldung möglichst automatisch den Daten-Container öffnet (beispielsweise Veracrypt für Windows/Linux oder dm-crypt für Linux).

3. **Backups auf externen Medien** enthalten in der Regel die wichtigen privaten Daten und sollten daher verschlüsselt sein. Dabei sollte die Wiederherstellung auch bei totalem Datenverlust möglich sein. Es ist nicht sinnvoll, die Daten mit einem PGP-Schlüssel zu chiffrieren, der nach einem Crash nicht mehr verfügbar ist.

4. **Daten in der Cloud** sollten ebenfalls transparent verschlüsselt werden. Außerdem sollte die Verschlüsselung die Synchronisation geänderter Dateien im Hintergrund nicht behindern. Container-basierte Lösungen wie dm-crypt oder Veracrypt sind weniger geeignet, da man bei einer kleinen Änderung nicht den gesamten Container hochladen möchte. Besser geeignet sind verzeichnisbasierte Ansätze wie ecryptfs, CryFS oder Cryptomator.

5. Wer eine **Manipulation der Systemdaten** befürchtet, kann seinen Rechner komplett verschlüsseln (z. B. mit dm-crypt für Linux).

16.1 Konzepte der vorgestellten Tools

Um die vorgestellten Tools sinnvoll einzusetzen, ist es nötig, die unterschiedlichen Konzepte zu verstehen.

KeepassXC kann nicht nur Passwörter speichern sondern ist als hierarchisch organisierte, verschlüsselte Datenbank für viele sensible Textdaten geeignet. Falls die Standardfelder nicht ausreichen, kann man für jeden Datensatz zusätzliche Felder definieren und auch Dateien als BLOB einfügen.

LibreOffice kann einzelne Dokumente mit sensiblen Inhalten (Texte, Tabellenkalkulationen usw.) mit einer Passphrase oder mit GnuPG-Schlüsseln verschlüsseln.

GnuPG arbeitet Datei-orientiert. Einzelne Dateien können verschlüsselt werden. Die unverschlüsselten Originaldateien sind danach sicher(!) zu löschen, damit keine Spuren auf der Festplatte bleiben.

ecryptfs und **Cryptomator** arbeiten verzeichnisbasiert und sind für die Cloud geeignet. Es gibt bei dem Verfahren zwei Verzeichnisse:

1. Das Verzeichnis A mit den verschlüsselten Daten wird auf den Datenträger geschrieben bzw. in die Cloud synchronisiert.
2. Ein zweites, virtuelles Verzeichnis B oder ein virtuelles Laufwerk bietet transparenten Zugriff auf die entschlüsselten Dateien, wenn das Tool gestartet wurde.

Für Schreib- und Leseoperationen wird das Verzeichnis B verwendet, wo man die Daten unverschlüsselt sieht, sobald Cryptomator oder ecryptfs gestartet wurden.

CryFS hat nach Ansicht der Entwickler noch nicht die Stabilität einer Version 1.0 erreicht, ist aber schon nutzbar. Es arbeitet ähnlich wie ecryptfs oder Cryptomator mit zwei Verzeichnissen. Es werden aber nicht nur die Dateien verschlüsselt, sondern auch die Verzeichnisstruktur und Metadaten der Dateien wie z. B. die Dateigröße werden verborgen. In dem Verzeichnis mit den verschlüsselten Dateien sieht man nur verschlüsselte Blöcke identischer Größe.

dm-crypt/LUKS arbeiten Container-basiert. Es ist zuerst ein verschlüsselter Container fester Größe zu erstellen, der dann wie ein Datenträger in das Dateisystem eingebunden werden kann. Als Container können komplette USB-Sticks, ganze Partitionen der Festplatte oder (große) Dateien genutzt werden.

Ein Container nimmt immer die gleiche Menge an Platz ein, egal ob leer oder voll. Ist der Container verschlossen, kommt niemand an die dort lagernden Daten heran. Mit einem Schlüssel kann der Container geöffnet werden (gemounted: in das Dateisystem eingehängt) und jeder, der an einem offenen Container vorbeikommt, hat Zugriff auf die dort lagernden Daten. Als Schlüssel dient eine Passphrase und/oder Schlüsseldatei(en).

Der Zugriff auf Dateien innerhalb des geöffneten Containers erfolgt mit den Standardfunktionen für das Öffnen, Schließen und Löschen von Dateien. Auch Verzeichnisse können angelegt und gelöscht werden. Die Verschlüsselung erfolgt transparent ohne weiteres Zutun des Nutzers.

Veracrypt arbeitet wie *dm-crypt/LUKS* mit Containern. Zusätzlich bietet es mit *versteckten Volumes* eine Art doppelten Boden für den verschlüsselten Container. Der Zugriff auf diesen

Bereich ist mit einem zweiten Schlüssel, einer weiteren Passphrase und/oder Schlüsseldatei(en) geschützt. Öffnet man den Container mit dem ersten Schlüssel, erhält man Zugriff auf den äußeren Bereich. Verwendet man den zweiten Schlüssel zum Öffnen des Containers, erhält man Zugriff auf den Inhalt im doppelten Boden.

Während ein einfacher Container leicht als verschlüsselter Bereich erkennbar ist, kann der doppelte Boden innerhalb eines Containers ohne Kenntnis des zweiten Schlüssels nicht nachgewiesen werden. Ist man zur Herausgabe der Schlüssel gezwungen, kann man versuchen, nur den Schlüssel für den äußeren Container auszuhändigen und die Existenz des doppelten Bodens zu leugnen.

Ob es plausibel ist, die Existenz des doppelten Bodens zu leugnen, hängt von vielen Faktoren ab. Zeigt z. B. die Historie der geöffneten Dokumente einer Textverarbeitung, dass vor kurzem auf einen verschlüsselten Bereich zugegriffen wurde, und man präsentiert einen äußeren Container, dessen letzte Änderung Monate zurück liegt, trifft man wahrscheinlich auf einen verärgerten Richter. Auch der Such-Index verschiedener Programme für die Indexierung der Dokumente auf dem lokalen Rechner (Windows Suche...) liefern möglicherweise Hinweise auf den versteckten Container.

Außerdem bietet Veracrypt verschiedene Verschlüsselungsalgorithmen (Cipher) oder entsprechende Kombinationen. Man kann bei einem Veracrypt-Container nicht von außen erkennen, welche Cipher verwendet wurden. Beim Öffnen des Containers werden mit dem Passwort alle Varianten durchprobiert, bis eine passt.

Auch ein Angreifer, der mit Brute-Force das Passwort erraten will, müsste eigentlich immer alle Varianten ausprobieren. Die gängigen Tools zum Knacken eines Veracrypt-Containers wie Elcomsoft u. Ä. verwenden häufig eine Abkürzung und probieren nur die Default-Einstellung AES aus. Dann geht der Angriff wesentlich schneller.

Um den maximal möglichen Schutz bei Veracrypt zu erreichen, sollte man beim Erstellen eines Containers also immer einen anderen Cipher für die Verschlüsselung auswählen und nicht den Defaultwert übernehmen. Dann muss auch ein Angreifer den langsamen Weg probieren und alle Cipher testen. Welchen Cipher man wählt, ist dabei egal, Hauptsache nicht AES.

16.2 Gedanken zur Passphrase

Die im folgenden vorgestellten Tools zur Datenverschlüsselung arbeiten in der Regel mit symmetrischer Verschlüsselung (Ausnahme GnuPG: hybride Verschlüsselung).

1. Bei der Initialisierung wird eine kleine Menge von Zufallszahlen generiert, die als Schlüssel für die symmetrische Verschlüsselung mit AES256-XTS o. Ä. dient.
2. Dieser Schlüssel aus Zufallszahlen wird mit einer Passphrase verschlüsselt und im Header der verschlüsselten Daten gespeichert.
3. Beim Zugriff auf die Daten wird zuerst der Schlüssel aus Zufallszahlen mit dem Passphrase entschlüsselt und danach für den Zugriff auf die Daten genutzt.

Es ist nach derzeitigem Stand der zivilen Kryptoanalyse unmöglich, die symmetrische Verschlüsselung wie AES-XTS oder Twofisch usw. mit mathematischen Methoden zu knacken, wenn hinreichend zufällige Zufallszahlen als Schlüssel verwendet werden.

Alle bekannten Angriffe auf moderne Datenverschlüsselungen konzentrieren sich darauf, die Passphrase zu erraten, um Zugriff auf den Schlüssel für die symmetrische Verschlüsselung zu bekommen und somit die geschützten Daten lesen zu können.

Die Stärke und Länge der Passphrase ist deshalb der entscheidende Faktor für die Sicherheit der Datenverschlüsselung und gleichzeitig das schwächste Glied in der Kette. Eine Passphrase, welche die gleiche Stärke gegen Brute-Force-Angriffe wie AES128 hätte, müsste bspw. aus mindestens 12 zufällig generierten Wörtern bestehen (Diceware):

```
"stuff plastic young air easy husband exact install web stick hurt embody"
```

Das ist schon etwas kompliziert zu merken und in der täglichen Benutzung ganz schön umständlich. In der Regel werden die meisten Anwender einfachere Passphrasen wählen und damit ist die Passphrase der schwächste Punkt der Verschlüsselung.

Wie findet man eine ausreichend starke Passphrase?

Ein 6-stelliges Passwort zu knacken, kostet 0,10 Euro. Eine 8-stellige Kombination hat man mit 300 Euro wahrscheinlich und mit weniger als 800 Euro sicher geknackt. Um eine 15-stellige Kombination aus zufälligen Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen oder eine Diceware-Passphrase aus 6 Wörtern mit 50 % Wahrscheinlichkeit zu knacken, würden auch die Computer der NSA viele Jahre benötigen.

Für eine gute Passphrase sollte man mindestens 12 zufällige Zeichen verwenden (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) oder eine Diceware-Passphrase mit mindestens 5 Wörtern. Für eine gute Passphrase sind mindestens 65 Bit Entropie nötig.

- Passwortspeicher wie KeepasXC enthalten einen Generator für wirklich zufällige Zeichenkombinationen oder auch Diceware-Passphrasen.

  Ein Passwortspeicher wie KeepassXC o. Ä. ist aber evtl. nicht immer verfügbar, wenn man Zugriff auf Datenträger braucht (das sollte man bedenken).

- Ein memorierbares Passwortsystem hat den Vorteil, dass man nicht von Tools abhängig ist und bei einem Crash des Computers kein aktuelles Backup braucht.

  Die **Akronym-Methode** verwendet die Anfangsbuchstaben der Wörter in einem leicht merkbaren Satz und leitet den variablen Anteil aus der Verwendung ab:

  - Merksatz: *Die Sonne schien am ganzen Sonntag nur für uns.*
  - Passwort für USB-Sticks: *DSsagSn4u-STICK*
  - Passwort für Systemplatte: *DSsgaSn4u-BOOT*

  Die **Collage-Methode** verwendet ein Wort in mehreren Übersetzungen und lässt die Vokale weg. Variable Anhängsel sind ebenfalls möglich:

  - *Ergebnis:Result=42* könnte folgendes Passwort ergeben: rgbns:Rslt=42
  - *Pferd?Horse!Cheval* könnte folgendes Passwort ergeben: Pfrd?Hrs!Chvl

- Beim **Diceware**-Verfahren werden zufällige Kombinationen aus Wörtern aus einer Liste statt zufälliger Zeichenkombinationen verwendet. Wortkombinationen kann man sich leichter merken als sinnlose Zeichenketten.

  Für den klassischen Weg zur Erstellung einer Diceware-Passphrase benötigt man eine Wortliste (bspw. die *DeReKo-Liste*[1] mit den häufigsten deutschen Wörtern laut Leibnitz-

[1] https://www.privacy-handbuch.de/download/diceware-dereko.txt

Institut) und einen Würfel. Für jedes Wort würfelt man fünf Mal und erhält damit eine Zahlenkombination. Diese Kombination sucht man in der Wortliste und wiederholt den Vorgang für 5–7 Wörter.

```
26431 gebilde
53612 schmal
42221 macht
66123 zauber
34641 karwoche
```

Ein Sonderzeichen zur Worttrennung kann man sich aussuchen. Und die gewürfelte Diceware Passphrase ist dann: *gebilde-schmal-macht-zauber-karwoche*.

Wenn man keine Würfel im Haushalt findet, kann man auch online würfeln.[2]

- Beim **Challenge-Response**-Verfahren mit Yubikeys wird ein einfaches Passwort an den Yubikey geschickt (Challenge), der mit HMAC-SHA ein starkes Passwort ableitet (Response), das für den Zugriff auf den Schlüssel für die symmetrische Verschlüsselung verwendet wird.

  Challenge-Response mit Yubikeys muss von der Software unterstützt werden:

  – KeepassXC-Datenbanken für Passwörter können damit geschützt werden.
  – dmcrypt/LUKS bietet Unterstützung für Challenge-Response mit Yubikeys.

  Um den Yubikey für Challenge-Response vorzubereiten, ist die nötige Software zu installieren. Linuxer finden das Yubico Personalisation Tool in den Repositorys:

```
> sudo apt install yubikey-personalisation
```

  Dann wird der zweite Passwort-Slot des Yubikey für den Challenge-Response initialisiert:

```
> ykpersonalize -2 -ochal-resp -ochal-hmac -ohmac-lt64
↪  -oserial-api-visible
```

Herausgabe von Passwörtern an Strafverfolgungsbehörden

Zur Herausgabe von Passwörtern im Fall einer Beschlagnahme des Rechners oder eines verschlüsselten Datenträgers gibt es immer wieder Missverständnisse. In Deutschland gelten folgende gesetzliche Reglungen:

- Richten sich die Ermittlungen gegen den Besitzer des Rechners oder Datenträgers, muss man keine Passwörter herausgeben, da man sich selbst nicht belasten muss.
- Richten sich die Ermittlungen gegen Dritte, ist man als Zeuge zur Herausgabe von Schlüsseln und Passwörtern zur Unterstützung der Strafverfolgung verpflichtet.

  Es gibt nur zwei Ausnahmen:

  1. Man kann sich auf das Recht zur Zeugnisverweigerung berufen, um Verwandte ersten Grades nicht belasten zu müssen.

[2] https://online-wuerfel.de/5-wuerfel

2. Man kann glaubhaft(!) versichern, dass man sich selbst belasten würde.

Im Zweifel sollte man einen Anwalt konsultieren, wenn man in dieser Situation ist.

In Großbritannien ist es bereits anders. Gemäß dem dort seit 2007 geltendem RIPA-Act können Nutzer von Verschlüsselung unter Strafandrohung zur Herausgabe der Schlüssel gezwungen werden. Es drohen bis zu zwei Jahre Gefängnis oder Geldstrafen. Dass die Anwendung des Gesetzes nicht auf böse Terroristen beschränkt ist, kann man bei Heise.de nachlesen. Das Gesetz wurde als Erstes gegen eine Gruppe von Tierschützern angewendet.[3]

Bei Einreise in die USA sind die Grenzbehörden berechtigt, elektronische Geräte (Laptops und Smartphones) zu durchsuchen. Eine Herausgabe von Passwörtern kann ohne Durchsuchungsbeschluss nicht erzwungen werden, aber die Behörden können das Gerät zur weiteren Untersuchung einziehen, wenn man das Passwort nicht herausgeben will. Die EFF.org rät, mit einer leeren, unverschlüsselten Festplatte einzureisen und ein datenloses Handy zu nutzen.[4]

Den Polizeibehörden ist bekannt, dass es starke Verschlüsselung für Festplatten gibt, die im ausgeschalteten Zustand nicht geknackt werden kann. Deshalb sind die Festnahme-Spezialisten des SEK u. Ä. darin geschult, bei einer Festnahme (Polizei-Sprech: *Zugriff*) die Computer im eingeschalteten Zustand zu übernehmen und ein Backup der unverschlüsselten Daten anzufertigen.

- Ross Ulbricht (der Betreiber von Silk Road 2.0) wurde festgenommen, während er seinen Tor-Hidden-Service administrierte. Das FBI konnte den eingeschalten Laptop übernehmen und als Beweis die aktiven Login-Sessions auf den Servern des Drogenhandelsplatzes sicherstellen. Das war sicher kein Zufall sondern beabsichtigt.
- Der deutsche Betreiber eines illegalen Waffenhandels im Deep Web konnte bei der Festnahme mit dem Fuß das Stromkabel aus seinem batterielosen Laptop reißen und die Verschlüsselung damit aktivieren. Das SEK hatte aber zweifellos den Auftrag, bei der Festnahme den Laptop im eingeschalteten Zustand sicherzustellen.[5]

[3] http://www.heise.de/newsticker/meldung/99313
[4] https://www.eff.org/wp/digital-privacy-us-border-2017
[5] http://motherboard.vice.com/de/read/bis-das-sek-kommt

16.3 Dokumente verschlüsselt speichern

Es gibt mehrere Anwendungen, die Dokumente verschlüsselt speichern können. Das Öffnen der Dokumente ist dann nur möglich, wenn das notwendige Passwort angegeben wird. Die verschlüsselte Speicherung ist bei vertraulichen Daten wie Steuererklärungen, Mitgliederlisten für politisch aktive Vereine usw. sinnvoll.

Man kann verschlüsselte Dokumente auch als Quick&Dirty-Alternative zu verschlüsselten E-Mails verwenden, indem man den Inhalt in ein verschlüsseltes Dokument schreibt und dieses Dokument als Anhang mit der E-Mail schickt. Das Passwort zum Öffnen des Dokumentes muss man dem Empfänger über einen sicheren Kanal mitteilen.

LibreOffice-Dokumente verschlüsselt speichern

LibreOffice bietet die Möglichkeit, Dokumente mit AES256 verschlüsselt zu speichern, indem man beim Speichern die Option *Mit Kennwort speichern* aktiviert. Außerdem können die Dokumente mit OpenPGP verschlüsselt gespeichert werden (Abb. 16.1).

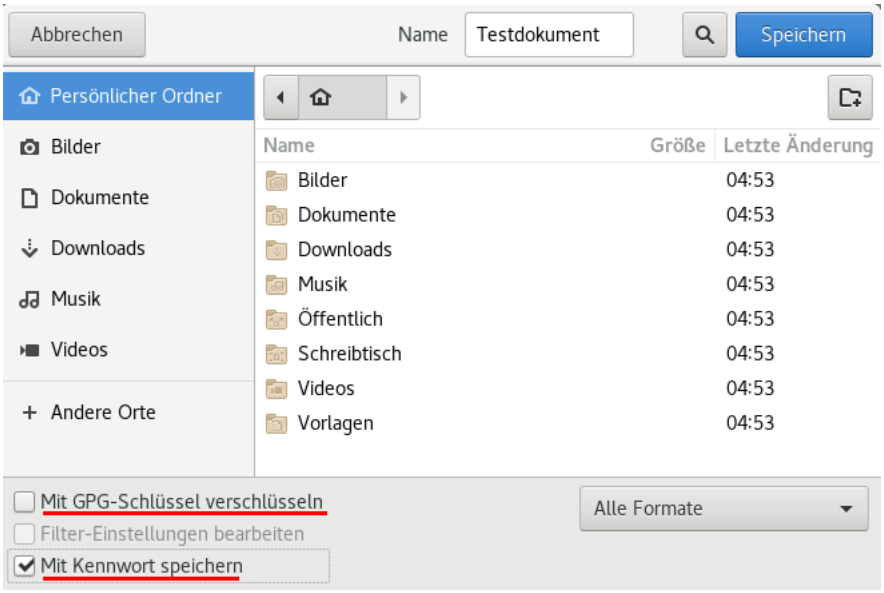


Abbildung 16.1: Verschlüsselte Speicherung in LibreOffice aktivieren

Im folgenden Dialog kann man den/die OpenPGP-Schlüssel auswählen oder ein Kennwort für das Öffnen der verschlüsselten Datei festlegen. Um keine Spuren auf der Festplatte zu hinterlassen, sollte man den Schutz aktivieren, bevor das Dokument erstmalig gespeichert wird und bevor sensitive Daten in das Dokument geschrieben werden.

PDF-Dokumente

Der PDF-Standard definiert ein Berechtigungsmodell, das auch die verschlüsselte Speicherung von Dokumenten ermöglicht. Dieser Standard ist aber *Broken by Design*. Ein Angreifer kann das PDF-Dokument modifizieren, sodass ihm beim Öffnen des Dokumentes der vertrauliche Inhalt via Internet zugesendet wird.[6]

[6] https://www.pdf-insecurity.org/

> *We analyze the security of encrypted PDF and show how an attacker can exfiltrate the content without having the corresponding keys.*

Die kryptografischen Signaturen im PDF-Standard sind ebenfalls kaputt by Design.

16.4 Quick and Dirty mit GnuPG

Eine Möglichkeit ist die Verschlüsselung einzelner Dateien oder Verzeichnisse mit GnuPG. Die grafischen Tools *GPA* (GNU Privacy Assistent) oder *Kleopatra* bieten dafür im Menü den Punkt *Datei* → *Datei verschlüsseln/signieren* und *Datei* → *Datei entschlüsseln/prüfen*.

Noch einfacher geht es, wenn man im bevorzugten Dateimanager mit der rechten Maustaste auf eine Datei klickt und im Kontextmenü den Punkt *Datei verschlüsseln* wählt. Es startet ein Assistent, der durch die Auswahl der Schlüssel usw. führt.

Abbildung 16.2: Kleopatra GnuPG GUI: Assistent zur Verschlüsselung von Dateien

Mit der Auswahl eines Schlüssels legt man fest, wer die Datei wieder entschlüsseln kann. Für Backups wird in der Regel der eigene Schlüssel verwendet. Es ist auch möglich, mehrere Schlüssel für verschiedene Empfänger zu nutzen. Die Verwaltung der OpenPGP-Schlüssel ist im Kapitel E-Mails verschlüsseln beschrieben. Anschließend ist das unverschlüsselte Original NICHT(!) in den Papierkorb sondern in den Reißwolf zu werfen.

Sollen mehrere Dateien in einem Container verschlüsselt werden, erstellt man ein Verzeichnis und kopiert die Dateien dort hinein. Anschließend verpackt man dieses Verzeichnis mit *WinZip, 7zip* o. Ä. in einem Archiv und verschlüsselt dieses Archiv.

Zum Entschlüsseln reicht in der Regel ein Klick (oder Doppelklick) auf die verschlüsselte Datei. Nach Abfrage der Passphrase für den Schlüssel liegt das entschlüsselte Original wieder auf der Platte.

GnuPG für WINDOWS

Diese simple Verschlüsselung klappt allerdings unter WINDOWS nicht auf Anhieb. Es ist zuerst das Programmpaket **gpg4win**[7] zu installieren.

[7] https://www.gpg4win.org

16.5 BitLocker für Windows

BitLocker ist standardmäßig in den Windows-Pro- und Enterprise-Versionen für die Verschlüsselung von Festplatten enthalten. Die Windows Home Edition enthält mit der *Geräteverschlüsselung* eine abgerüstete Version mit weniger Optionen zur Verwaltung der Schlüssel und Recovery-Keys.

Voraussetzungen für die Aktivierung von BitLocker sind ein TPM-2.0-Chip im Rechner und eine UEFI-Boot-Installation. Die Windows Home Edition benötigt außerdem einen Microsoft-Account, weil der Recovery-Key bei dieser Windows-Edition zwingend in die OneDrive-Cloud hochgeladen wird.

Bei der Installation von Windows 10/11 werden die Daten standardmäßig verschlüsselt gespeichert. Der Schlüssel für den Zugriff auf die Daten wird aber ungeschützt auf der Festplatte abgelegt. Mit der Aktivierung von BitLocker bzw. der Geräteverschlüsselung wird nur der Schlüssel in den TPM-Chip verschoben und ein Recovery-Key erzeugt.

- Das hat den Vorteil, dass die Aktivierung praktisch mit einem Mausklick erfolgen kann und der Nutzer keine länger dauernde Verschlüsselung abwarten muss.
- Das hat den Nachteil, dass die Person, die Windows installiert, eine Kopie des Schlüssels behalten könnte. Wenn man sein Windows 10/11 nicht selbst installiert hat und sicher sein will, dass kein unbefugter Dritter den Schlüssel von BitLocker geklaut hat, muss man alles einmal entschlüsseln und dann wieder neu verschlüsseln.

Aktivierung der Geräteverschlüsselung in Windows 10/11 Home Edition

1. Man muss sich mit einem Account anmelden, der administrative Rechte erlangen kann und für den ein Microsoft-Cloud-Konto eingerichtet wurde.
2. Dann kann man die Geräteverschlüsselung in den *Einstellungen* aktivieren:
   - in Windows 10 unter *Update* → *Geräteverschlüsselung*
   - in Windows 11 unter *Datenschutz und Sicherheit* → *Geräteverschlüsselung*

   Die Aktivierung erfordert nur einen Klick. Damit wird im Hintergrund ein Recovery-Key erzeugt und in die Microsoft-Cloud hochgeladen. Die Entschlüsselung wird an den TPM-Chip gebunden und SecureBoot kann nicht mehr deaktiviert werden (TPM PCR 7). Wenn jemand die Festplatte aus dem Rechner ausbaut, hat er ohne den Recovery-Key nur unlesbaren Datensalat.

   (Wenn man den Recovery-Schlüssel nicht dauerhaft in der Cloud liegen lassen möchte, kann man ihn auf folgender Webseite löschen: https://onedrive.live.com/recoverykey)
3. Es besteht natürlich die Möglichkeit, das sich ein Angreifer des kompletten Rechners bemächtigt. Um zu verhindern, dass dieser Angreifer den Rechner bootet und die Verschlüsselung der Festplatte damit öffnet, kann man im BIOS ein Administrator- bzw. Supervisor-Passwort setzen und die Option *Power-on-password* aktivieren. Das Passwort muss man zukünftig immer eingeben, wenn man den Rechner einschaltet, egal welches Bootmedium man verwendet.

Aktivierung von BitLocker in Windows 10/11 Pro und Enterprise

Es gibt mehrere Möglichkeiten, BitLocker in Windows 10/11 Pro und Enterprise für ein Laufwerk zu aktivieren. Microsoft empfiehlt die App *BitLocker verwalten*. Um die App zu starten, gibt man im Suchfeld beim Startbutton *BitLocker* ein und startet die App. Man kann BitLocker aber auch genau wie die Geräteverschlüsselung in Windows Home in den Einstellungen aktivieren.

Im Unterschied zur Geräteverschlüsselung der Home-Version muss man bei BitLocker den Recovery-Key nicht in der Microsoft-Cloud speichern. Man kann ihn statt dessen in Firmenumgebungen auf dem Active-Directory-Server ablegen, auf einem USB-Stick speichern oder ausdrucken.

Außerdem bietet BitLocker Möglichkeiten zur Pre-Boot-Authentifizierung, so dass man auf die bei Windows Home nötigen Spielereien im BIOS mit dem *Power-on-password* verzichten kann:

- PIN-Eingabe vor dem Windows Start[8]
- USB-Stick mit Schlüsseldatei als Token für den Start
- Wenn man ein Network Bound Unlock einrichtet, bootet Windows nur, wenn der Rechner sich in dem konfiguriertem heimischen LAN oder Firmen-LAN befindet.[9]

Blockcipher für die Verschlüsselung

BitLocker und die Geräteverschlüsselung der Windows Home Edition verwenden XTS-AES-128 als Blockcipher für die Daten. Nach übereinstimmender Einschätzung von NIST, NSA Suite B und BSI ist das keine starke Verschlüsselung. Für die Verschlüsselung von dauerhaft auf Datenträgern gespeicherten Daten wird XTS-AES-256 empfohlen. Um XTS-AES-256 zu verwenden, müssen alle Daten vollständig entschlüsselt werden (BitLocker bzw. Geräteverschlüsselung deaktivieren), ein Registry-Key ist zu setzen und dann sind die Daten durch Aktivierung von BitLocker bzw. Geräteverschlüsselung neu zu verschlüsseln.

Den Registry-Key setzt man im Terminal mit folgendem Kommando:

```
cmd /c reg.exe add HKLM\SOFTWARE\Policies\Microsoft\FVE /v EncryptionMethod
↪  /t REG_DWORD /d 7 /f
```

Das Entschlüsseln und neu Verschlüsseln kann einige Stunden dauern.

[8] https://www.heise.de/tipps-tricks/BitLocker-auf-Windows-10-Festplatte-richtig-verschluesseln-4325375.html
[9] https://learn.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-enable-network-unlock

16.6 dm-crypt/LUKS für Linux

Das Modul dm-crypt/LUKS ist fester Bestandteil des Linux-Kernels und in allen Linux-Distributionen gut integriert. Die Verschlüsselung wird auch von Regierungen und Geheimdiensten zum Schutz vertraulicher und geheimer Daten eingesetzt. dm-crypt/LUKS ist FIPS-2 zertifiziert, wird vom BSI regelmäßig evaluiert und ist in Deutschland bis VS-GEHEIM zugelassen (allerdings ab VS-NfD nur mit Smartcards als Zugriffsschutz, nicht mit Passwörtern).

dm-crypt/LUKS verschlüsselt Blockdevices (Festplattenpartitionen, USB-Sticks oder Imagedateien) und arbeitet vollständig transparent. Es können bis zu 8 unterschiedliche Passphrasen und Schlüsseldateien als Credentials für den Zugriff auf einen Container definiert werden. Außerdem können Veracrypt-Container geöffnet werden.

Aufgrund der langjährigen Integration ist die Nutzung unter Linux einerseits einfach mit den Tools zur Verwaltung von Datenträgern möglich und automatisiert. Andererseits bietet die Kommandozeile im Terminal mehr Optionen für Genießer. Beim Formatieren eines Datenträgers (z. B. USB-Stick) muss man nur die Option zum Verschlüsseln aktivieren.

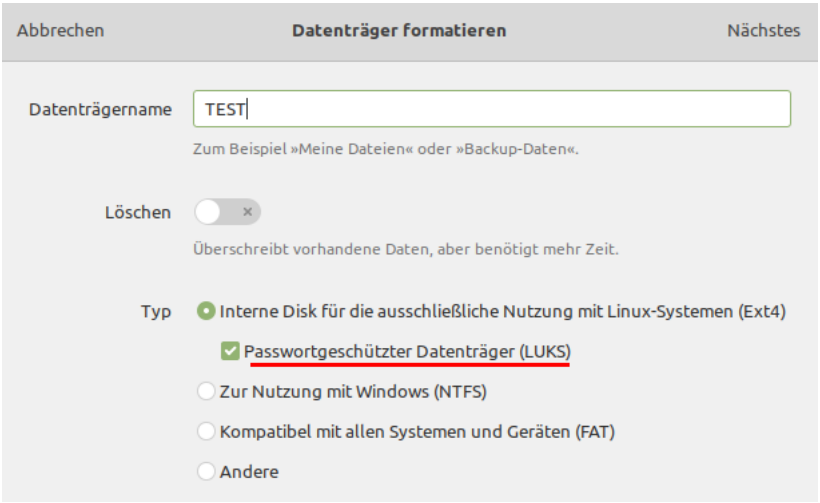


Abbildung 16.3: Datenträger verschlüsseln unter Linux

Im nächsten Schritt wird man nach der Passphrase gefragt, die man wie üblich zweimal eingeben muss. Diese Passphrase wird im Slot 0 im LUKS-Header gespeichert. Die Verwendung von mehreren unterschiedlichen Passphrasen oder Keyfiles als Schlüssel wird in dieser einfachen Variante für Mausschubser nicht unterstützt. Dafür muss man die Kommandozeile nutzen.

Wenn man den verschlüsselten USB-Stick am Linux Rechner anschließt, wird man nach der Passphrase für den Zugriff auf die Daten gefragt und der Datenträger wird geöffnet.

16.6.1 Linux-System komplett verschlüsseln

Neben der einfachen Verschlüsselung von Datenträgern bieten alle Linux-Distributionen bei der Installation die Möglichkeit, das komplette System mit Ausnahme der Boot-Partition zu verschlüsseln, wenn man die Festplatte komplett löscht und den Logical Volume Manager (LVM) für die neue Installation aktiviert. Für die Verschlüsselung des gesamten Systems mit dm-crypt/LUKS ist dann nur ein kleines Häkchen zu setzen.

Beim Linux-Mint-Installer findet man die Option unter dem Punkt *Erweiterte Funktionen ...* Bei anderen Linux-Distributionen sieht es ebenso oder ähnlich aus.

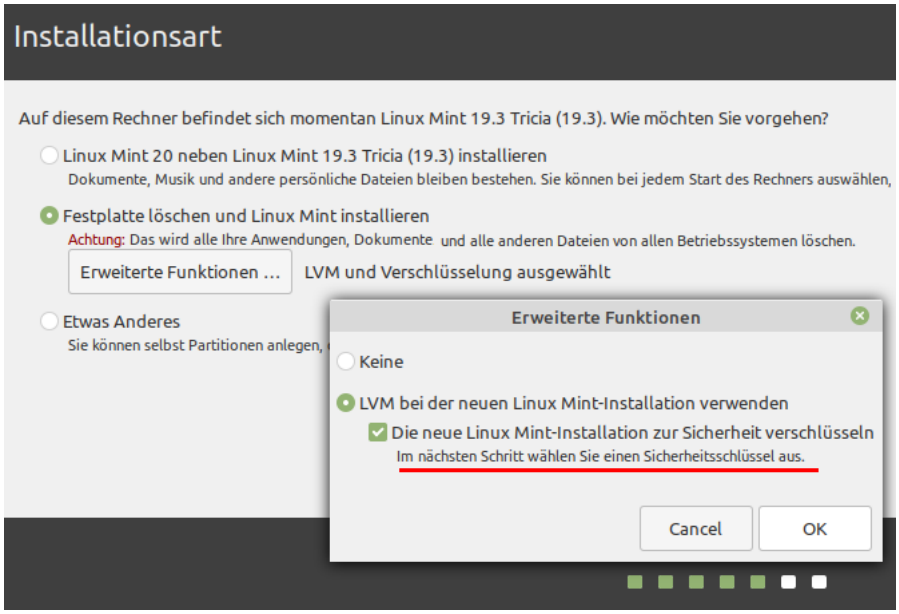


Abbildung 16.4: Linux Mint bei der Installation komplett verschlüsseln

Da man sich bei einem persönlichen Computer durch Eingabe der Passphrase beim Booten schon ausreichend authentifiziert hat, kann man auf eine zweite Eingabe eines Passwort beim Login Bildschirm verzichten und den automatischen Login für den Standardnutzer aktivieren. Dieses Verhalten kann man entweder bei der Installation auswählen oder nachträglich für den Login Manager konfigurieren. Passende Hinweise zur jeweiligen Distribution liefert jede Suchmaschine.

BIOS Einstellungen

Hier ist ein Beispiel für einen *Evil Maid Attack*: Die Zielperson lässt den vollständig verschlüsselten Linux-Laptop unbeaufsichtigt im Hotel o. Ä. liegen. Die böse Maid kommt mit einem USB-Stick, bootet den Laptop mit dem Stick und installiert einen modifizierten Kernel in der unverschlüsselten Boot-Partition oder flasht ein bösartiges BIOS, welches die Sicherheit der Festplattenverschlüsslung komplett aushebeln kann.

Deshalb gehören folgende BIOS Einstellungen zum Sicherheitskonzept dazu:

1. Bootreihenfolge festlegen (immer die Festplatte zuerst).
2. Administrator- bzw. Supervisor-Passwort setzen. Dieses Passwort wird abgefragt, wenn man die BIOS-Einstellungen ändern oder von einem USB-Stick booten möchte.

   Da man dieses Passwort nur selten braucht, sollte man es sicher speichern. Wenn man es nicht mehr findet, kann man nie mehr von einem USB-Stick booten!

   (Ich bin der Meinung, dass man das gleiche Passwort wie für die Festplattenverschlüsselung nehmen könnte, das man sich gut merken kann, da man es fast jeden Tag beim Booten des Rechners eingibt, weil es gegen den gleichen Angreifer schützen soll. Es gibt aber auch die Meinung, dass ein anderes, eigenes Passwort sinnvoll ist.)
3. Tamper Protection aktivieren (wenn vorhanden). Die Tamper Protection kann nur aktiviert werden, wenn ein Supervisor-Passwort gesetzt wurde. Sie warnt, wenn das Gehäuse eines Laptops geöffnet wurde. Die Warnung muss im BIOS zurückgesetzt werden, bevor man

weiterarbeiten kann. (Bei rabiater Behandlung des Laptops kann es auch zu Fehlalarmen kommen.)

Um die BIOS-Einstellungen zu öffnen, muss man beim Start des Rechners je nach Hersteller die Taste F1, F2, ESC oder ENTER gedrückt halten.

16.6.2 Für Genießer in der Konsole mit cryptsetup

Mit mit dem Tool *cryptsetup* können alle Optionen von dm-crypt/LUKS ausgereizt werden, wenn man Spaß an einem Full-Text-Adventure auf der Linux-Konsole hat.

Alle folgenden Schritte sind als *Root* auszuführen. Zum Aufwärmen soll zuerst die Partition auf einem USB-Stick */dev/sdb1* verschlüsselt werden. Debian und Ubuntu enthalten das Skript luksformat, dass alle Aufgaben erledigt.

```
# luksformat -t ext4 /dev/sdb1
```

Das ist alles. Der Vorgang dauert ein wenig und es wird drei Mal die Passphrase abgefragt. Ein Keyfile kann dieses Script nicht nutzen!

Am Beispiel einer verschlüsselten Containerdatei werden die einzelnen Schritte beschrieben, welche das Script *luksformat* aufruft. Soll eine Partition (Festplatte oder USB-Stick) verschlüsselt werden, entfallen die Schritte 1 und 8. Das als Beispiel genutzte Device */dev/loop5* ist durch die Partition zu ersetzen, beispielsweise */dev/hda5* oder */dev/sdb1*.

1. Zuerst ist eine leere Imagedatei zu erstellen. Im Beispiel wird es unter dem Dateinamen *geheim.luks* im aktuellen Verzeichnis erstellt. Der Parameter *count* legt die Größe in MByte fest. Anschließend ist das Image als Loop-Device einzubinden. Das Kommando *losetup -f* ermittelt das nächste freie Loop-Device (Ergebnis: *loop0*).

   ```
   # dd if=/dev/zero of=geheim.luks bs=1M count=100
   # losetup -f
   /dev/loop0
   # losetup /dev/loop0 geheim.luks
   ```

2. Die ersten 2 MByte sind mit Zufallswerten zu füllen. Das Füllen der gesamten Datei würde sehr lange dauern und ist nicht nötig:

   ```
   # dd if=/dev/urandom of=/dev/loop0 bs=1M count=2
   ```

3. Anschließend erfolgt die LUKS-Formatierung mit der Festlegung der Verschlüsselung. Moderne Linux-Distributionen wie Fedora 36 verwenden LUKS2 inzwischen standardmäßig, es müsste also nicht angegeben werden. Die Option -y veranlasst eine doppelte Abfrage des Passwortes, das *keyfile* ist optional:

   ```
   # cryptsetup luksFormat --type luks2 /dev/loop0 [keyfile]
   ```

4. Das verschlüsselte Device wird dem Device-Mapper unterstellt. Dabei wird das zuvor eingegebene Passwort abgefragt. Das Keyfile ist nur anzugeben, wenn es auch im vorherigen Schritt verwendet wurde. Der <name> kann frei gewählt werden. Unter /dev/mapper/<name> wird später auf den verschlüsselten Container zugegriffen:

```
# cryptsetup open --type luks /dev/loop0 <name> [ keyfile ]
```

5. Wer paranoid ist, kann das verschlüsselte Volume mit Zufallszahlen füllen. Der Vorgang kann in Abhängigkeit von der Größe der Containerdatei sehr lange dauern:

```
# dd if=/dev/urandom of=/dev/mapper/<name>
```

6. Ein Dateisystem wird auf dem Volume angelegt:

```
# mkfs.ext4 /dev/mapper/<name>
```

7. Das Volume ist nun vorbereitet und wird wieder geschlossen:

```
# cryptsetup close <name>
```

8. Die Containerdatei wird ausgehängt:

```
# losetup -d /dev/loop0
```

Verschlüsselte Container öffnen/schließen

Um eine verschlüsselte Partition auf einem USB-Stick auf der Kommandozeile zu öffnen, sind zwei Schritte als *root* nötig:

1. Im ersten Schritt wird das verschlüsselte Device dem Device-Mapper unterstellt. Der *name* kann frei gewählt werden. Zusätzlich kann man ein Keyfile nutzen.

```
> sudo cryptsetup open --type luks /dev/sdc1 <name> [keyfile]
Enter LUKS passphrase:
```

2. Danach kann es mit *mount* in das Dateisystem eingehängt werden, z. B. nach /mnt.

```
> sudo mount /dev/mapper/<name> /mnt
```

Das Schließen des Containers erfolgt in umgekehrter Reihenfolge. Dabei werden alle Keys für den Zugriff auf den Container im Kernel sicher gelöscht (wipe).

```
> sudo umount /mnt
> sudo cryptsetup close <name>
```

Das Öffnen einer Containerdatei auf der Kommandozeile erfordert drei Schritte als *root*. Als erstes ist die verschlüsselte Imagedatei als Loop-Device einzuhängen. Das Loop-Device kann dann wie eine verschlüsselte Partition behandelt werden.

```
> sudo losetup /dev/loop0 geheim.luks
> sudo cryptsetup open --type luks /dev/loop0 <name> [keyfile]
Enter LUKS passphrase:
> sudo mount /dev/mapper/<name> /mnt
```

Das Schließen des Containers erfolgt in umgekehrter Reihenfolge.

```
> sudo umount /mnt
> sudo cryptsetup close <name>
> sudo losetup -d /dev/loop0
```

Alte LUKS-Container modernisieren

Die Kryptografie entwickelt sich weiter und neue Verfahren werden state-of-the-art. Wenn man sich vor Jahren einen Datenträger mit dem damals üblichen LUKS-Format und der damals üblichen Krypto erstellt hat, hat man evtl. den Wunsch, auf aktuellere Kryptoalgorithmen zu wechseln. Ein älterer LUKS1-Container könnte folgende Cipher verwenden:

```
> cryptsetup luksDump /dev/sdb1
LUKS header information for /dev/sdb1

Version:     1
Cipher name: aes
Cipher mode: xts-plain64
Hash spec:   sha256
```

Diesen LUKS1-Container kann man in das LUKS2-Format konvertieren und für alle Passwortslots die Schlüsselableitungsfunktion auf Argon2id umstellen. Das macht es professionellen Angreifern mit Tools wie Elcomsoft Passwort Recovery unmöglich, die GPU-Power von Grafikkarten für Brute-Force-Angriffe auf die Passwörter zu nutzen:

```
> sudo cryptsetup convert --type luks2 /dev/sdb1
> sudo cryptsetup luksConvertKey --pbkdf argon2id /dev/sda1
```

Wenn der Container noch älter ist, könnte es sein, dass AES-CBC verwendet wurde:

```
> cryptsetup luksDump /dev/sdc1
LUKS header information for /dev/sdc1

Version:     1
Cipher name: aes
Cipher mode: cbc-essiv:sha256
Hash spec:   sha1
```

Dann könnte man auch den Datenbereich mit AES256-XTS neu verschlüsseln:

```
> sudo cryptsetup-reencrypt /dev/sdc1
```

Die Neuverschlüsselung dauert sehr lange und darf auf keinen Fall unterbrochen werden!

Veracrypt-Container

Das Tool *cryptsetup* kann auch Truecrypt- und Veracrypt-Container öffnen. Auf einem aktuellen Linux-System muss man also keine zusätzliche Software installieren, wenn man gelegentlich Truecrypt/Veracrypt-Container öffnen möchte. Eine Truecrypt-verschlüsselte Partition auf dem USB-Stick öffnet man in zwei Schritten:

```
> sudo cryptsetup open --type tcrypt [Optionen] /dev/sdc1 <name>
Enter passphrase:
> sudo mount /dev/mapper/<name> /mnt
```

Als [Optionen] können zusätzlich folgende Parameter angegeben werden:

- - -veracrypt verwendet man für Container im Veracrypt-Format.
- - -key-file kann man mehrfach nutzen, um Schlüsseldateien anzugeben.
- - -tcrypt-hidden öffnet den Hidden-Container im Truecrypt-Volume.
- - -tcrypt-system ist für Systempartitionen mit Boot-Manager zu nutzen.
- - -readonly muss man nicht erklären.

Wenn man eine Containerdatei öffnen möchte, dann ist die Datei zuerst als Loop-Device einzuhängen. Das Loop-Device kann dann wie eine verschlüsselte Partition behandelt werden.

```
> sudo losetup /dev/loop1 geheim.tc
> sudo cryptsetup [Optionen] open --type tcrypt /dev/loop1 <name>
Enter passphrase:
> sudo mount /dev/mapper/<name> /mnt
```

Das Schließen des Containers erfolgt wie oben bei LUKS.

Passwörter verwalten

Mit Root-Rechten ist es möglich, bis zu 7 zusätzliche Passwörter für das Öffnen eines Containers festzulegen oder einzelne Passwörter wieder zu löschen.

Um die Passwörter einer verschlüsselten Imagedatei namens *geheim.img* zu verwalten, ist die Datei zuerst als Loop-Device einzuhängen, beispielsweise als */dev/loop5*. Dieser Schritt entfällt für verschlüsselte Partitionen:

```
# losetup /dev/loop5 geheim.luks
```

Das Hinzufügen eines Passwortes und damit eines neuen Keyslots erfolgt mit folgendem Kommando, wobei als <device> beispielsweise */dev/loop5* für die eingebundene Imagedatei oder */dev/sda5* für eine Festplattenpartition anzugeben ist. Das Keyfile ist optional. Mit der Option –key-slot wählt man einen bestimmten Slot von 0 bis 7 aus.

```
# cryptsetup --key-slot <slot>  luksAddKey <device> [ keyfile ]
```

Ein Keyslot und das zugehörige Passwort können mit folgendem Kommando wieder entfernt werden:

```
# cryptsetup luksKillSlot <device> <slot>
```

Als <slot> ist die Nummer des Keyslots anzugeben, also eine Zahl von 0 bis 7. Deshalb ist es nötig, sich zu merken, welches Passwort auf welchen Keyslot gelegt wurde. Eine Übersicht, welche Keyslots belegt und welche noch frei sind, liefert *luksDump*:

```
# cryptsetup luksDump <device>
LUKS header information for <device>
...
```

16.6.3 Hardware-Token verwenden (FIDO2, Nitrokeys, Yubikeys)

Die Passphrase ist der schwächste Punkt bei der Verwendung moderner Verfahren zur Verschlüsselung von Datenträgern, insbesondere wenn man im täglichen Gebrauch einfach zu merkende Passphrasen geringer Komplexität bevorzugt.

Im Folgenden werden einige Möglichkeiten vorgestellt, die Sicherheit der Verschlüsselung durch Verwendung von Hardware-Token (Nitrokey, Yubikey, USB-Stick) zu verbessern. Bei allen Varianten ist folgendes Grundkonzept empfehlenswert:

1. Es wird ein verschlüsselter Container erstellt (Festplattenpartition, USB-Stick). Dabei wird eine echt knackige und hochkomplexe Passphrase verwendet, die bei einem Angriff von hochpotenten Hackern mehrere Jahrzehnte standhalten würde.

   Diese Passphrase benötigt man zum Hinzufügen von Hardware-Token oder zum Entfernen von verlorenen Token. Sie kann als Backup zum Öffnen des Containers dienen, wenn das/die Hardware-Token verloren gehen, und könnte off-site in einem Tresor hinterlegt werden.

2. Wenn man der eigenen Kreativität bei der Suche nach einer Passphrase nicht vertraut, kann man einen automatisch generierten Recovery-Key ausrollen lassen:

   ```
   > sudo systemd-cryptenroll --recovery-key <device>
   Please enter current passphrase for disk <device> ******************
   A secret recovery key has been generated for this volume:

   gbdncrvt-cfhkkghh-vfibidfe-hdhhidjk-jbbjcttb-ukfrglic-jkicnirg-tbtktcgh

   Please save this secret recovery key at a secure location.
   ```

   Dann kann man die beim Erstellen des Containers gewählte Passphrase löschen:

   ```
   # cryptsetup luksKillSlot <device> 0
   ```

3. Dann kann man ein oder mehrere Keyslots von LUKS mit Hardware-Token vorbereiten und in der täglichen Arbeit nutzen. (Evtl. sind kleine Scripte hilfreich.)

Variante A: LUKS2-Container mit FIDO2-Security-Token öffnen

FIDO2-Security-Token wurden für den sicheren, passwortlosen Login entwickelt, um die unsicheren Username-Passwort-Kombinationen zu ersetzen.

Moderne Linux-Distributionen mit systemd-Version 2.48+ können diese FIDO2-Token auch zum passwortlosen Entsperren von LUKS2-Containern verwenden, wenn die Token die HMAC-Secret-Erweiterung unterstützen (z. B. Nitrokey FIDO2, Yubikey ab Version 5).

1. Bei einem nagelneuen FIDO2-Token muss man zuerst eine PIN für die Authentifizierung konfigurieren, damit man eine echte Zwei-Faktor-Authentifizierung konfigurieren kann.

   Die PIN sollte nach aktuellen Empfehlungen von BSI und NIST mindestens 6-stellig sein.

   Mäuschenschubser könnten dafür den Browser Google Chrome (oder Chromium) nehmen. In den Einstellungen unter *Datenschutz & Sicherheit → Sicherheit → Sicherheitsschlüssel verwalten* kann man die PIN für FIDO2-Token konfigurieren.

   Für Linuxer gibt es die FIDO2 Tools, die man mit dem bevorzugten Paketmanager installiert:

```
Ubuntu: > sudo apt install fido2-tools
Fedora: > sudo dnf install fido2-tools
```

Mit folgendem Kommando kann man ein PIN für ein neues FIDO2 Token setzen:

```
> fido2-token -S /dev/hidrawX
```

Mit folgendem Kommando kann man die PIN später bei Bedarf ändern:

```
> fido2-token -C /dev/hidrawX
```

(Das X ist durch die Nummer für das FIDO2 Token zu ersetzen, in der Regel ist es 1.)

2. Im ersten Schritt erstellt man den LUKS2(!)-Container (verschlüsselten USB-Stick, Partition oder Containerdatei) und schützt ihn mit einer knackigen Passphrase:

   ```
   > sudo cryptsetup luksFormat --type luks2 <device>
   ```

   Container im älteren LUKS1-Format können nicht mit FIDO2-Token geöffnet werden. Man könnte versuchen, einen LUKS1-Container nach LUKS2 zu konvertieren:

   ```
   > sudo cryptsetup convert <device> --type luks2
   ```

3. Im nächsten Schritt wird ein FIDO2-Security-Token zum Öffnen hinzugefügt. Das Token muss dabei eingesteckt sein und es darf nur ein FIDO-Token gesteckt sein:

   ```
   > sudo systemd-cryptenroll [Optionen] --fido2-device=auto <device>
   ```

   Mehrere FIDO2-Token fügt man entweder nacheinander hinzu oder man steckt alle verfügbaren Token gleichzeitig ein und verwendet folgendes Kommando, um alle hinzuzufügen:

   ```
   > sudo systemd-cryptenroll [Optionen] --fido2-device=list <device>
   ```

   Mit folgenden Optionen kann man festlegen, welche Sicherheitsfeatures aktiviert werden:

   - Entsperren des FIDO2 Token mit PIN Eingabe erforderlich oder nicht erfoderlich:

     ```
     --fido2-with-client-pin=yes|no (Default: yes)
     ```

   - Drücken der Präsenstaste am FIDO2 Token erforderlich oder nicht nötig:

     ```
     --fido2-with-user-presence=yes|no (Default: yes)
     ```

   - Eingabe eines zusätzlichen Passwortes nötig (nicht von allen Token unterstützt):

     ```
     --fido2-with-user-verification=yes|no (Default: no)
     ```

4. Beim Öffnen des Containers wird man standardmäßig weiterhin nach der Passphrase gefragt. Die Nuzung des FIDO2-Token kann man mit folgendem Kommando erzwingen:

   ```
   > sudo cryptsetup open --type luks --token-only <device> <name>
   ```

   oder auch möglich:

```
> sudo /usr/lib/systemd/systemd-cryptsetup attach <name> <device> -
↪ fido2-device=auto
```

Den Befehl könnte man in einem kleinen Script verwenden. Wenn man eine externe Festplatte oder einen verschlüsselten USB-Stick mit einem FIDO2-Stick per Script öffnen will, sollte man das Gerät mit UUID angeben, um unabhängig von der Reihenfolge beim Einstecken zu sein:

```
> sudo cryptsetup open --type luks --token-only UUID=<uuid> <name>
```

Die <uuid> kann mit dem Befehl *blkid* ermittelt werden.

5. Wenn man eine im Laptop oder PC fest eingebaute verschlüsselte Festplatte standardmäßig mit einem FIDO2-Token öffnen möchte, kann man in der Datei /etc/crypttab für das Device in der vierten Spalte die Option *fido2-device=auto* einfügen:

```
<Name> <Gerät> - luks,fido2-device=auto...
```

Wenn es sich dabei um die verschlüsselte Root-Partition handelt, muss abschließend noch das Bootimage neu gebaut werden:

```
> sudo update-initramfs -u
```

Zukünftig muss man keine hochkomplizierte Passphrase mehr eintippen sondern steckt beim Booten einfach das FIDO2-Token rein, das man nicht verlieren sollte.

6. Wenn ein Token verloren geht, muss man es natürlich entfernen. Das folgende Kommando löscht alle FIDO2-Token. die für den LUKS2-Container autorisiert wurden:

```
> sudo systemd-cryptenroll --wipe-slot=fido2 <device>
```

Die weiterhin gültigen Token kann man danach wieder hinzufügen (3.) oder man kombiniert das Löschen und Hinzufügen, indem man alle weiterhin gültigen FIDO2-Token anschließt und folgenden Befehl eingibt:

```
> sudo systemd-cryptenroll --wipe-slot=fido2 --fido2-device=list
↪ <device>
```

Variante B: LUKS2-Container mit PKCS#11-Token öffnen

Linux-Distributionen mit systemd-Version 2.48+ können PKCS#11-Token zum Entsperren von LUKS2-Containern verwenden, wenn das Token die PIV-Erweiterung unterstützt.

1. Zuerst ist das Token vorzubereiten (RSA-Schlüsselpaar erzeugen, PINs ändern usw.).
2. Im nächsten Schritt erstellt man den LUKS2(!)-Container (USB-Stick, verschlüsselte Partition oder Containerdatei) und schützt ihn mit einer knackigen Passphrase (s. o.).
3. Danach wird der Container einmal mit der knackigen Passphrase geöffnet:

```
> sudo cryptsetup open --type luks <device> <name>
```

4. Im nächsten Schritt wird ein PKCS#11-Token zum Öffnen des Containers hinzugefügt. Das Token muss dabei eingesteckt sein:

   ```
   > sudo systemd-cryptenroll --pkcs11-token-uri=auto <device>
   ```

   Es können entweder mehrere Token nacheinander hinzugefügt werden, oder gleichzeitig mit folgendem Befehl:

   ```
   > sudo systemd-cryptenroll --pkcs11-token-uri=list <device>
   ```

5. Beim Öffnen des Containers wird man weiterhin nach der Passphrase gefragt. Für FIDO2-Token kann man folgendes Kommando verwenden:

   ```
   > sudo cryptsetup open --type luks --token-only <device> <name>
   ```

   oder auch möglich:

   ```
   > sudo /usr/lib/systemd/systemd-cryptsetup attach <name> <device> -
   ↪  pkcs11-uri=auto
   ```

   Den Befehl könnte man in einem kleinen Script verwenden. Wenn man eine externe Festplatte oder einen verschlüsselten USB-Stick mit FIDO2-Stick per Script öffnen will, sollte man das Gerät mit UUID angeben, um unabhängig von der Reihenfolge beim Einstecken zu sein:

   ```
   > sudo cryptsetup open --type luks --token-only UUID=<uuid> <name>
   ```

   Die <uuid> kann mit dem Befehl *blkid* ermittelt werden.

6. Wenn man eine im Laptop oder PC fest eingebaute verschlüsselte Festplatte standardmäßig mit einem FIDO2-Token öffnen möchte, kann man in der Datei /etc/crypttab für das Device in der vierten Spalte die Option*pkcs11-uri=auto* einfügen:

   ```
   <Name> <Gerät> - luks,pkcs11-uri=auto...
   ```

   Wenn es sich dabei um die verschlüsselte Root-Partition handelt, muss abschließend noch das Bootimage neu gebaut werden:

   ```
   > sudo update-initramfs -u
   ```

   Zukünftig muss man keine komplizierte Passphrase mehr eintippen sondern steckt beim Booten einfach das PKCS#11-Token rein, das man nicht verlieren sollte.

7. Wenn ein Token verloren geht, muss man es natürlich entfernen. Das folgende Kommando löscht alle PKCS#11-Token, die für den LUKS2-Container autorisiert wurden:

   ```
   > sudo systemd-cryptenroll --wipe-slot=pkcs11 <device>
   ```

   Die weiterhin gültigen Token kann man danach wieder hinzufügen. Das Löschen und Hinzufügen der weiterhin gültigen PKCS#11-Token kann auch hier mit einem Kommando erfolgen. Die gültigen Token müssen dabei angeschlossen sein:

   ```
   > sudo systemd-cryptenroll --wipe-slot=pkcs11 --pkcs11-token-uri=list
   ↪  <device>
   ```

Variante C: LUKS Container mit GnuPG Smartcard öffnen

GnuPG-Smartcards im Format von USB-Sticks gibt es bei Nitrokey, Yubikey oder GnuK. Die Idee ist einfach erklärt: Es wird das Keyfile für das Öffnen des LUKS-Containers verwendet, das mit dem OpenPGP-Key des Nitrokey verschlüsselt wurde. Zum Öffnen des Containers wird das Keyfile mit gpg2 entschlüsselt und via Pipe an cryptsetup übergeben. Eine kurze Anleitung, die sich auf das Wesentliche beschränkt:

1. Ein frischer Nitrokey ist erst mal einzurichten (Schlüssel erzeugen, PIN ändern usw.)

2. Da die folgenden Operationen als *root* durchgeführt werden, ist der OpenPGP-Schlüssel des Nitrokey zu exportieren und im Schlüsselring von *root* zu importieren. Außerdem ist ein re-bind des privaten Schlüssels der Nitrokey-Smartcard anzustoßen:

   ```
   > gpg2 --export "User-ID" > /tmp/luks-pgp-key.pgp
   > sudo gpg2 --import /tmp/luks-pgp-key.pgp
   > sudo gpg2 --card-status
   > rm /tmp/luks-pgp-key.pgp
   ```

3. Es wird ein Keyfile mit Zufallszahlen erzeugt (z. B. /root/.gnupg/key.bin):

   ```
   > sudo dd if=/dev/urandom of=/root/.gnupg/key.bin bs=512 count=8
   ```

4. Das Keyfile wird als Schlüssel für den Container in nächsten freien Keyslot eingefügt. Es wird dabei eine gültige Passphrase für das Öffnen des Containers abgefragt:

   ```
   > sudo cryptsetup luksAddKey <device> /root/.gnupg/key.bin
   ```

5. Das Keyfile wird mit GnuPG verschlüsselt und das Orginal sicher gelöscht:

   ```
   > sudo gpg2 --encrypt --recipient /root/.gnupg/key.bin
   > sudo shred -u /root/.gnupg/key.bin
   ```

6. Zum Öffnen des Containers werden folgende Kommandos verwendet, die man sich als Script ablegen kann. <device> und <mount-point> sind anzupassen. <name> kann beliebig gewählt werden und dient nur zur Identifikation im Devicemapper:

   ```
   > sudo su
   # gpg2 --decrypt /root/.gnupg/key.bin.gpg | cryptsetup open
   ↪  --key-file=- <device> <name>
   # mount /dev/mapper/<name> <mount-point>
   # exit
   ```

   Mit KDialog oder Zenity könnte man das Script grafisch aufpeppen und einen Starter auf den Desktop legen. Kreativität und Spieltrieb sind dabei keine Grenzen gesetzt. Wenn man das grafisch aufgepeppte Script ohne ein Terminal im Hintergrund nutzen möchte, dann muss man die Option *–no-tty* bei dem gpg2-Kommando hinzufügen:

   ```
   > gpg2 --no-tty --decrypt /root/.gnupg/key.bin.gpg | cryptsetup ...
   ```

Full Disc Encryption: Wenn man bei der Installation das System vollständig verschlüsselt hat, kann man den Nitrokey auch zum Öffnen des Root-Containers beim Booten verwenden.

Die Nitrokey GmbH stellt dafür eine ausführliche Anleitung für Ubuntu und Debian bereit.

Wichtig ist, dass man sein System schon bei der Installation passend vorbereitet und nicht die automatische Partitionierung der Festplatte nutzt! Es darf nur eine unverschlüsselte Bootpartition und eine verschlüsselte Root-Partition erstellt werden. Anderenfalls kommt es zu Fehlern.

Variante D: LUKS Container mit Yubikey öffnen

Die Firma Yubico bietet mit *yubikey-luks* eine Software zur Nutzung ihrer Yubikeys als Schlüssel für einen LUKS-Container, die mit einem Challenge-Response-Verfahren arbeitet.

Die Passphrase wird als Challenge an den Yubikey gesendet, der mit kryptografischem Voodoo einen Response ableitet, der als Schlüssel zum Öffnen des Containers dient. Die Passphrase (Challenge) kann dabei einfach und leicht merkbar sein, da der Yubikey als zweiter Faktor für das Öffnen des Containers nötig ist und ein starkes Passwort ableitet.

1. Die Software kann mit dem bevorzugten Paketmanager installiert werden:

   ```
   > sudo apt install yubikey-luks yubikey-personalization
   ```

2. Der zweite Passwort-Slot des Yubikey wird für Challenge-Response vorbereitet:

   ```
   > ykpersonalize -2 -ochal-resp -ochal-hmac -ohmac-lt64
   ↪  -oserial-api-visible
   ```

3. Das Challenge-Response-Passwort wird in einen freien Keyslot des LUKS Containers eingetragen. Es gibt ein Script, dass die Aufgabe übernimmt. Dabei wird zweimal das neue Challenge-Passwort für den Yubikey sowie eine gültige Passphrase für das Öffnen des LUKS-Containers abgefragt:

   ```
   > sudo yubikey-luks-enroll -d <device> -s <key-slot>
   ```

   Falls man den Überblick verloren hat, welche Keyslots im LUKS-Container noch frei sind, kann man sich die Belegung mit folgendem Kommando anzeigen lassen:

   ```
   > sudo cryptsetup luksDump
   LUKS header information for <device>
   ...
   Key Slot 0: ENABLED
   Key Slot 1: DISABLED
   ...
   Key Slot 7: DISABLED
   ```

4. Zukünftig kann man zum Öffnen des Containers den Yubikey anschließen und muss nur das einfache Challenge-Passwort in der Passwortabfrage eingeben. Andere Methoden zum Öffnen des Containers stehen weiterhin zur Verfügung.

Full Disc Encryption: Wenn man bei der Installation das System vollständig verschlüsselt hat, kann man den Yubikey auch zum Öffnen des Root-Containers beim Booten verwenden.

Dafür ist die Partition mit dem verschlüsselten Root-Container zu ermitteln und der Yubikey als Hardware-Token zum Öffnen hinzuzufügen, wie oben beschrieben. Die folgenden Schritte funktionieren auf einem Debian-System und davon abgeleiteten Derivaten:

1. Zuerst das BACKUP der Daten aktualisieren, falls man etwas kaputtspielt!
2. Am einfachsten identifiziert man den Root-Container mit einem Blick in die Datei */etc/crypttab*. In der ersten Zeile das zweite Element ist die Kennung für das <device>, welches für das Kommando *yubikey-luks-enroll* zu verwenden ist.
3. Danach ist die Datei /etc/crypttab anzupassen. In der (ersten) Zeile für den Root-Container ist das Schlüsselwort *luks* mit dem vollständigen Pfad zu *ykluks-keyscript* zu ergänzen, also *. . . luks,keyscript=/usr/share/yubikey-luks/ykluks-keyscript. . .*

   Also: aus der Zeile. . .

   ```
   cryptroot UUID=xxxx ... luks
   ```

   . . . wird diese Zeile:

   ```
   cryptroot UUID=xxxx ...
   ↪  luks,keyscript=/usr/share/yubikey-luks/ykluks-keyscript
   ```

   Alle anderen Parameter bleiben so erhalten, wie bei der Installation konfiguriert.
4. Danach ist noch das Bootimage neu zu bauen mit:

   ```
   > sudo update-initramfs -u
   ```
5. Wenn man den Rechner neu bootet, kann man statt der bisherigen (hoffentlich starken und komplexen) Passphrase, die man bei der Installation vergeben hat, auch den Yubikey anschließen und das einfachere Challenge-Passwort eingeben.

16.6.4 LUKS-Nuke – hinterhältige Datenzerstörung

LUKS-Nuke bietet die Möglichkeit, eine vollständig verschlüsselte Installation von Debian-basierten Distributionen auf die zukünftige Entsorgung der Festplatte vorzubereiten.

Einmal eingerichtet, ist die Handhabung einfach: Beim Booten des Systems gibt man statt der Passphrase zum Öffnen des Systemcontainers die vorkonfigurierte Nuke-Passphrase ein und einige Millisekunden später ist nur noch unbrauchbarer Datenmüll auf der Festplatte.

(Einsatzmöglichkeiten für ein solches Feature sind der Fantasie des Lesers überlassen.)

LUKS-Nuke wurde für Kali Linux entwickelt, einer Linux-Distribution für *Offensive Security* (Pentesting). In dieser Distribution installiert man das Paket aus den Repositorys:

```
> sudo apt install cryptsetup-nuke-password
```

Im zweiten Schritt wird die Nuke-Passphrase konfiguriert, die man zwei Mal eingeben muss, und im Hintergrund werden automatisch alle notwendigen Systemanpassungen eingerichtet:

```
> sudo dpkg-reconfigure cryptsetup-nuke-password
```

LUKS-Nuke löscht bei Eingabe der Nuke-Passphrase statt der korrekten Passphrase zum Öffnen des Systemcontainers alle Keyslots im LUKS-Header, so das die Daten nicht mehr entschlüsselt werden können. Wenn man ein Backup des LUKS-Headers off-site speichert, kann man mit einer Linux-Live-DVD die Daten wieder lesbar machen.

1. Ein Backup des LUKS-Headers erstellt man mit folgendem Kommando:

   ```
   > sudo cryptsetup luksHeaderBackup --header-backup-file luksheader.bck
   ↪  <device>
   ```

   Bei Kali Linux ist das <device> üblicherweise /dev/sda5, bei anderen Distributionen ist es evtl. anzupassen. Das Backup kann man verschlüsseln und off-site ablegen.

2. Für ein Restore des alten LUKS-Headers bootet man eine Linux-Live-DVD und stellt den Header mit den Schlüsseln mit folgendem Kommando wieder her:

   ```
   > sudo cryptsetup luksHeaderRestore <device> --header-backup-file
   ↪  luksheader.bck
   ```

Da Kali Linux auf Debian basiert, kann man das Paket *cryptsetup-nuke-passphrase* auch auf anderen Linux-Distributionen installieren, die von Debian abgeleitet sind. Dafür könnte man die Kali-Live-DVD starten und das Paket mit folgendem Kommando herunterladen:

```
> apt download cryptsetup-nuke-password
```

Anschließend transferiert man das Paket auf das eigene System und installiert es mit:

```
> sudo dpkg -i cryptsetup-nuke-pass*.deb
```

Dann die Konfiguration der Nuke-Passphrase und Anpassung des Systems – FERTIG:

```
> sudo dpkg-reconfigure cryptsetup-nuke-password
```

(Getestet mit Debian 10 - für alle anderen Distributionen keine Gewährleistung.)

16.7 zuluCrypt für Linux

zuluCrypt ist eine 100 % kompatible Open-Source-Alternative zu Veracrypt für Linux-Nutzer und kann in aktuellen Linux-Distributionen mit den üblichen Tools zur Paketverwaltung installiert werden.

Die Verwendung von zuluCrypt statt cryptsetup ist empfehlenswert, wenn man öfters mit Containerdateien arbeitet, wenn man Features für hohe Sicherheitsanforderungen verwendet (Passphrase + Keyfile als Credentials oder Hidden Volumes) oder Datenträger verschlüsseln möchte, die bei Bedarf auch unter Windows geöffnet werden können.

Neben Truecrypt und Veracrypt beherrscht das Tool auch dm-crypt/LUKS-Verschlüsselung und unterstützt alle Features im GUI und nicht nur auf der Kommandozeile.

Als kleine Besonderheit kann zuluCrypt verschlüsselte Container in einer Videodatei verstecken (Steganografie). Dabei wird dm-crypt zur Verschlüsselung verwendet.

Das zuluCrypt-Paket besteht aus vier Komponenten:

- *zuluCrypt-gui* ist das universelle GUI-Tool zum Erstellen von verschlüsselten Containerdateien und Datenträgern sowie zum Öffnen und Schließen der Container.
- *zuluCrypt-cli* ist ein Tool für die Kommandozeile mit gleichem Funktionsumfang.
- *zuluMount-gui* dient zum Öffnen und Schließen der Container.
- *zuluMount-cli* macht das Gleiche auf der Kommandozeile.

In der Regel wird man wahrscheinlich mit mit dem zuluCrypt-GUI arbeiten. Er verwaltet einerseits die geöffneten Container in einem übersichtlichen Hauptfenster und kann anderseits auch Datenträger verschlüsseln und verschlüsselte Containerdateien erstellen. Dabei werden alle Features von Truecrypt, Veracrypt und dm-crypt/LUKS unterstützt, inklusive Hidden-Volumes (Veracrypt) und Passwort + Keyfiles als Credentials.

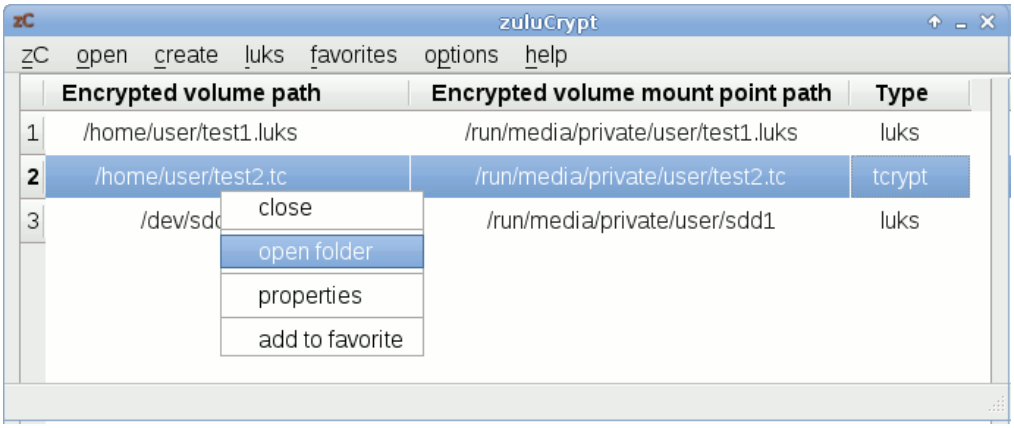


Abbildung 16.5: Hauptfenster von zuluCrypt

16.8 Backups verschlüsseln

Es ist beruhigend, wenn alles Nötige für eine komplette Neuinstallation des Rechners zur Verfügung steht: Betriebssystem, Software und ein Backup der persönlichen Daten. Betriebssystem und Software hat man als Linux-Nutzer mit einer Installations-CD/DVD der genutzten Distribution und evtl. einer zweiten CD für Download-Stuff schnell beisammen. Für WINDOWS wächst in kurzer Zeit eine umfangreiche Sammlung von Software.

Die kleine Ideensammlung für das Backup persönlicher Daten erhebt keinen Anspruch auf Vollständigkeit. Grundsätzlich sollten diese Daten verschlüsselt werden. Als Schlüssel für den Zugriff sollte eine gut merkbare Passphrase genutzt werden. Keyfiles oder OpenPGP-Schlüssel könnten bei einem Crash verloren gehen.

16.8.1 Schnell mal auf eine externe SSD-Festplatte

Die persönlichen Daten oder einzelne Verzeichnisse mit häufig geänderten Dateien könnte man regelmäßig mit einer Kopie auf einem verschlüsselten, externen Datenträger synchronisieren. Inzwischen gibt es preiswerte USB-SSD-Festpatten mit beachtlicher Kapazität. Aufgrund der einfachen Verwendung sind sie für Backups im privaten Bereich gut geeignet.

Die Wiederherstellung ist einfach, da die Daten als 1:1 Kopie auf dem Backupmedium liegen.

Das Backup-Medium sollte man mit Veracrypt oder dm-crypt/LUKS komplett verschlüsseln. Die vollständige Verschlüsselung verhindert eine Manipulation des Datenträgers. Der Verfassungsschutz demonstrierte auf der CeBIT 2007, dass sich mit manipulierten Sticks Trojaner einschleusen lassen. Die vollständige Verschlüsselung des Backup-Mediums macht es überflüssig, sich um eine zusätzliche Verschlüsselung der Daten beim Backup zu kümmern. Man kann die Daten nach dem Öffnen des Backup-Containers einfach synchronisieren.

Die von verschiedenen Herstellern angebotenen Verschlüsselungen sind oft unsicher. USB-Datentresore mit Fingerabdruckscanner lassen sich einfach öffnen[10]. Einige USB-Sticks mit Verschlüsselung verwenden zwar starke Algorithmen (in der Regel AES256), legen aber einen zweiten Schlüssel zur Sicherheit auf dem Stick ab, der mit geeigneten Tools ausgelesen werden kann und Zugriff auf die Daten ermöglicht. Selbst eine Zertifizierung des NIST ist keine Garantie für saubere Implementierung.[11]

Unison-GTK oder FreeFileSync

Für die Synchronisation der Daten stehen z. B. *Unison-GTK*[12] oder *FreeFileSync*[13] für verschiedene Betriebssysteme (auch WINDOWS) zur Verfügung. Die Programme bieten ein GUI für die Synchronisation von Verzeichnissen. Die Installation ist einfach: Download, Entpacken und Binary starten. Linuxer können das Paket *unison-gtk* bzw. *unison-gui* mit der Paketverwaltung installieren.

Nach dem ersten Start wählt man Quell- und Zielverzeichnis für das Default-Profil. Es ist möglich, mehrere Profile anzulegen. Bei jedem weiteren Start erscheint zuerst ein Dialog zur Auswahl des Profils (Abb. 16.6).

Nach Auswahl des Profils analysiert Unison die Differenzen und zeigt im Hauptfenster an, welche Aktionen das Programm ausführen würde. Ein Klick auf *Go* startet die Synchronisation.

[10] https://heise.de/-270060
[11] https://heise.de/-894962
[12] https://github.com/bcpierce00/unison
[13] https://freefilesync.org

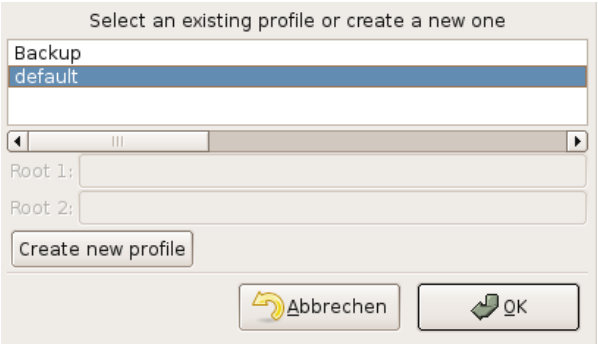


Abbildung 16.6: Profil nach dem Start von Unison-GTK auswählen

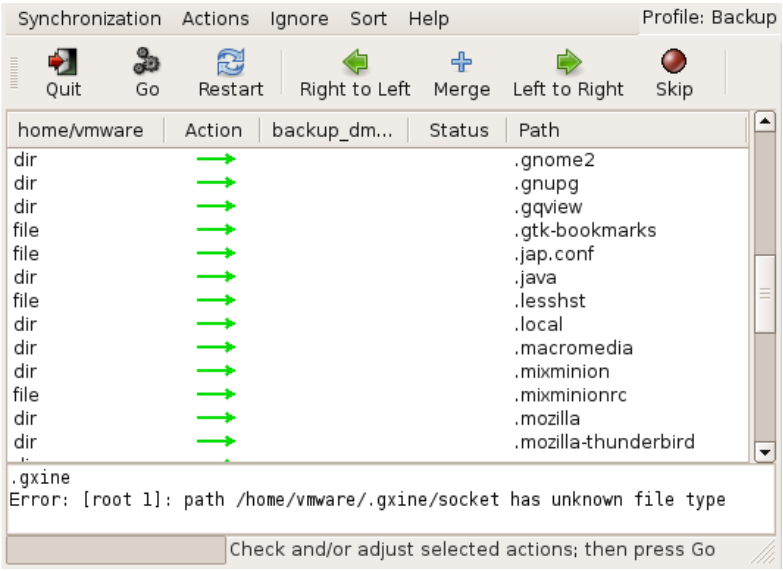


Abbildung 16.7: Hauptfenster von Unison-GTK

Achtung: Unison und FreeFileSync synchronisieren in beide Richtungen und eignen sich damit auch zum Synchronisieren zweier Rechner. Verwendet man einen neuen (leeren) Stick, muss auch ein neues Profil angelegt werden! Es werden sonst alle Daten in den Quellverzeichnissen gelöscht, die im Backup nicht mehr vorhanden sind.

Neben der Möglichkeit, lokale Verzeichnisse zu synchronisieren, können Unison und FreeFileSync auch ein Backup auf einem anderen Rechner via SSH synchronisieren.

rsync

Das Tool *rsync* ist in allen Linux-Distributionen enthalten und insbesondere für Scripte einfach verwendbar. Es synchronisiert die Dateien eines Zielverzeichnisses mit dem Quellverzeichnis und überträgt dabei nur die Änderungen. Ein Beispiel zeigt das Sichern des Standardverzeichnisses *Dokumente* für den aktuellen User:

```
> rsync -av --delete-before --force $HOME/Dokumente /backup_dir/
```

Der Befehl legt im *backup_dir* ein Verzeichnis *Dokumente* an und kopiert alle Daten in dieses Unterverzeichnis. Sollte das Verzeichnis *.thunderbird* im Backup-Verzeichnis bereits vorhanden sein, werden nur die Änderungen übertragen, was wenige Sekunden dauert.

Die Option *–delete* löscht im Original nicht mehr vorhandene Dateien auch in der Sicherungskopie. Weitere Hinweise liefert die Manual-Page von *rsync*.

Eine zweite Variante zum Sichern des gesamten $HOME Verzeichnisses inklusive einiger versteckten Verzeichniss und exklusive eines Verzeichnisses (mp3) mit großen Datenmengen:

```
> rsync -avxSH --delete-before --force --progress
↪ --include=$HOME/.thunderbird --include=$HOME/.mozilla
↪ --exclude=$HOME/mp3 $HOME /backup_dir/
```

Standardmäßig sichert *rsync* keine versteckten Dateien und Verzeichnisse, die mit einem Punkt beginnen. Diese Dateien und Verzeichnisse müssen mit *–include* angegeben werden. Im Beispiel werden die Daten von Thunderbird und Firefox mit gesichert.

Ein Script, welches alle nötigen Verzeichnisse synchronisiert, ist schnell gestrickt. Eine Backupfreundliche Struktur im $HOME-Verzeichnis erleichtert dies zusätzlich.

```
!/usr/bin/sh

rsync -av --delete-before --force $HOME/Dokumente
↪ /run/media/<user>/<Device-ID>/
rsync -av --delete-before --force $HOME/Bilder
↪ /run/media/<user>/<Device-ID>/
rsync -av --delete-before --force $HOME/.thunderbird
↪ /run/media/<user>/<Device-ID>/
rsync -av --delete-before --force $HOME/.mozilla
↪ /run/media/<user>/<Device-ID>/
```

Grsync

Grsync ist ein grafischen Interface für *rsync*. Auch dieses Tool ist in allen Linux/Unix-Distributionen enthalten.

Nach dem Start kann man mit dem Button "+" mehrere Profile für verschiedene, wiederkehrende Aufgaben anlegen. Jedem Profil werden ein Quell- und ein Zielverzeichnis sowie die Parameter für *rsync* zugeordnet. Ein Klick auf die kleine Rakete oben rechts startet die Synchronisation (Abb. 16.8).

16.8.2 Online-Backups in der Cloud

Neben dem Backup auf einem externen Datenträger kann man auch Online-Speicher nutzen. Bei TeamDrive.com, DataStorageUnit.com, ADrive.com, rsync.net u. v. a. m. gibt es Angebote ab 3,- Euro monatlich. Wer einen eigenen (V)Server gemietet hat, kann seine Backups auch dort ablegen. Um die Verschlüsselung der Daten vor dem Upload muss man sich immer selbst kümmern.

Ein Online-Backup ist praktisch, wenn man mit Laptop in ein Land wie die USA reist. Bei der Einreise werden möglicherweise die Daten der Laptops gescannt und auch kopiert. Die EFF.org

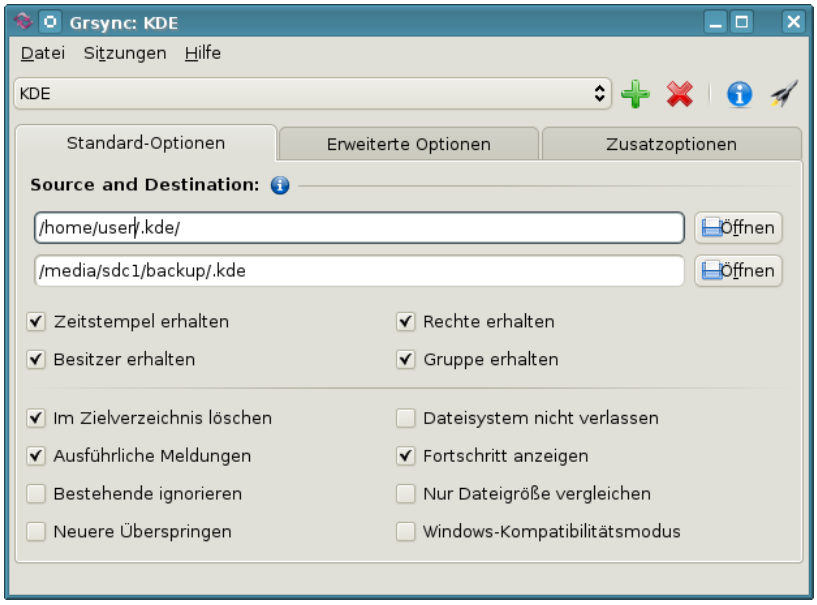


Abbildung 16.8: Hauptfenster von Grsync

empfiehlt, vor der Reise die Festplatte zu „reinigen“[14]. Man könnte ein Online-Backup erstellen und auf dem eigenen Rechner die Daten sicher(!) löschen, also *shred* bzw. *wipe* nutzen. Bei Bedarf holt man sich die Daten wieder auf den Laptop. Vor der Abreise wird das Online-Backup aktualisiert und lokal wieder alles gelöscht.

Mit dem Gesetzentwurf zum Zugriff auf Bestandsdaten der Telekommunikation (BR-Drs. 664/12) vom 24.10.2012 räumt die Bundesregierung den Geheimdiensten und Strafverfolgern die Möglichkeit ein, ohne richterliche Prüfung die Zugangsdaten zum Online-Speicher vom Provider zu verlangen. Um die gespeicherten Daten, die meist aus dem Bereich *privater Lebensführung* stammen, angemessen vor dem Verfassungsschutz zu schützen, ist man auf Selbsthilfe und Verschlüsselung angewiesen.

An ein Online-Backup werden deshalb folgende Anforderungen gestellt:

- Das Backup muss auf dem eigenen Rechner ver- und entschlüsselt werden, um die Vertraulichkeit zu gewährleisten.
- Es sollten nur geänderte Daten übertragen werden, um Zeitbedarf und Traffic auf ein erträgliches Maß zu reduzieren.

duplicity ist ein kleines Backup-Tool für Linux, dass die Daten lokal ver- und entschlüsselt, bevor sie in einen beliebigen Cloud-Speicher hochgeladen werden.

Duplicity für Linux

Duplicity ist ein Backup-Tool für Linux/Unix, speziell für die Nutzung von Online-Speicherplatz. Es bietet transparente Ver- und Entschlüsselung mit OpenPGP und überträgt nur geänderte Daten, um Traffic und Zeitbedarf minimal zu halten.

Die Distributionen stellen i. d. R. alles für die Installation in Repositorys bereit.

[14] https://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t

```
Ubuntu: > sudo aptitude install duplicity
Fedora: > sudo dnf install duplicity
```

Duplicity ist ein Kommandozeilen-Tool. Ein verschlüsseltes Backup schiebt man mit folgendem Kommando auf den Server:

```
> duplicity Verzeichnis Backupaddresse
```

Vom lokalen Verzeichnis *Verz* wird ein Backup erstellt, mit OpenPGP symmetrisch verschlüsselt und in 200MB großen Häppchen unter der Backup Adresse abgelegt. Das erste Backup ist ein Full-Backup und alle weiteren Backups sind inkrementelle Backups. Da ein Restore sehr lange dauern würde, wenn man monatelang nur inkrementelle Backups macht, sollte man regelmäßig (z. B. monatlich) ein Full-Backup einfügen:

```
> duplicity --full-if-older-than=1M Verz Backupadresse
```

Da Datenspeicher nicht unendlich groß sind, muss man alte Backups gelegentlich löschen:

```
> duplicity remove-older-than 3M Backupadresse
```

Die Zeiten kann man in Tagen (D), Wochen (W), Monaten (M) oder Jahren (Y) angegeben.

Das Passwort für die Verschlüsselung wird beim Start des Programms abgefragt, was in automatisiert ablaufenden Backupscripten unpraktisch ist. Dafür ist es besser, einen OpenPGP Schlüssel zu verwenden und mit der Option *–encrypt-key* mit der ID oder Mail-Adresse des OpenPGP-Key. Diese Option kann mehrfach angegeben werden, um mehreren Teilnehmern ein Restore des Backups zu erlauben.

```
> duplicity --encrypt-key="0x12345670" Verzeichnis Backupaddresse
```

Die **Backupadresse** kodiert das Übertragungsprotokoll, den Server und das Verzeichnis auf dem Server. Duplicity kann mit vielen Protokollen umgehen. Backupadressen haben folgenden Aufbau:

- Man kann ein lokales Backupverzeichnis nutzen (z. B. auf einem externen Datenträger):

  ```
  file:///backupverzeichnis
  ```

- Viele Anbieter von Online-Speicherplatz unterstützen *webdav* oder die SSL-verschlüsselte Übertragung mit *webdavs*:

  ```
  webdavs://user[:password]@server.tld/dir
  ```

- Das sftp-Protokoll (ssh) ist vor allem für eigene Server interessant. Loginname und Passwort könnten ebenfalls in der Adresse kodiert werden:

  ```
  ssh://user[:password]@server.tld[:port]/dir
  ```

Für die Automatisierung in Scripten wäre ein SSH-Schlüssel besser geeigent als ein Passwort, den man *ssh-keygen* erstellt und dessen öffentlichen Part man mit *ssh-copy-id* auf das Zielsystem übertragen kann.

- *scp* und *rsync* können ebenfalls für die Übertragung zum Server genutzt werden:

  ```
  scp://user[:password]@server.tld[:port]/dir
  rsync://user[:password]@server.tld[:port]/dir
  ```

  Das Verzeichnis ist bei *rsync* relativ zum Login-Verzeichnis. Um einen absoluten Pfad auf dem Server anzugeben, schreibt man zwei Schrägstriche.

- Amazon S3 Cloud Services werden unterstützt:

  ```
  s3://server/bucket_name[/prefix]
  ```

- Man kann sein IMAP-Postfach für das Backup nutzen, möglichst mit SSL-verschlüsselter Verbindung. Diese Variante ist nicht sehr performant, viele Mail-Provider sehen das nicht gern:

  ```
  imaps://user[:password]@mail.server.tld
  ```

Ein **Restore** erfolgt nur in ein leeres Verzeichnis! Es ist ein neues Verzeichnis zu erstellen. Beim Aufruf zur vollständigen Wiederherstellung des letzten Backups sind Backupadresse und lokales Verzeichnis zu tauschen. Weitere Parameter sind nicht nötig.

```
> mkdir /home/user/restore
> duplicity Backupaddresse /home/user/restore
```

Man kann einzelne Dateien wiederherstellen, wenn man sie versehentlich gelöscht hat:

```
> duplicity --file-to-restore=Path Backupaddresse /home/user/restore
```

Man kann auch einen älteren Zustand wiederherstellen (gesamtes Backup oder einzelne Dateien), bspw. den Zustand aller Daten vor 10 Tagen restaurieren:

```
> duplicity --restore-time 10D Backupaddresse /home/user/restore
```

Weitere Informationen findet man in der Manual-Page von *duplicity*.

Kapitel 17

Daten löschen

Neben der sicheren Aufbewahrung von Daten steht man gelegentlich auch vor dem Problem, Dateien gründlich vom Datenträger putzen zu müssen. Es gibt verschiedene Varianten, Dateien vom Datenträger zu entfernen. Über die Arbeit der einzelnen Varianten sollte Klarheit bestehen, anderenfalls erlebt man evtl. eine böse Überraschung.

17.1 Dateien in den Papierkorb werfen

Unter WINDOWS wird diese Variante als *Datei(en) löschen* bezeichnet, was etwas irreführend ist. Es wird überhaupt nichts beseitigt. Die Dateien werden in ein spezielles Verzeichnis verschoben. Sie können jederzeit wiederhergestellt werden. Das ist kein Bug, sondern ein Feature.

Auch beim Löschen der Dateien in dem speziellen Müll-Verzeichnis werden keine Inhalte beseitigt. Lediglich die von den Dateien belegten Bereiche auf dem Datenträger werden als „frei“ gekennzeichnet. Falls sie nicht zufällig überschrieben werden, kann ein mittelmäßig begabter Angreifer sie wiederherstellen. Forensische Toolkits wie *Sleuthkit* unterstützen dabei. Sie bieten Werkzeuge, die den gesamten als frei gekennzeichneten Bereich eines Datenträgers nach Mustern durchsuchen und Dateien aus den Fragmenten wieder zusammensetzen können.

17.2 Dateien sicher löschen (Festplatten)

Um sensible Daten sicher vom Datenträger zu putzen, ist es nötig, sie vor dem Löschen zu überschreiben. Es gibt diverse Tools, die einzelne Dateien oder ganze Verzeichnisse schreddern können.

- Für WINDOWS gibt es AxCrypt (http://www.axantum.com/AxCrypt/). Das kleine Tool zur Verschlüsselung von Dateien integriert sich in den Explorer und stellt in der Premium-Version zusätzliche Menüpunkte für das sichere Löschen von Dateien bzw. Verzeichnissen bereit.
- Unter Linux kann KGPG einen Reißwolf auf dem Desktop installieren. Dateien können per Drag-and-Drop aus dem Dateimanager auf das Symbol gezogen werden, um sie zu schreddern.
- Für Liebhaber der Kommandozeile gibt es *shred* und *wipe* für Linux. Einzelne Dateien kann man mit *shred* löschen:

```
> shred -u dateiname
```

Für Verzeichnisse kann man *wipe* nutzen. Das folgende Kommando überschreibt rekursiv (Option -r) alle Dateien in allen Unterverzeichnissen 4x (Option -q) und löscht anschließend das gesamte Verzeichnis.

```
> wipe -rqf verzeichnis
```

Standardmäßig (ohne die Option -q) überschreibt *wipe* die Daten 34x. Das dauert bei großen Dateien sehr lange und bringt keine zusätzliche Sicherheit.

Btrfs soll das kommende neue Dateisystem für Linux werden und wird bereits bei einigen Server-Distributionen eingesetzt. Bei diesem Dateisystem funktionieren shred und wipe NICHT. Btrfs arbeitet nach dem Prinzip *Copy on Write*. Beim Überschreiben einer Datei werden die Daten zuerst als Kopie in einen neuen Bereich auf der Festplatte geschrieben, danach werden die Metadaten auf den neuen Bereich gesetzt. Ein gezieltes Überschreiben einzelner Dateien auf der Festplatte ist bei Btrfs nicht mehr möglich.

Auch bei diesen Varianten bleiben möglicherweise Spuren im Dateisystem zurück. Aktuelle Betriebssysteme verwenden ein Journaling-Filesystem. Daten werden nicht nur in die Datei geschrieben, sondern auch in das Journal. Es gibt kein Tool für sicheres Löschen von Dateien, welches direkten Zugriff auf das Journal hat. Die Dateien selbst werden aber sicher gelöscht.

17.3 Dateireste nachträglich beseitigen

Mit Bleachbit[1] kann man die Festplatte nachträglich von Dateiresten säubern. Das Programm gibt es für Windows und Linux. Linuxer können es auch aus den Repositorys installieren.

Nach der Installation ist Bleachbit als Administrator bzw. *root* zu starten und nur die Option *Free disk space* zu aktivieren (Abb. 17.1). Außerdem ist in den Einstellungen ein beschreibbares Verzeichnis auf jedem Datenträger zu wählen, der gesäubert werden soll. Anschließend startet man die Säuberung mit einem Klick auf den Button *Clean*.

Die Säuberung einer größeren Festplatte dauert einige Zeit. Dabei werden nur die als *frei* gekennzeichneten Bereiche überschrieben, das Dateisystem bleibt intakt.

17.4 Dateien sicher löschen (SSDs)

Die für Festplatten empfohlenen Tools funktionieren nicht mit Flash-basierten Solid-State-Disks (SSDs). Um die Speicherzellen zu schonen, sorgt die interne Steuerelektronik dafür, dass für jeden Schreibvorgang andere Zellen genutzt werden. Ein systematisches Überschreiben einzelner Dateien ist nicht möglich. Mehr Informationen liefert die Publikation *Erasing Data from Flash Drives*.[2]

Für SSDs ist die TRIM-Funktion zu aktivieren. Dabei werden die Speicherzellen eines Blocks einige Zeit nach dem Löschen der Datei auf den Ursprungszustand zurückgesetzt. Weitere Maßnahmen zum sicheren Löschen sind nicht nötig.

[1] https://www.bleachbit.org
[2] https://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf

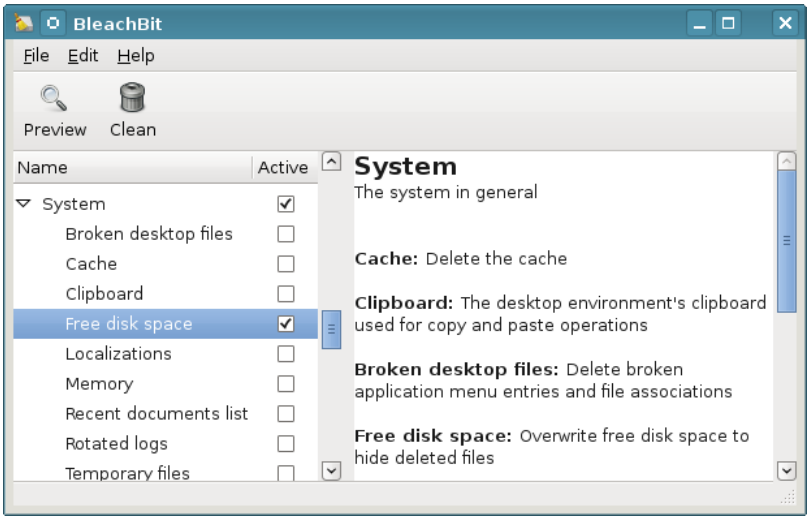


Abbildung 17.1: Bleachbit

Windows aktiviert TRIM standardmäßig, wenn bei der Installation eine SSD-Festplatte gefunden wurde. Mit folgendem Befehl kann man prüfen, ob TRIM aktiv ist:

```
> fsutil behavior query disabledeletenotify
```

Wenn ein Wert = 0 ausgegeben wird, ist Trim aktiviert. Wird ein Wert = 1 ausgegeben wird (weil man eine SSD nachträglich eingebaut hat oder den AHCI-Mode im BIOS erst nachträglich aktiviert), kann man die Trim-Funktion mit folgendem Kommando aktivieren:

```
> fsutil behavior set disabledeletenotify 0
```

Mit *fsutil* wird das Trimmen lediglich aktiviert. Ob es wirklich funktioniert, kann man mit dem kleinen Tool *trimcheck*[3] prüfen. Das Tool ist in einem Verzeichnis auf dem Datenträger abzulegen, den man testen möchte, und als Administrator zu starten.

Linuxer haben für das Trimmen der Datenträger drei Möglichkeiten:

1. Standardmäßig verwenden die meisten Linux-Distributionen *Batched TRIM*. Einmal pro Woche werden alle eingebauten SSDs gesäubert.
   Mit folgendem Kommando kann man prüfen, ob die Säuberung aktiv ist:

   ```
   > sudo systemctl status fstrim.timer
       fstrim.timer - discard unsed blocks once a week
         Loaded: loaded
         Active: active (waiting)
         ...
   ```

   Aktivierung/Deaktivierung der wöchentlichen Säuberung erfolgt mit:

   ```
   > sudo systemctl enable/disable fstrim.timer
   ```

[3] https://github.com/CyberShadow/trimcheck

2. Alternativ kann man *Online TRIM* verwenden, um ungenutzte Blöcke unmittelbar nach dem Löschen der Dateien zu säubern. Für unverschlüsselte Datenträger wird es in */etc/fstab* aktiviert, indem man die Mount-Option *discard* hinzufügt:

   ```
   UUID=[NUMSLETTER] / ext4 discard,noatime,errors=remount-ro 0 1
   ```

   Bei LUKS-verschlüsselten Datenträgern ist *Online TRIM* in */etc/crypttab* zu aktivieren, indem man die Mount-Option *discard* hinzufügt:

   ```
   sda2-crypt /dev/sda2 none luks,discard
   ```

   Nach dem Ändern der Mount-Optionen in */etc/fstab* oder */etc/crypttab* ist es eine gute Idee, die initramfs-Images neu zu bauen:

   ```
   > sudo update-initramfs -u -k all
   ```

3. Außerdem kann man das Trimmen eines SSD-Datenträgers per Hand starten:

   ```
   > sudo fstrim <Mountpoint>
   ```

   Linux-Distributionen ohne systemd enthalten in der Regel ein Cron-Script, das wöchentlich den fstrim Befehl für alle internen Datenträger aufruft.

17.5 Gesamten Datenträger säubern (Festplatten)

Bevor ein Laptop oder Computer entsorgt oder weitergegeben wird, sollte man die Festplatte gründlich putzen. Am einfachsten erledigt man den Job mit **ShredOS**.[4] Nach dem Download der IMG-Datei kann man sie auf einen USB-Stick brennen (siehe Kapitel Boot-Medium für die Linux Installation oder Live-DVD erstellen) und den Computer von diesem Stick booten. (Hinweis: Secure-Boot muss im BIOS des Rechners für ShredOS deaktiviert werden.)

Nach dem Booten wählt man mit Maustasten und Leertaste die zu löschenden Festplatten aus und startet den Löschvorgang mit S. Dann kann es mehrere Stunden dauern.

Eine beliebige Linux-Live-DVD tut es auch (wenn man bereits eine Live-DVD nutzt). Nach dem Booten des Live-Systems öffnet man ein Terminal (Konsole) und überschreibt die gesamte Festplatte. Der Datenträger wird dabei 4x überschrieben, es dauert einige Zeit.

- Für die erste IDE-Festplatte:

  ```
  > wipe -kq /dev/hda
  ```

- Für SATA- und SCSI-Festplatte:

  ```
  > wipe -kq /dev/sda
  ```

Wenn die Live-DVD das Tool *wipe* nicht enthält, kann man alternativ *dd* (disk doubler) nutzen. Um die erste IDE-Festplatte einmal mit NULL und dann noch einmal mit Zufallszahlen zu überschreiben, kann man folgende Kommandos nutzen:

```
> dd if=/dev/zero of=/dev/hda
> dd if=/dev/urandom of=/dev/hda
```

(Einmal mit NULLEN überschreiben reicht.)

[4] https://github.com/PartialVolume/shredos.x86_64

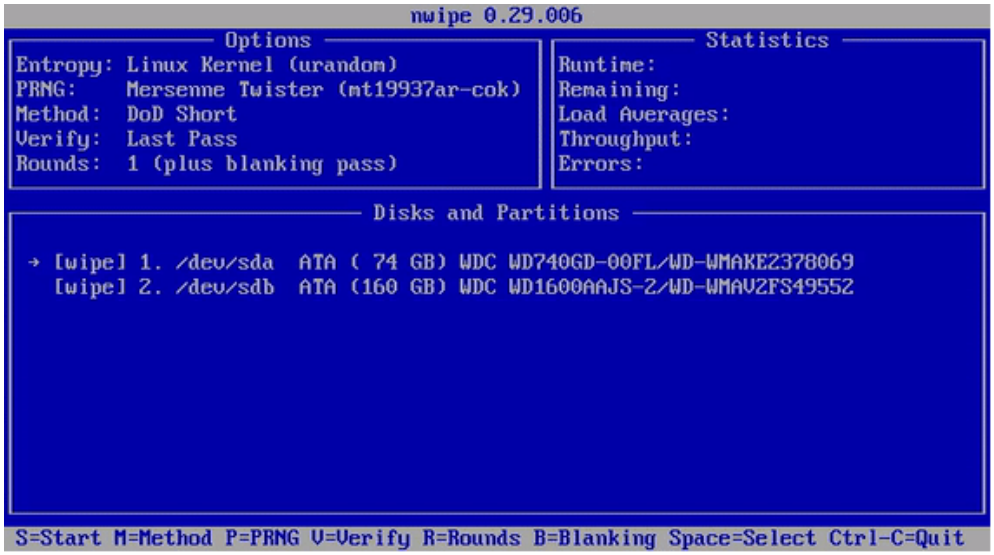


Abbildung 17.2: ShredOS Bedienoberfläche

17.6 Gesamten Datenträger säubern (SSDs)

Wenn man die Haupt-Festplatte (SSD) mit dem Betriebssystem in einem Laptop/PC löschen möchte, muss man von einem anderen Datenträger booten. Man kann eine Linux-Live-DVD nehmen (z. B. Linux Mint), das man auf einen USB-Stick brennt und dann als Bootmedium verwendet. Eventuell muss man die *nvme-cli*-Toolbox noch installieren.

Wenn man die SSDs säubern will, muss man zwischen SATA und NVMe unterscheiden:

SATA-SSDs lassen sich am einfachsten komplett bereinigen, wenn der Datenträger den ATA-Befehl SECURE-ERASE unterstützt. Diese Funktion muss allerdings durch den Datenträger bereitgestellt werden. Linuxer können dafür das Tool *hdparm* nutzen.

Als erstes ist zu prüfen, ob SECURE-ERASE unterstützt wird:

```
> sudo hdparm -I /dev/sda
```

Das Ergebnis muss einen Abschnitt *Security* enthalten und muss auf *not frozen* stehen. Falls die Ausgabe *frozen* liefert, wird SECURE-ERASE im BIOS blockiert.

```
Security:
    Master password revision code = 64060
        supported
    not enabled
    not locked
    not frozen
        expired: security count
        supported: enhanced erase
```

Hinweis: wenn der Zustand *frozen* ist statt *not frozen*, kann man den Rechner suspendieren, mit einem Tastendruck wieder aufwecken und es nochmal versuchen.

Dann kann man ein Passwort setzen und den Datenträger vollständig löschen:

```
> sudo hdparm --user-master u --security-set-pass p /dev/sda
> sudo hdparm --user-master u --security-erase-enhanced p /dev/sda
```

NVMe-SSDs können unter Linux mit der Toolbox *nvme-cli* gereinigt werden. Die Toolbox kann bei den gängigen Linuxen mit dem Paketmanager installiert werden:

```
Ubuntu: > sudo apt install nvme-cli
Fedora: > sudo dnf install nvme-cli
```

Man kann sich anzeigen lassen, welche NVMe-SSDs vorhanden sind:

```
> sudo nvme list
```

SECURE-ERASE für ein Device startet man mit folgendem Kommando:

```
> sudo nvme format -s1 <device>
```

Wenn das Kommando einen Fehler anzeigt, kann man den Rechner suspendieren, mit einem Tastendruck wieder aufwecken und es nochmal versuchen.

```
> systemctl suspend
```

Falls der Datenträger SECURE-ERASE nicht unterstützt, bleibt nur das einfache Überschreiben des Datenträgers. Dabei werden aber nicht alle Speicherzellen garantiert gelöscht. Unter Linux auf der Kommandozeile geht das wieder mit:

```
> dd if=/dev/zero of=/dev/sdc
```

17.7 Tools zum Löschen von SSDs im BIOS von Laptops

Einige Hersteller integrieren Tools zum sicheren Löschen eingebauter SSDs ins BIOS:

- Moderne Lenovo-ThinkPads ab T490/T590 haben mit *ThinkShield secure wipe* eine eingebaute BIOS-Erweiterung zum sicheren Löschen der Festplatte.

  1. Als Erstes muss *ThinkShield secure wipe* aktiviert werden. Dafür öffnet man die BIOS-Einstellungen (Taste F1 beim Booten) und geht dort zum Reiter *Security*.
  2. Nach einem Neustart öffnet man beim Booten die Bootauswahl (Taste F12 beim Booten) und wählt auf dem Reiter *App Menu* die App *ThinkShield*.

  Für ältere Lenovo-ThinkPad-Laptops bis einschließlich T480/T580 gibt es die *ThinkPad Drive Erasing CD*[5], die man auf einen USB-Stick brennen kann. Von diesem Stick bootet man (Taste F12 beim Booten) und kann dann die eingebaute Festplatte schreddern.

- Bei Business-Laptops von Asus findet man das Secure Erase Tool im BIOS (Taste F2 beim Booten) unter *Tools* und kann dort die eingebaute Festplatte direkt löschen.

[5] https://support.lenovo.com/de/de/downloads/ds019026

- Business-Laptops von HP haben ebenfalls ein Secure Erase Tool im BIOS (Taste F10 beim Booten). Man findet es auf dem Reiter *Security* unter *Hard Drive Utilities* und kann dort ebenfalls die eingebaute Festplatte direkt löschen, ohne Neustart.
- Laptops von Dell bringen *Dell Data Wipe* im BIOS mit (Taste F2 beim Booten).
    1. *Dell Data Wipe* kann man unter *Maintainance* → *Data Wipe* → *Wipe at next boot* aktivieren und muss es beim Speichern der BIOS-Settings zweimal bestätigen.
    2. Nach dem Reboot wird man noch zweimal gefragt, ob man die eingebauten Datenträger wirklich, wirklich schreddern will, dann werden sie sicher gelöscht.

17.8 Datenträger zerstören

Den Datenträger physisch zu zerstören, ist die ultimative Form der Datenvernichtung. Man kann es selbst versuchen, mit Bohrmaschine und Flex in der Kellerwerkstatt, oder man übergibt die Daten an einen professionellen Serviceanbieter, der das fachmännisch erledigt.

Die Berliner Firma Nitrokey.com bietet mit NiroShred[6] in Kooperation mit der Rhenus Data Office GmbH diesen Service für Privatkunden und kleinere Unternehmen an. Die Datenträger (SSDs, Festplatten, USB-Sticks, Handys, CDs oder DVDs) werden per Post an die Nitrokey GmbH gesendet, gesammelt der Rhenus Data Office GmbH übergeben und dort gemäß DSGVO, BDSG und DIN 66399 geschreddert. Das Material wird am Ende recycelt. Somit eignet sich der Service auch zur sauberen Entsorgung von alten Smartphones (Kosten: 12,- Euro + Porto), um das grüne Gewissen ein bisschen zu beruhigen.

Hinweis: Der Postversand innerhalb Deutschlands ist vom BSI für vertrauliche Daten bis zur Geheimhaltungsstufe VS-NfD (Nur für Dienstgebrauch) zugelassen.

[6] https://shop.nitrokey.com/de_DE/shop/product/nitroshred-datentragervernichtung-on-demand-106

Kapitel 18

Daten anonymisieren

Fotos, Office-Dokumente, PDFs und andere Dateitypen enthalten in den Metadaten viele Informationen, die auf den ersten Blick nicht sichtbar sind, jedoch vieles verraten können.

Fotos von Digitalkameras enthalten in den EXIF-Tags oft eine eindeutige ID der Kamera, Zeitstempel der Aufnahmen, bei neueren Modellen auch GPS-Daten. Die IPTC-Tags können Schlagwörter und Bildbeschreibungen der Fotoverwaltung enthalten. XMP-Daten enthalten den Autor und der Comment üblicherweise die verwendete Software.

Office-Dokumente enthalten Informationen zum Autor, letzte Änderungen, Kommentare von anderen Bearbeitern, verwendete Softwareversion u. v. a. m.

Es ist manchmal interessant, wenn man die letzten Änderungen rückgängig machen kann und sieht, welche Formulierungen oder Zahlen zuletzt geändert oder angepasst wurden. Office-Dokumente sollte man NIE veröffentlichen!

PDF-Dokumente enthalten ebenfalls viele Metadaten. Besonders geschwätzig sind PDFs, die mit Microsoft Office generiert wurden. Sie enthalten nicht nur beschreibende Metadaten für das Dokument, sondern evtl. auch URLs, von denen Bilder eingebunden wurden, Kommentare, Lesezeichen usw.

Ein Beispiel: Professionelle Personalmanager schauen sich bei online zugesendeten Bewerbungen routiniert die Metadaten der Dokumente an. Wenn der Autor des Dokuments nicht der Bewerber selbst war, sondern bspw. *bewerbungsmappe.de*, hat man Hinweise, wo die Vorlage herkommt, und kann diese Informationen in die Bewertung einfließen lassen.

Vor dem Upload von Fotos und anderen Dateien ins Internet ist es ratsam, diese überflüssigen Informationen zu entfernen. Es gibt mehrere Firmen, die sich auf die Auswertung dieser Metadaten spezialisiert haben. Ein Beispiel ist die Firma Heypic, die die Fotos von Twitter durchsucht und anhand der GPS-Koordinaten auf einer Karte darstellt. Auch Strafverfolger nutzen diese Informationen. Das FBI konnte einen Hacker mit den GPS-Koordinaten im Foto seiner Freundin finden[1].

Der *StolenCameraFinder*[2] sucht anhand der Kamera-ID in den EXIF-Daten alle Fotos, die mit dieser Digital-Kamera gemacht wurden (Smartphone-Kameras werden nicht unterstützt). Da die Kamera-ID mit hoher Wahrscheinlichkeit eindeutig einer Person zugeordnet werden kann, sind viele Anwendungen für diese Suche denkbar. Die verbesserte Version *CameraForensics*[3] ist nur für Strafverfolgung verfügbar.

[1] http://www.tech-review.de/include.php?path=content/news.php&contentid=14968
[2] http://www.stolencamerafinder.com
[3] https://www.cameraforensics.com/

18.1 Fotos und Bilddateien anonymisieren

Fotos und Bilddateien vor der Veröffentlichung im Internet anonymisieren:

- Wenn man ein Foto in einem Bildbearbeitungsprogramm geöffnet hat, kann man beim Export ins JPEG- oder PNG-Format festlegen, dass keine Metadaten gespeichert werden sollen.

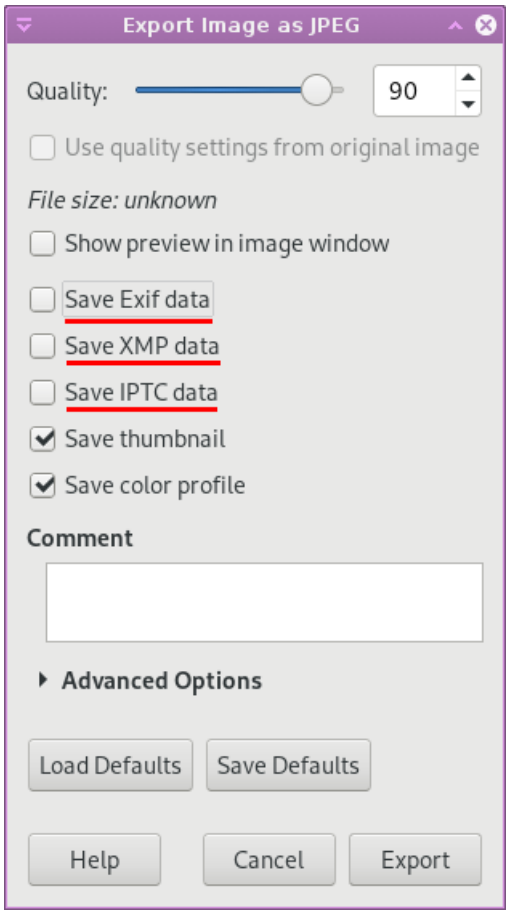


Abbildung 18.1: Foto ohne Metadaten speichern (Gimp)

  Durch das Speichern wird das Foto auch neu komprimiert, was individuelle Eigenschaften der Kamera verwischt und die Analyse mit Image-Forensic-Tools erschwert.

- **exiv2** (für Linux) ist ein nettes kleines Tool zum Bearbeiten von EXIF-, XMP- und IPTC-Informationen in Bilddateien. Es ist in den meisten Linux-Distributionen enthalten und kann mit dem bevorzugten Paketmanager installiert werden:

  ```
  Ubuntu: > sudo apt install exiv2
  ```

  Nach der Installation kann man z. B. Fotos auf der Kommandozeile säubern:

  ```
  > exiv2 rm foto.jpg
  ```

Das Kommando kann man als Service-Menü für Bilddateien in verschiedene Dateimanager integrieren. Für Konqueror und Dolphin (KDE) steht eine passende Datei auf der Webseite[4] zum Download bereit.

18.2 PDF-Dokumente säubern

PDF-Dokumente können Metadaten enthalten, die Informationen über die verwendete Software, den Autor u. a. m. verraten. Das Beispiel zeigt die (sparsamen) Metadaten einer PDF-Präsentation, die mit der LaTeX-Klasse *Beamer* erstellt wurde:

```
File Size       : 76 kB
File Type       : PDF
MIME Type       : application/pdf
PDF Version     : 1.5
Linearized      : No
Page Count      : 3
Page Mode       : UseOutlines
Author          : Max Mustermann
Title           : Sinnlose Präsentation für Metadaten
Creator         : LaTeX with Beamer class
Producer        : pdfTeX-1.40.18
Create Date     : 2018:05:08 12:38:21+02:00
Modify Date     : 2018:05:08 12:38:21+02:00
Trapped         : False
PTEX Fullbanner : pdfTeX, Version 3.14159265-2.6-1.40.18 (TeX Live
↪  2017/Debian) kpathsea version 6.2.3
```

Wenn man PDF-Dokumente im Internet veröffentlicht, werden die Metadaten von Suchmaschinen gescannt und in den Index aufgenommen. Würde man eigene PDF-Dokumente in einem anonymen Blog veröffentlichen, könnte man anhand der Metainformationen als Autor deanonymisiert werden.

Die online versendeten PDFs oder Bewerbungsunterlagen werden ebenfalls geprüft:

> *Mein erster Blick bei allen PDF-Bewerbungen und PDF-Dateien von Banken, Versicherungen und Firmen erfolgt stets in die Dateieigenschaften der PDFs. Das ist immer aufschlussreich, oft witzig, manchmal peinlich oder aus Daten- und IT-Sicherheitsblickwinkel bedenklich ...*
>
> *Bei Bewerbungsunterlagen habe ich damit einen wunderbaren Ansatzpunkt für Diskussionen, wenn der Autor eines PDFs z. B. bewerbungsmappe.de oder der Name eines Nicht-Ehepartners oder der bisherige Arbeitgeber ist. Man erkennt sofort ...*

Neben den Metainformation des PDF-Dokumentes können auch eingebundene Bilder verräterische Metainformationen enthalten. Die Auswertung ist allerdings komplizierter.

Da oben ein LaTeX-Dokument als Beispiel genannt wurde, hier ein kleiner Hinweis: LaTeX erstellt PDF-Dokumente mit minimalen Metadaten, wenn man das Paket *pdfprivacy* einbindet:

[4] https://www.privacy-handbuch.de/handbuch_43b.htm

```
\documentclass[twoside,a4paper,11pt,hyphens]{report}
\usepackage{pdfprivacy}
...
```

Warnhinweis: Es gibt einige Tools, die behaupten, Metadaten aus PDFs mit dem ExifTool entfernen zu können. Dabei werden eingebettete Bilder jedoch *nicht* gereinigt! Außerdem sind die Änderungen reversibel (die alten Daten sind weiterhin im PDF enthalten), wenn das Dokument nicht nachträglich linearisiert wird.

PDF-Dokumente säubern unter Windows

PDF-Dokumente sollte man zuerst in eine neues PDF-Dokument drucken, um die Metainformationen von eingebetteten Bildern und Medien zu entfernen. Dafür braucht man einen PDF-Drucker. Unter Windows bietet z. B. *PDF Creator* von PDF24.org diesen Drucker. Nach der Installation des Pakets steht ein PDF-Drucker zur Verfügung.

Nach dem Konvertieren in ein sauberes PDF kann man z. B. mit dem *Hexonic PDF Metadata Editor*[5] die restlichen Metadaten wie Erstellungsdatum und Drucksoftware aus dem Dokument entfernen. Nach dem Download und evtl. der Installation kann man das Tool starten und die zu säubernden PDF-Dokumente laden.

PDF-Dokumente säubern unter Linux

Auch unter Linux sollte man ein PDF-Dokument zuerst in ein neues PDF drucken. CUPS stellt standardmäßig einen PDF-Drucker dafür bereit.

Die verbleibenden Metainformationen von dem Druckvorgang kann man mit den Tools *exiftool* und *qpdf* entfernen. Beide Programme kann man mit dem bevorzugten Paketmanager installieren:

```
Debian: > sudo apt install libimage-exiftool-perl qpdf
Fedora: > sudo dnf install perl-Image-ExifTool qpdf
```

Nachdem das PDF mit einem PDF-Viewer in eine neue PDF-Datei namens *datei-print.pdf* gedruckt wurde, können die restlichen Metadaten mit *exiftool* auf leere Werte gesetzt werden. Danach wird das PDF-Dokument mit *qpdf* linearisiert, damit die reversiblen Rückstände verschwinden:

```
> exiftool -all:all= datei-print.pdf
  Warning: [minor] ExifTool PDF edits are reversible.
    1 image files update

> qpdf --linearize datei-print.pdf datei-clean.pdf

> rm datei-print.pdf
```

exiftool arbeitet in-place und modifiziert die Input-Datei direkt, *qpdf* liest eine Input-Datei und schreibt das Ergebnis in eine neue Output-Datei.

Mit folgendem Kommando kann man dann die Metadaten prüfen:

[5] http://www.hexonic.de/index.php/hexonic-pdf-metadata-editor

```
> exiftool -all:all datei-clean.pdf
....
MIME Type : application/pdf
PDF Version : 1.5
Linearized : Yes
Page Mode : UseOutlines
Page Count : 4
```

Man könnte sich auch ein kleines Script schreiben, um den Aufruf zu vereinfachen. Das folgende Mini-Script pdf-meta-clean.sh (mit ein bisschen Fehlerbehandlung) wird mit dem Dateinamen der zu reinigenden PDF-Datei aufgerufen. Es macht seine Arbeit und danach sind die Metadaten weg. (Es wird kein Backup der originalen Datei behalten!)

```
#!/bin/bash

if [ -z "$1" ]; then
   echo "Usage: `basename $0` <Dateiname>"
   exit 1
fi

if [ ! -f "$1" ]; then
   echo "FEHLER Die Datei $1 ist nicht vorhanden!"
   exit 1
fi

FILETYPE=`mimetype -b "$1"`
if [ $FILETYPE != "application/pdf" ]; then
   echo "FEHLER: Datei $1 ist keine PDF Datei!"
   exit 1
fi

if [ ! -w "$1" ]; then
   echo "FEHLER Die PDF Datei $1 kann nicht modifiziert werden!"
   exit 1
fi

if [ -z `which exiftool` ]; then
   echo "FEHLER: Das Programm exiftool ist nicht installiert!"
   exit 1
fi

if [ -z `which qpdf` ]; then
   echo "FEHLER: Das Programm qpdf ist nicht installiert!"
   exit 1
fi

exiftool -all:all= "$1"
TFILE=`mktemp`
cp "$1" "$TFILE"
qpdf --linearize "$TFILE" "$1"
```

```
rm "$TFILE"
exit 0
```

Nach dem Download könnte man das Script nach /usr/local/bin kopieren und als ausführbar markieren:

```
> sudo cp Download/pdf-meta-clean.sh /usr/local/bin/pdf-meta-clean
> sudo chmod +x /usr/local/bin/pdf-meta-clean
```

Dann kann man folgendes Kommando aufrufen, um eine PDF-Datei zu reinigen:

```
> pdf-meta-clean dateiname.pdf
```

PDF-Dokumente säubern mit MAT2 (Linux)

MAT2 (Metadata Anonymisation Toolkit 2)[6] ist ein Kommandozeilentool für Linux, das Metadaten von vielen Bild-, Audio-, Video- und Office-Formaten sowie von PDFs entfernen kann.

Für PDFs werden die oben beschriebenen Schritte in einem Kommando zusammengefasst. Ein PDF-Dokument wird mit der Cairo-Bibliothek gedruckt und dann werden die Metadaten entfernt.

Pakete[7] gibt es für Debian-basierte Distributionen, OpenMandriva und Void Linux (Debian enthält eine veraltete Version, die man durch eine aktuellere Version aus den Backports ersetzen sollte). In der Live-DVD TAILS ist MAT2 enthalten. Ubuntus können es wie folgt nutzen:

```
> sudo apt install mat2
> mat2 --inplace <Datei> (ohne Backup der org. Datei bereinigen)
```

Für Mäuschenschubser gibt es mit dem *Metadata Cleaner*[8] ein MAT2-GUI für alle Linux-Distributionen als Flatpak-Paket, das neben MAT2 auch alle benötigten Bibliotheken und Tools mitbringt.

PDF-Dokumente säubern in QubesOS

Die sicherheitsoptimierte Linux-Distribution QubesOS hat einen eingebauten Konverter für PDF-Dateien, den man im Dateimanager mit einem Rechtsklick auf ein PDF-Dokument aufrufen kann: *Convert to trusted PDF*. Das Tool ist primär für die Behandlung von möglicherweise bösartigen Dokumenten gedacht, die man aus dem Internet heruntergeladen oder per E-Mail bekommen hat. Es lässt sich aber auch gut zum Reinigen von eigenen PDFs nutzen.

Es wird *qubes-app-linux-pdf-converter* gestartet. Das Rendering des (möglicherweise bösartigen) PDF-Dokumentes erfolgt in einer Disposable VM, die danach gelöscht wird, und die gerenderten Bitmaps werden zu einem neuen, ganz harmlosen PDF zusammengesetzt. Wie bei QubesOS üblich, dauert der Vorgang insbesondere bei großen PDF-Dokumenten einige Zeit.

[6] https://0xacab.org/jvoisin/mat2
[7] https://pkgs.org/download/mat2
[8] https://metadatacleaner.romainvigier.fr

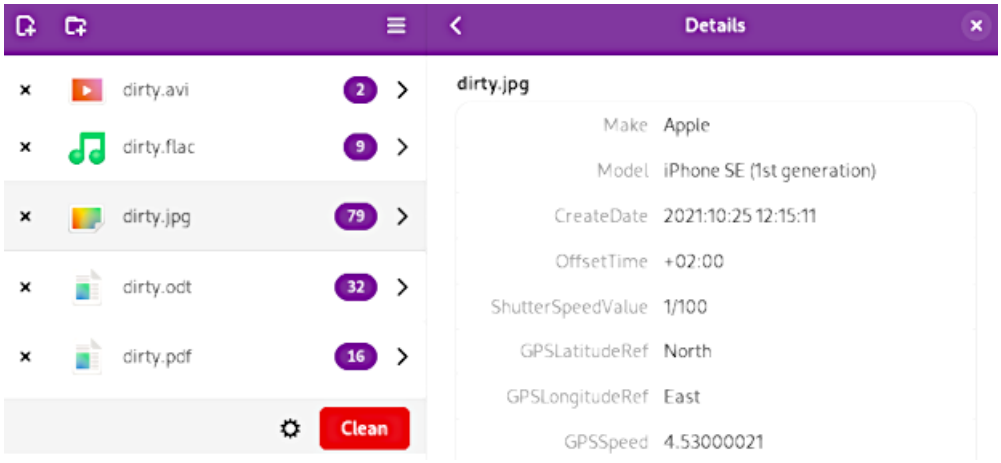


Abbildung 18.2: Metadata Cleaner

PDF-Dokumente säubern mit Dangerzone

Dangerzone[9] ist vom QubesOS-PDF-Konverter inspiriert und eine Umsetzung dieses Konzeptes für Windows, MacOS und verschiedene Linux-Distributionen.

Ein (möglicherweise bösartiges) PDF- oder Office-Dokument (aus dem Internet?) wird in einer virtuellen Wegwerf-Umgebung (Docker) virtuell gedruckt und das Ergebnis neu zusammengesetzt. Dabei werden neben allen Bösartigkeiten auch die Metadaten aus dem Dokument entfernt.

18.3 MS Office Dokumente säubern

Microsoft Office Dokumente (Word, Excel, Powerpoint) enthalten viele Metadaten. Neben den Namen der Autoren, Kommentare, verwendete Vorlagen, Zeitstempel der Erstellung und letzten Änderungen werden auch Informationen über den zuletzt verwendeten Drucker und den Speicherort des Dokumentes gespeichert. Teilweise kann man auch die letzten Änderungen nachverfolgen. Das ist schon seit mehr als 20 Jahren bekannt und war schon öfters peinlich:

Unter Umständen kann ein einzelnes MS Office Dokument einem motiviertem Angreifer genug Informationen für einen Angriff auf ein Firmennetzwerk liefern. Ein kleines Beispiel:

[9] https://github.com/freedomofpress/dangerzone

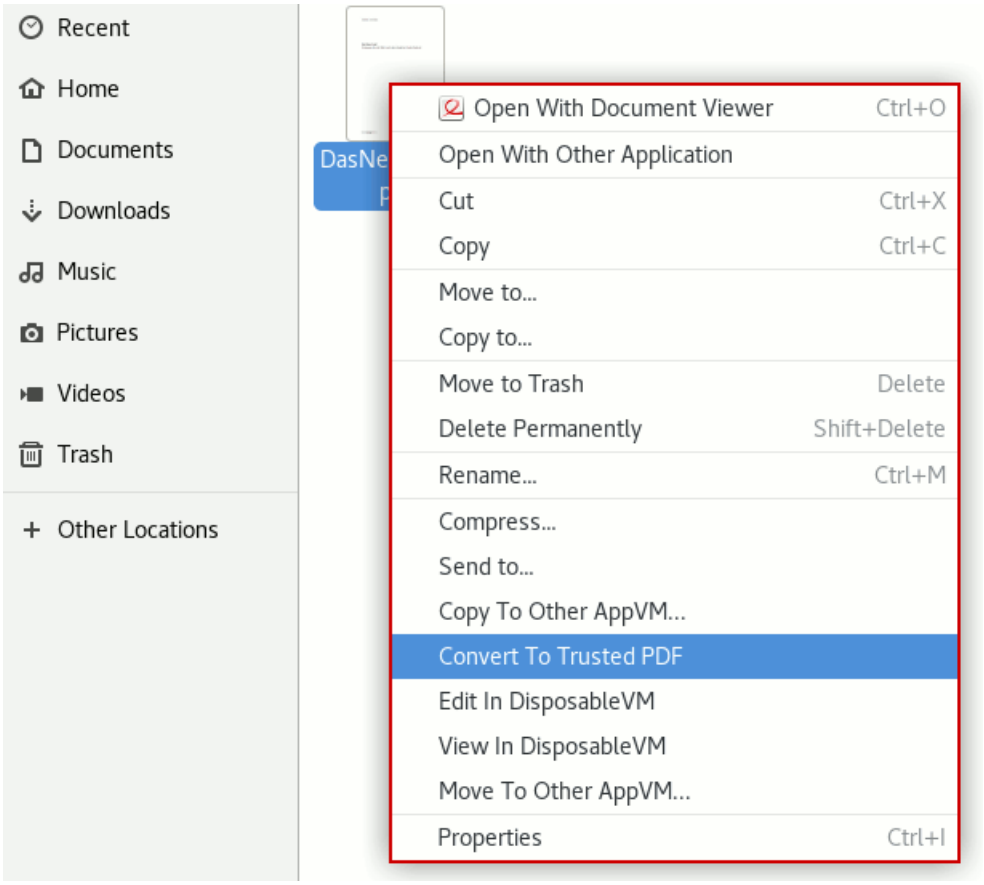


Abbildung 18.3: QubesOS: PDF-Konverter aufrufen

1. Der Angreifer findet in den Metadaten die Adresse und Typ eines angreifbaren HP Druckers (CVE-2021-39238, CVE-2021-39237 - Wer patcht die Firmware von Netzwerkdruckern?) oder einen ungepatchten Windows Druckserver (PrintNightmare CVE-2021-34527).[10] [11]
2. Mit den Informationen aus dem Inhalt des Dokumentes (der Speicherort verrät im Verzeichnispfad evtl. noch eine brauchbare Projektnummer o. Ä.) konstruiert er eine glaubhafte Phishing E-Mail an den oder die Autoren, deren Namen er in den Metadaten findet.
3. E-Mail Adressen lassen sich in Firmen oft aus den Namen der Zielpersonen erraten.
4. Mit der E-Mail werden die Opfer auf eine Webseite gelockt, die aus dem Browser heraus einen Cross-Site-Printing Angriff auf den HP Drucker oder den Druckserver abfeuert.[12]
5. Der kompromittierte Drucker könnte Firmendaten ausleitet oder das Netz infiltrieren.

Metadaten aus MS Office Dokumenten entfernen

Manchmal muss man ein MS Office Dokument weiterzugeben und möchte Metadaten vor der Weitergabe an Dritte entfernen, auch wenn das Dokument nicht im Internet publiziert wird.

[10] https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-548868-10M2.html
[11] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
[12] https://book.hacktricks.xyz/network-services-pentesting/pentesting-printers/cross-site-printing

MS Office Programme (Word, Excel, Powerpoint) bieten die Möglichkeit, Metadaten zu entfernen. Unter *Datei* → *Informationen* → *Auf Probleme prüfen* wählt man *Dokument prüfen* (Abb. 18.4).

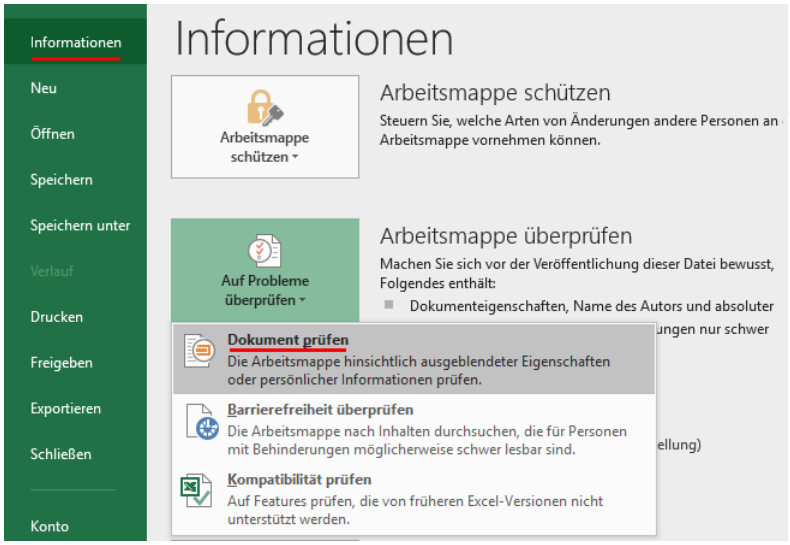


Abbildung 18.4: Metadata in MS Office Dokumenten entfernen

In dem sich öffnenden Dialog klickt man auf *Prüfen* und kann die Metadaten löschen (Abb. 18.5).

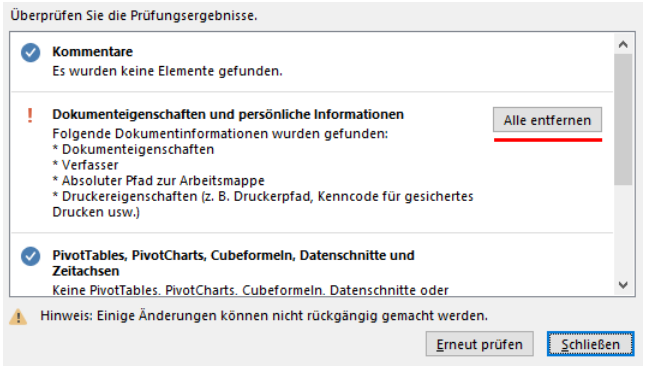


Abbildung 18.5: Gefundene Metadata in MS Office Dokumenten löschen

MS Office Dokumenten in PDFs konvertieren

Für die Publikation im Internet oder Weitergabe an firmenfremde Dritte sind PDFs besser geeignet als MS Word Dokumente oder Powerpoint Präsentationen. Dabei gibt es zwei Möglichkeiten:

1. Beim **PDF Export** werden sicherheitskritische Informationen über die IT Infrastruktur entfernt aber Name des Autors, UUID des Dokumentes, Softwareversion... bleiben erhalten:

```
PDF Version  : 1.7
Linearized   : No
Page Count   : 11
Language     : de-DE
Tagged PDF   : Yes
```

```
XMP Toolkit  : 4.8-911
Producer     : Microsoft® Word 2020
Creator      : Mustermann, Max
Creator Tool : Microsoft® Word 2020
Create Date  : 2023:03:02 17:20:66+01:00
Modify Date  : 2023:03:02 17:20:66+01:00
Document ID  : uuid:XXXXXX-YYYY-YYYY-YYYY-ZZZZZZZ
Instance ID  : uuid:XXXXXX-YYYY-YYYY-YYYY-ZZZZZZZ
Author       : Mustermann, Max
```

2. Das **Drucken als PDF** ist ein bisschen sparsamer bei Metadaten:

```
PDF Version : 1.7
Linearized  : No
Author      : maxe (Windows User Login Kennung)
Create Date : 2023:03:02 17:20:66+01:00
Modify Date : 2023:03:02 17:20:66+01:00
Producer    : Microsoft: Print To PDF
Title       : Dateiname.pdf
Page Count  : 11
```

   Die verbliebenen Metadaten könnte man mit einem PDF Metadaten Editor rausputzen.

Hinweis: auch für LibreOffice und OpenOffice gilt, dass das Drucken als PDF weniger Metadaten enthält als der PDF Export aus Writer oder Impress.

Datenreihen als CSV statt Excel Tabelle

Wenn man einfache Datenreihen im Internet veröffentlichen möchte, kann man Excel Tabellen für die Erfassung der Daten nutzen und das Arbeitsblatt dann als CSV Datei exportieren. CSV Dateien sind einfache Textdateien, bei denen die Werte in einer Zeile durch Semikolon oder Komma getrennt sind. Der Empfänger kann die Daten in MS Excel oder LibreOffice importieren.

Kapitel 19

Daten verstecken

Geheimdienste orakeln seit Jahren immer wieder, dass *Terroristen* über versteckte Botschaften in Bildern kommunizieren. Telepolis berichtete 2001 und 2008 kritisch-ironisch über Meldungen von Scotland Yard, wonach islamische Terroristen ihre Kommunikation in pornografischen Bildern verstecken würden. Stichhaltige Belege für die Nutzung von **Steganografie** konnten bisher nicht geliefert werden. Andere Journalisten hinterfragten die Meldungen weniger kritisch:

> „Bislang ist zwar noch nicht bewiesen, ob die Terrorverdächtigen die Bilder – bei einem Verdächtigen wurden 40.000 Stück gefunden – nur zum persönlichen Vergnügen heruntergeladen haben oder ob tatsächlich ein Kommunikationsnetzwerk aufgebaut wurde.“ (Welt Online[1], wieder einmal viel heiße Luft.)

Wie funktioniert diese Technik, über die *Zeit Online* bereits 1996 berichtete, und können Nicht-Terroristen das auch nutzen?

Ein Beispiel

Statt Bits und Bytes werden in diesem Beispiel Buchstaben genutzt, um das Prinzip der Steganografie zu erläutern. Nehmen wir mal an, Terrorist A möchte an Terrorist B die folgende kurze Botschaft senden:

```
Morgen!
```

Statt die Nachricht zu verschlüsseln, was auffällig sein könnte, versteckt er sie in dem folgenden, harmlos aussehenden Satz:

```
Mein olles radio geht einfach nicht!
```

Wenn der Empfänger weiß, dass die eigentliche Botschaft in den Anfangsbuchstaben der Wörter kodiert ist, wäre es ganz gut, aber nicht optimal.

Ein Beobachter könnte auf den Gedanken kommen: *„Was? Wieso Radio? Der zahlt doch keine GEZ!“* Er wird aufmerksam und mit ein wenig Probieren kann er die Botschaft extrahieren. Also wird Terrorist A die Nachricht zusätzlich verschlüsseln, nehmen wir mal eine einfache Caesar-Verschlüsselung mit dem Codewort KAWUM, es entsteht:

```
Ilpcmg!
```

und ein neuer, halbwegs sinnvoller Satz wird konstruiert und verschickt.

[1] http://www.welt.de/politik/article2591337/

19.1 Allgemeine Hinweise

Das Beispiel verdeutlicht, welche Voraussetzungen für die Nutzung von Steganografie zum Austausch von versteckten Botschaften gegeben sein müssen:

- Sender und Empfänger müssen sich darüber verständigt haben, wie die Nutzdaten versteckt werden.
- Das Passwort für die Verschlüsselung muss ausgetauscht werden.
- Die Modalitäten für den Austausch der Trägermedien müssen geklärt werden. Wo kann der Empfänger die Fotos mit den versteckten Botschaften finden?

Wenn diese Voraussetzungen geklärt sind, kann es losgehen

1. Der Absender schreibt seine Botschaft mit einem einfachen Texteditor.
2. Die Textdatei wird in einem (anonymisierten) Foto oder in einer Audiodatei mit Steganografie-Tools wie z. B. *DIIT* oder *steghide* versteckt und gleichzeitig mit dem Passwort verschlüsselt.
3. Das Foto könnte man dem Empfänger per E-Mail senden. Das ist aber nicht unbedingt die beste Idee, da dabei die Metadaten der Kommunikation ausgewertet werden können (A hat B eine Mail geschrieben, Stichwort: Kommunikationsanalyse). Um auch die Metadaten der Kommunikation zu verstecken, könnte der Absender das Foto in seinem (anonymen) Blog veröffentlichen. Man könnte es bei Flickr oder Twitpic hochladen oder an eine öffentliche Newsgruppe im Usenet senden. Wichtig ist, dass es öffentlich publiziert wird und der Empfänger nicht erkennbar ist. Außerdem kann der Absender verschiedene Maßnahmen ergreifen, um selbst anonym zu bleiben.
4. Der Empfänger muss wissen, wo er aktuelle Nachrichten finden kann. Fotos oder Audiodateien, in denen der Empfänger eine Botschaft vermutet, sind herunterzuladen.
5. Danach kann der Empfänger versuchen, die geheime Botschaft aus dem Trägermedium zu extrahieren. Dabei ist das gleiche Tool wie beim Verstecken zu verwenden. Wenn er alles richtig macht und das korrekte Passwort verwendet, wird die Textdatei extrahiert und kann mit einem einfachen Texteditor gelesen werden.

Unsichtbare Markierungen, Wasserzeichen

Man kann Steganografie-Tools auch nutzen, um unsichtbare Wasserzeichen an Bildern oder Audiodateien anzubringen.

Wenn Fotos oder Videos nur einem kleinen Kreis von Personen zugänglich gemacht werden sollen, dann können individuelle Wasserzeichen steganografisch in den Dateien versteckt werden. Sollten diese Fotos oder Videos in der Öffentlichkeit auftauchen, kann das Leck anhand des unsichtbaren steganografischen Wasserzeichens ermittelt werden.

19.2 steghide

steghide ist ein Klassiker unter den Tools für Steganografie und wird auf der Kommandozeile gesteuert. Es kann beliebige Daten verschlüsselt in JPEG, BMP, WAV oder AU Dateien verstecken. Die verwendeten Algorithmen sind sehr robust gegen statistische Analysen. Die Download-Seite bietet neben den Quellen auch Binärpakete für Windows. Nutzer von Debian und Ubuntu installieren es wie üblich mit *aptitude*.

Um die Datei *geheim.txt* zu verschlüsseln und in dem Foto *bild.jpg* zu verstecken, ruft man es mit folgenden Parametern auf (mit dem Parameter -sf kann optional eine dritte Datei als Output verwendet werden, um das Original nicht zu modifizieren):

```
> steghide embed -cf bild.jpg -ef geheim.txt
Enter passphrase:
Re-Enter passphrase:
embedding "geheim.txt" in "bild.jpg"... done
```

Der Empfänger extrahiert die geheimnisvollen Daten mit folgendem Kommando (mit dem Parameter -xf könnte ein anderer Dateiname für die extrahierten Daten angegeben werden):

```
> steghide extract -sf bild.jpg
Enter passphrase:
wrote extracted data to "geheim.txt".
```

Außerdem kann man Informationen über die Coverdatei bzw. die Stegodatei abfragen. Insbesondere die Information über die Kapazität der Coverdatei ist interessant, um abschätzen zu können, ob die geheime Datei reinpasst:

```
> steghide info bild.jpg
Format: jpeg
Kapazität: 12,5 KB
```

19.3 stegdetect

Auch die Gegenseite ist nicht wehrlos. Manipulationen von steghide, F5, outguess, jphide usw. können z. B. mit *stegdetect*[2] erkannt werden. Ein GUI steht mit *xsteg* zur Verfügung, die Verschlüsselung der Nutzdaten kann mit *stegbreak* angegriffen werden. Beide Zusatzprogramme sind im Paket enthalten.

Der Name *stegdetect* ist eine Kurzform von *Steganografie-Erkennung*. Das Programm ist nicht nur für den Nachweis der Nutzung von *steghide* geeignet, sondern erkennt anhand statistischer Analysen auch andere Tools.

Auch *stegdetect* ist ein Tool für die Kommandozeile. Neben der zu untersuchenden Datei kann mit einem Parameter -s die Sensitivität eingestellt werden. Standardmäßig arbeitet stegdetect mit einer Empfindlichkeit von 1.0 ziemlich oberflächlich. Sinnvolle Werte liegen bei 2.0 bis 5.0.

```
> stegdetect -s 2.0 bild.jpg
F5(***)
```

[2] http://www.outguess.org/download.php

Im Beispiel wird eine steganografische Manipulation erkannt und vermutet, dass diese mit dem dem Tool F5 eingebracht wurde (was nicht ganz richtig ist, da *steghide* verwendet wurde).

Frage: Was kann man tun, wenn auf der Festplatte eines mutmaßlichen Terroristen 40.000 Bilder rumliegen? Muss man jedes Bild einzeln prüfen?

Antwort: Ja – und das geht so:

1. Der professionelle Forensiker erstellt zuerst eine 1:1-Kopie der zu untersuchenden Festplatte und speichert das Image z. B. in *terroristen_hda.img*

2. Mit einem kurzen Dreizeiler scannt er alle 40.000 Bilder in dem Image:

   ```
   > losetup -o $((63*512)) /dev/loop0 terroristen_hda.img
   > mount -o ro,noatime,noexec /dev/loop0 /mnt
   > find /mnt -iname "*.jpg" -print0 | xargs -0 stegdetect -s 2.0 >>
   ↪  ergebnis.txt
   ```

   (Für Computer-Laien und WINDOWS-Nutzer sieht das vielleicht nach Voodoo aus, für einen Forensiker sind das jedoch Standardtools, deren Nutzung er aus dem Ärmel schüttelt.)

3. Nach einiger Zeit wirft man einen Blick in die Datei *ergebnis.txt* und weiß, ob es etwas interessantes auf der Festplatte des Terroristen gibt.

Kapitel 20

Betriebssysteme

Der Widerstand gegen Ausforschung und Überwachung sowie der Kampf um die Hoheit über den eigenen Computer beginnt bei der Auswahl des Betriebssystems. Einige stichpunktartige Gedanken sollen zum Nachdenken anregen.

20.1 Microsoft Windows

Mit Windows 8.0 hat Microsoft begonnen, das bei Smartphones akzeptierte Device-based-Tracking auch bei PCs einzuführen. Ähnlich wie Google bei Android will Microsoft als eine der größten Tracking-Familien im Internet seine Datenberge erweitern.

Das Erstellen eines User-Accounts unter Windows 8.1 ist ein echtes Dark Pattern. Der Nutzer wird massiv gedrängt, den User-Account auf dem Rechner mit einem Online-Konto bei Hotmail oder Windows Live zu verbinden. Nur wenn man in der Eingabemaske falsche Angaben macht, findet man in der Fehlermeldung den unscheinbaren Link für das Erstellen eines User-Accounts ohne Online-Konto.

In Windows 10 wurde das Device-based Tracking weiter ausgebaut. Es wird für jeden Account auf dem Rechner eine *Unique Advertising ID* generiert. Diese ID wird auch Dritten zur eindeutigen Identifikation zur Verfügung gestellt. In der neuen Privacy Policy von Microsoft (Juli 2015) steht außerdem:

> *We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary [...].*

Private Daten, die Microsoft in der Standardkonfiguration sammelt:

- Persönliche Interessen, die sich aus dem Surfverhalten sowie aus den über die Apps gesammelten Daten ergeben, werden an Microsoft gesendet (eine Sport-App sendet die bevorzugten Teams, eine Wetter-App die häufig angefragten Städte usw.).
- Standortdaten aller Geräte mit Windows werden an MS übertragen. Es werden bevorzugt GPS oder die WLANs der Umgebung genutzt, um den Standort so genau wie möglich zu bestimmen.
- Kontaktdaten der Freunde und Bekannten werden an MS übertragen, wenn man Tools von Microsoft als Adressbuch nutzt.

- Inhalte von E-Mails, Instant Messages und Voice/Video-Messages (z. B. Skype) gehören ebenfalls zu den den Daten, die MS sammelt.
- Der Windows Defender übermittelt alle installierten Anwendungen an Microsoft.
- Mit der digitalen Assistentin *Cortana* wird in der Standardkonfiguration eine Art Abhörzentrale eingerichtet, die das Wohnzimmer direkt mit Microsoft verbindet.
- Das Schreibverhalten wird analysiert und an Microsoft gesendet. Das Profil der typischen Tastenanschläge könnte zukünftig für die Identifikation bei Texteingaben in Webformularen oder Chats genutzt werden (Stichwort: Keystroke Biometrics[1]).
- Die eindeutige UUID, die Windows bei der Kommunikation mit Microsoft-Servern sendet (z. B. bei Softwareupdates), wird vom NSA und GCHQ als Selektor für Taylored Access Operations (TAO) verwendet, um gezielt die Computer von interessanten Personen oder Firmen anzugreifen. Microsoft ist seit 2007 Partner im PRISM Programm der NSA.
- Als besonderes Highlight gehören auch die automatisch generieren Recovery Keys der Festplattenverschlüsselung Bitlocker zu den Daten, die MS in seiner Cloud sammelt und NSA/FBI/CIA zur Verfügung stellt. (Crypto War 3.0?)

  Mit Windows 10 Pro oder Enterprise kann man den Upload des Recovery-Key verhindern[2], indem man den Rechner einmal komplett verschlüsselt (mit Key Upload), dann die Verschlüsselung deaktiviert (damit muss das System wieder komplett entschlüsselt werden), den alten Recovery-Schlüssel löscht und nochmal den Rechner komplett verschlüsselt. Erst beim zweiten Versuch wird man gefragt, ob man den Recovery-Key evtl. lokal sichern möchte. Das kostet Zeit und ist auch wieder ein echtes Dark Pattern in der Benutzerführung.

Wenn man es schafft, einen Benutzeraccount ohne Cloud-Anbindung einzurichten und in den Einstellungen unter Datenschutz die Privacy-Features aktiviert, kann man die Sammelleidenschaft von Windows 10 etwas reduzieren, aber nicht vollständig abstellen.[3]

Experten des BSI warnten 2013 vor dem Einsatz von Windows 8 in Kombination mit TPM 2.0 und bezeichneten es als inakzeptables Sicherheitsrisiko für Behörden und Firmen. Nutzer eines Trusted-Computing-Systems verlieren nach Ansicht der Experten die Kontrolle über ihren Computer. (Das ist doch der Sinn von Trusted Computing – oder?)

> *Aus Sicht des BSI geht der Einsatz von Windows 8 in Kombination mit einem TPM 2.0 mit einem Verlust an Kontrolle über das verwendete Betriebssystem und die eingesetzte Hardware einher. Daraus ergeben sich für die Anwender, speziell auch für die Bundesverwaltung und kritische Infrastrukturen, neue Risiken.*

T. Baumgärtner von Microsoft(!) erklärte in einer Antwort:

> *Das betrifft aber nur bestimmte Behörden, der Verfassungsschutz oder der BND sollten das System natürlich besser nicht nutzen.*
> ...
> *Für normale Nutzer bietet das TPM 2.0 ein enormes Plus an Sicherheit.*

Ähmm ...

[1] https://de.wikipedia.org/wiki/Tippverhalten
[2] https://theintercept.com/2015/12/28/recently-bought-a-windows-computer-microsoft-probably-has-your-encryption-key/
[3] http://arstechnica.com/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft/

20.1.1 Windows datenschutzfreundlich konfigurieren

Die Standardinstallation von Windows kann man mit einigen Einstellungen datenschutzfreundlicher konfigurieren und sicherer. Man kann die Telemetrie einschränken, überflüssige Cloud Features und Software wie One Drive deinstallieren (wenn man es nicht verwendet)... usw.

Wenn man kein Diplom als Microsoft Certified Engineer (MCE) hat und nicht weiß, an welchen Schrauben man drehen kann, dann könnte die Webseite **Privacy.sexy** hilfreich sein.[4]

1. Die Webseite bietet auf der linken Seite die Möglichkeit, in mehreren Kategorien eine Auswahl zu treffen, welche Features man deaktivieren möchte. Als Einsteiger könnte man mit der Vorauswahl *Standard* beginnen und später weitere Optionen hinzufügen.

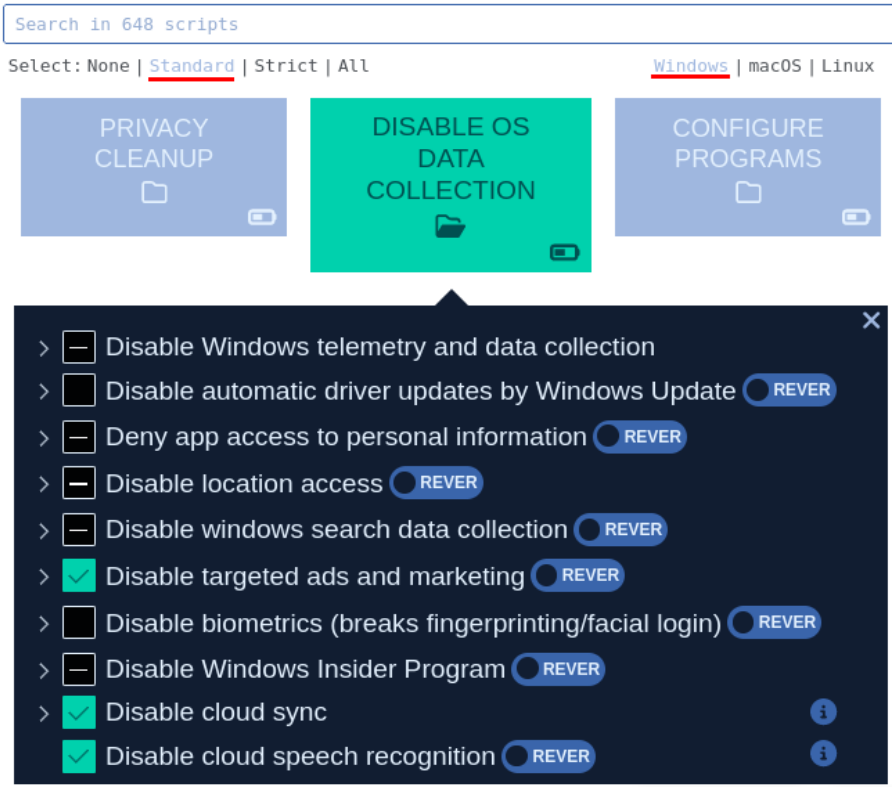


Abbildung 20.1: Auswahl der zu deaktivierenden Windows Features auf Privacy.sexy

2. Auf der rechten Seite wird der Code für ein Batch Script angezeigt, welches die gewünschten Änderungen vornehmen würde. Das Script kann man mit den beiden grünen Button unten herunterladen oder in die Zwischenablage kopieren, um es im Texteditor zu übernehmen.

3. Das heruntergeladene Script führt man als Administrator aus - SCHWUPPS - fertig.

4. Wenn man versehentlich eine nützliche Option deaktiviert hat, die man eigentlich gern behalten möchte, dann kan man das leicht korrigieren. Man aktiviert zuerst die Vorauswahl *None*, wählt die versehentlich deaktivierte Option und aktiviert *Revert* hinter der Option.

   Das auf der rechten Seite angezeigte Batch Script lädt man wieder herunter und führt es als Adminstrator aus - und SCHWUPPS, das Feature ist wieder da.

[4] https://privacy.sexy/

20.1.2 Telemetrie in Windows 10

Die Microsoft Telemetrieserver sammeln pro Tag 65 Trillionen Meldungen von den weltweit genutzten Windows Computern und Microsoft Software ein (Stand 2023).

Windows 10 reagiert auf 1.000–1.200 Ereignisse, die eine Log-Meldung triggern, welche dann an die Telemetrie-Server von Microsoft übertragen wird. Microsoft Office sendet noch mehr Daten. Bei dem Paket MS Office Pro Plus lösen 23.000–25.000 Ereignisse eine Datenübertragung an Telemetrie-Server aus. 20–30 Teams arbeiten an der Auswertung, wobei Microsoft keinen Gesamtüberblick hat, welche Produkte welche Daten senden.[5]

Das BSI hat für Windows 10 die Telemetriedaten in der Analyse **SiSyPHuS Win10** genauer untersucht (preiswürdiger Titel). Dabei kommt das BSI zu dem Ergebnis, dass die Übertragung der Telemetriedaten in Windows 10 Basic durch die Konfiguration von Einstellungen nicht vollständig deaktivierbar ist.[6]

Als Schutz gegen die Datensammelwut empfiehlt das BSI, die Verbindungen zu den Windows-Telemetrie-Servern auf DNS-Ebene zu blockieren. Diese Blockade muss außerhalb des Windows-Betriebssystems erfolgen, da der Windows Defender die übliche Nutzung der Datei *%windir%/system32/drivers/etc/hosts* zur Blockade von Trackingservern auf DNS-Ebene für diesen Zweck blockiert.

Man kann folgende Lösungen nutzen:

1. Die Liste der Telemetrie-Server könnte auf dem Router in einer Blacklist gepflegt werden. Fast alle Router bieten diese Funktion zum Blockieren von DNS-Namen und man muss für alle Rechner im Heimnetz nur eine Liste an einer Stelle pflegen.

   In einer FritzBox findet man die DNS-Blacklist unter *Internet* → *Filter* → *Listen*.

2. Wenn man im lokalen Netz einen zentralen DNS-Resolver betreibt, kann man die DNS-Namensauflösung für die Telemetrie-Server an dieser Stelle blockieren und im DNS-Resolver eine Sperrliste konfigurieren.

3. Wenn der Datenverkehr von einer zentralen Firewall gefiltert wird, kann die DNS-Namensauflösung für die Telemetrie-Server auch auf der Firewall blockiert werden. Dabei wird der UDP-Datenverkehr auf Port 53 nach den Namen der Server gefiltert und Anfragen an Upstream-DNS-Server für diese Domains blockiert.

   Die Regel für eine *iptables* Firewall definiert man nach folgendem Muster:

   ```
   iptables -A OUTPUT -p udp --dport 53 -m string --hex-string \
   ↪  "|03|oca|09|telemetry|09|microsoft|03|com" -algo bm -j DROP
   ```

   Das Blockieren der IP-Adressen der Telemetrie-Server ist nicht sinnvoll, da es sich dabei um Cloud-Dienste mit wechselnden IP-Adressen handelt.

4. Wenn ein zentraler Proxy für den gesamten externen Datenverkehr im lokalen Netz eingesetzt wird, dann können Verbindungen zu den Telemetrie-Servern auch auf dem Proxy blockiert werden. Das BSI veröffentlicht eine Beispielkonfiguration für *squid*.

[5] https://www.golem.de/news/datenschutz-aerger-microsoft-sammelt-bis-zu-25-000%20ereignistypen-bei-office-1811-137815.html

[6] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html

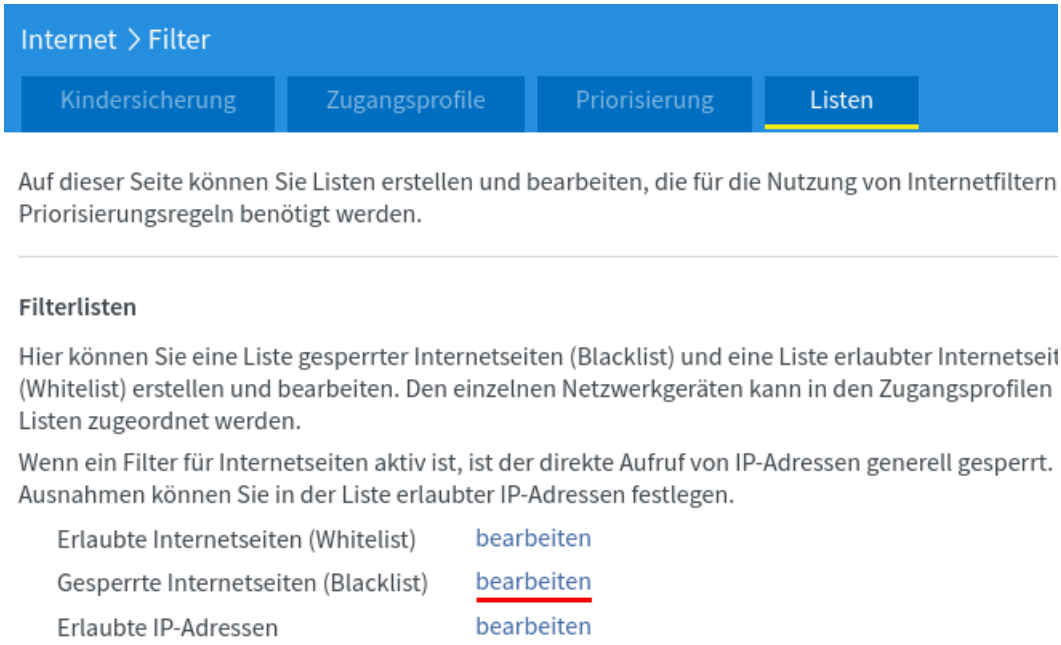


Abbildung 20.2: DNS-Blacklist in der Fritzbox verwalten

Die vom BSI untersuchte Windows-Version sendet Daten an folgende Server (Stand: Win 10 21H2)[7]):

```
au-v10.events.data.microsoft.com
alpha.telemetry.microsoft.com
asimov-win.settings.data.microsoft.com.akadns.net
au-v10.events.data.microsoft.com
au-v20.events.data.microsoft.com
au.vortex-win.data.microsoft.com
ceuswatcab01.blob.core.windows.net
ceuswatcab02.blob.core.windows.net
cy2.vortex.data.microsoft.com.akadns.net
db5-eap.settings-win.data.microsoft.com.akadns.net
db5.settings-win.data.microsoft.com.akadns.net
db5.vortex.data.microsoft.com.akadns.net
de-v20.events.data.microsoft.com
de.vortex-win.data.microsoft.com
eaus2watcab01.blob.core.windows.net
eaus2watcab02.blob.core.windows.net
eu-v10.events.data.microsoft.com
eu-v20.events.data.microsoft.com
eu.vortex-win.data.microsoft.com
events.data.microsoft.com
events-sandbox.data.microsoft.com
geo.settings-win.data.microsoft.com.akadns.net
geo.vortex.data.microsoft.com.akadns.net
```

[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Telemetrie-Endpunkte_Windows10_Build_Build_21H2.html

```
jp-v10.events.data.microsoft.com
jp-v20.events.data.microsoft.com
modern.watson.data.microsoft.com.akadns.net
oca.telemetry.microsoft.com
settings-win.data.microsoft.com
telecommand.telemetry.microsoft.com
uk-v20.events.data.microsoft.com
uk.vortex-win.data.microsoft.com
us4-v20.events.data.microsoft.com
us5-v20.events.data.microsoft.com
us-v10.events.data.microsoft.com
us-v20.events.data.microsoft.com
us.vortex-win.data.microsoft.com
v10.events.data.microsoft.com
v10.vortex-win.data.microsoft.com
v10-win.vortex.data.microsoft.com.akadns.net
v20.events.data.microsoft.com
v20.vortex-win.data.microsoft.com
vortex-win.data.microsoft.com
vortex-win-sandbox.data.microsoft.com
watson.telemetry.microsoft.com
weus2watcab01.blob.core.windows.net
weus2watcab02.blob.core.windows.net
```

Zukünftige Windows-Versionen können weitere oder andere Server nutzen.

20.1.3 Virescanner sind Snakeoil

Für 90 % der Windows-Nutzer ist ein Virenscanner ein unverzichtbares Sicherheitstool, aber nur 7 % der Security-Experten halten zusätzliche Virenscanner neben dem standardmäßig installierten Windows Defender für sinnvoll. Warum sind Sicherheitsexperten so skeptisch und bezeichnen diese Produktgruppe als Schlangenöl?

1. Virenscanner sind eine komplexe Software, die immer wieder selbst schwere Fehler enthält, die von einem Angreifer ausgenutzt werden können. Insbesondere die Parser für komplexe, exotische Dateiformate enthalten immer wieder Fehler.[8] [9] [10] [11]

   Da ein Virenscanner tief im System verankert ist und vollen Zugriff auf alle Systemkomponenten hat, kann ein Angreifer durch Ausnutzen von Bugs im Virenscanner das System vollständig kompromittieren, ohne dass der Anwender etwas bemerkt.

   Außerdem wird die Implementierung von Sicherheitsfeatures durch Softwareentwickler (z. B. die konsequente Umsetzung von ASLR) durch Virenscanner behindert, wie Robert O'Callahan berichtete. Er rät zur De-Installation.[12]

   Schlussfolgerung: Virenscanner machen den Rechner unsicher.[13]

[8] https://www.heise.de/-3250784
[9] https://www.heise.de/-3159436
[10] https://www.heise.de/-3149913
[11] https://www.heise.de/-2824437
[12] https://www.heise.de/-3609009
[13] https://www.golem.de/news/security-antivirenscanner-machen-rechner-unsicher-1407-108199.html

2. Viele Virenscanner brechen die TLS-Transportverschlüsselung der Webbrowser und E-Mail-Clients, um die verschlüsselten Inhalte zu scannen. Es ist ein klassischer Man-in-the-Middle-Angriff mit Zustimmung der Anwender. Damit wird die Sicherheit der TLS-Verschlüsselung massiv geschwächt.[14] [15]

   Moderne Webbrowser bieten umfangreiche Sicherheitsfeatures für TLS wie Strict Trasport Security (HSTS), Certificate Pinning (HKPS) oder mit Add-ons auch DANE/TLSA Validation. Virenscanner beherrschen diese Sicherheitsfeatures in der Regel nicht. (Ich kenne kein Produkt der Schlangenöl-Branche mit diesen Sicherheitsfunktionen.) Einige Virenscanner beherrschen nicht einmal das moderne TLS 1.2 und downgraden die Verschlüsselung auf die schwache Version TLS 1.0.

   AV-Hersteller sind grob fahrlässig bei HTTPS-Interception.[16]

3. Mit der Installation eines Virenscanners gibt der Nutzer die Hoheit über die Installation von Software praktisch teilweise auf. Es ist die Aufgabe eines Virenscanners, Software zu entfernen, die der Hersteller der Software für unpassend hält. Das kann auch zur Deinstallation von Software genutzt werden, die man nicht nutzen soll.

4. In der Regel verwenden Mainstream-Viren keine 0-Day-Exploits, um die Systeme zu kompromittieren. Die relativ teuren Angriffe mit 0-Day-Exploits werden nur für gezielte Angriffe auf besondere Ziele eingesetzt, und nicht bei Viren. Computer-Viren nutzen i. d. R. längst bekannte Lücken in der Software aus, die in verschiedenen Quellen nach der Beseitigung durch den Softwarehersteller publiziert wurden.

   Regelmäßige Updates der verwendeten Software und sichere Konfiguration des Systems schützen besser gegen die Angriffe mit Viren als ein Virenscanner.

   Hinweis: zur sicheren Konfiguration gehört als Erstes, dass man die Einstellungen der Benutzerkontensteuerung auf die höchste Sicherheitsstufe stellt. Es ist bedauerlich, dass Microsoft dieses Sicherheitsfeature nicht standardmäßig aktiviert.

5. Gegen potente Angreifer, die ein Target gezielt mit staatlich subventionierten Trojanern angreifen, können (und wollen?) kommerzielle Virenscanner nicht schützen. Das konnte man anhand der Veröffentlichungen zur NSA-Cyberwaffe *Regin* verfolgen.

   - Als Erstes fand Fox-IT den Trojaner *Regin* bei der Analyse des Einbruchs bei Belacom. Es wurde aber nichts veröffentlicht und die Signaturen wurden nicht in die Datenbank für Kunden aufgenommen. Ronald Prins von Fix-IT sagte nach der Veröffentlichung von *Regin* durch The Intercept im November 2014:

     > *We didn't want to interfere with NSA/GCHQ operations. Everyone seemed to be waiting for someone else to disclose details of Regin first, not wanting to impede legitimate operations related to global security.*

   - Dann wurde der Trojaner *Regin* von Symantec analysiert und auch nichts veröffentlicht. V. Thakur von Symantec sagte im November 2014 als Entschuldigung:

     > *We had been investigating Regin since last year, but only felt comfortable publishing details of it now.*

   - Im Sommer 2014 wurde *Regin* auf dem Laptop einer Mitarbeiterin im Bundeskanzleramt gefunden. Auch über diesen Vorfall wurde geschwiegen, bis die Bild-Zeitung im

[14] https://www.heise.de/-2482344
[15] https://www.heise.de/-3095024
[16] https://www.heise.de/-3620159

Dezember 2014 (nach der Veröffentlichung von The Intercept) den Vorgang marktschreierisch veröffentlichte. Die Bundesregierung wollte diese NSA-Spionage anfangs nicht kommentieren und dementierte halbherzig.

- Erst nachdem The Intercept im November 2014 angekündigt hatte, über *Regin* zu berichten, reagierten die Anti-Virus Firmen und informierten die Öffentlichkeit.

20.2 Apple MacOS

Wenn man die Apple-Datenschutzrichtlinien liest, erkennt man, das MacOS sich nicht als Betriebssystem eignet, wenn man seine Privatsphäre nicht mit Apple teilen möchte:

> *Wir erheben Daten wie namentlich Beruf, Sprache, Postleitzahl, Vorwahl, individuelle Geräteidentifizierungsmerkmale, Weiterleitungs-URL sowie Ort und Zeitzone, wo Apple Produkte verwendet werden, damit wir das Verhalten unserer Kunden besser verstehen und unsere Produkte, Dienste und Werbung verbessern können.*

Damit begann die heute allgegenwärtige Datensammlung *im Gerät* und für diese Innovation wurde Apple mit dem BigBrother 2011 geehrt.

Apple ist außerdem seit Oktober 2012 Partner im PRISM-Programm der NSA.

20.3 Linux-Distributionen

Es gibt eine Vielzahl von Linux-Distributionen, sodass man als potentieller Anwender erst einmal vor der Qual der Wahl steht: Debian und Derivate, OpenSuSE, OpenMandriva, Fedora, Gentoo für Bastler, Minidistributionen wie Puppy, KaliLinux für *Offensive Security* usw. Ich kenne nicht alle Distributionen, daher nur einige Gedanken.

Alltagstaugliche Distributionen mit Debian-Abstammung

- **Debian** ist ein robustes Arbeitstier unter den Linux-Distributionen. Die Maintainer bemühen sich vor allem um die Stabilität der zahlreichen Softwarepakete und weniger um neueste Features. In Kombination mit den langen Release-Zyklen ergibt sich ein System, das mit brandneuer Software und Hardware (insbesondere Laptops) öfters Probleme hat, aber nach erfolgreicher Installation lange Zeit stabil läuft.

- **MX Linux** ist ein Debian (stable) mit eleganterem Desktop, der vor allem Umsteigern von Windows die Arbeit erleichtert. Für den Unterbau werden die originalen Debian-Pakete verwendet, also eine große, aber nicht brandaktuelle Softwareauswahl.

  Um Debians Probleme mit aktueller Hardware zu lösen, gibt es *Advanced-Hardware-Support*-Versionen mit aktuellerem Linux-Kernel und neuen Grafiktreibern.

- **Ubuntu** ist angetreten, um das bessere Debian zu sein und mit aktueller Software auch neueste Hardware gut zu unterstützen. Zeitweise ging das Projekt mit dem Unity-Desktop eigene Wege und die Übertragung sämtlicher Suchanfragen auf dem Desktop an kommerzielle Dritte wie Amazon war ein Fiasko für die Privatsphäre.

  Daneben gibt es weitere Privacy-invasive Tools in Ubuntu, die ständig irgendwelche Ubuntu-Server kontaktieren. Einige kann man problemlos deinstallieren wie den Crash Reporter

apport und das Report Submission Tool *whoopsie*, das täglich den Server *daisy.ubuntu.com* kontaktiert. Die Deinstallation überflüssiger Software ist auch der Sicherheit dienlich. Ein Bug im Crash Reporter *apport* konnte beispielsweise jahrelang dazu genutzt werden, den Rechner aus der Ferne zu kompromittieren.[17]

Neben der halbjährlich aktualisierten Distribution gibt es **Ubuntu LTS** (Long Term Support), die man alle zwei Jahre komplett aktualisieren sollte. Der Long Term Support gilt nur für die 2.300 Pakete des Main-Repository. Der Rest der 45.000 Pakete wird manchmal nur mangelhaft oder sporadisch mit Sicherheitsupdates versorgt.

Ubuntu Pro bietet kostenpflichtige Subscriptions für Firmen mit 10 Jahren Support für das Main-Repository (2.300 Pakete) und das Universe-Repository (23.000+ Pakete) sowie kleine Zusatzfeatures wie FIPS-zertifizierte Kryptosoftware. Für Privatanwender gibt es eine kostenlose Subscription für bis zu 5 Rechner (dafür ist ein Account bei Ubuntu One nötig). Das Angebot positioniert sich als direkte Konkurrenz zu RedHat Enterprise Linux.

Wenn man einen Ubuntu-One-Account erstellt und ein Token für die Ubuntu-Pro-Subscription besorgt hat, kann man die Repositorys für die langfristigen Updates aktivieren:

```
> sudo pro attach <Token>
```

Danach kann man das System wie üblich auf den aktuellsten Stand bringen:

```
> sudo apt full-upgrade
```

Xubuntu, Kubuntu, Lubuntu oder Ubuntu Budgie sind Derivate, bei denen standardmäßig ein anderer Desktop installiert wird. Sie übernehmen komplett den Unterbau von Ubuntu. Man kann sich die Derivate herunterladen und vor der Installation live ausprobieren, ob man damit vielleicht besser zurechtkommt oder es hübscher findet.

Hinweis: die Aktivierung von Ubuntu Pro ist auch für diese Derivate empfehlenswert.

- **Linux Mint** ist das bessere Ubuntu und bietet mit Cinnamon einen eleganten Desktop, der sich besonders für Windows-Umsteiger eignet. Die Standardinstallation bietet einen hübschen, voll ausgestatteten Desktop ohne Snaps oder die Privacy-invasiven Tools wie *whoopsie*. Mit der Linux Mint Debian Edition (LMDE) gibt es auch eine Variante, die auf Debian basiert.

- **ElementaryOS** verwendet ebenfalls das Basissystem von Ubuntu und setzt darauf einen eleganten Desktop, der sich stark am Design von MacOS orientiert.

  Alle Anwendungen werden als Flatpak-Pakete installiert. Das ermöglicht sehr aktuelle Anwendungen, hat aber den Nachteil eines hohen Ressourcenbedarfs, weil Flatpak-Pakete die Bibliotheken selbst mitbringen und sie nicht mit anderen Anwendungen teilen.

  Vor dem Download bitten die Entwickler um eine Spende, aber man kann $0 angeben.

Alltagstaugliche Distributionen mit RHEL-Abstammung

- **RHEL** (RedHat Enterprise Linux) ist eine kommerzielle Linux-Distribution, für die man nur Updates bekommt, wenn man eine Lizenz kauft. RedHat konzentriert sich auf Sicherheit im kommerziellen Umfeld und bietet deshalb SELinux-Integration und eine deutlich kleinere

[17] https://www.golem.de/news/linux-sicherheit-ubuntu-bug-ermoeglicht-das-ausfuehren-von-schadcode-1612-125112.html

Software-Auswahl als Debian (vor allem bei Multimedia). Eine Major-Version von RHEL wird über 10 Jahre vollständig gepflegt, was für den Sicherheitsbereich wichtig ist.

Den Unterschied zwischen Debian und RedHat bei der Softwareausstattung bemerkt man schon bei kleinen Systemtools wie *top*. RedHat bietet standardmäßig nur *top*, während Debian auch Derivate wie *htop* oder *atop* mitbringt. Diese Derivate kann man in RedHat nur installieren, wenn man zusätzlich externe Repositorys einbindet.

- **Fedora** ist die Community-Version von RedHat, für die man auch ohne Lizenz Updates bekommt. Bei der Installation geht Fedora einen anderen, mehr sicherheitsorientierten Weg als die Ubuntu-Derivate. Statt eines voll ausgestatteten Desktops wird nur ein sehr minimales System installiert und man muss die benötigte Software nachinstallieren.

  Standardmäßig werden bei Fedora keine Office-Pakete und nur eine sehr magere Multimedia-Unterstützung installiert. Um eine mit den Ubuntus vergleichbare Unterstützung für Multimedia zu erhalten, kann man zusätzlich das RPMfusion-Repository einbinden[18] und die gewünschten Multimedia-Pakete installieren (was Nachteile hinsichtlich Sicherheit bringt, wenn man *bad* oder *ugly* Codecs installiert). Man könnte den VLC-Player installieren:

  ```
  > sudo dnf install vlc
  ```

  Neue Fedora-Versionen erscheinen halbjährlich. Updates werden für ein Jahr + ein paar Wochen bereitgestellt. Es gibt keine Long-Term-Support(LTS)-Versionen wie bei Ubuntu-Derivaten, sodass man ein System regelmäßig komplett aktualisieren muss.

  Neben der Standardversion mit dem GNOME Desktop gibt es wie bei Ubuntu die Fedora Spins[19] mit alternativen Desktops wie KDE, XFCE, LXDE, LXQT, Mate, Cinnamon, Budgy oder SWAY. Man kann sich die ISO Images der Spins herunterladen und als Live-System ausprobieren, bevor man sich entscheidet und eine Version dauerhaft installiert.

- **Nobara Linux** ist eine für Gamer optimierte Distribution auf Basis von Fedora. Die sehr aktuellen Kernel und Hardwaretreiber liefern eine hohe Performance.

  Das universille Linux-Spiele-Tool Lutris, den Steam-Installer sowie ProtonUp-Qt kann man einfach mit der Packetverwaltung installieren und sofort mit Daddeln loslegen.

Rolling-Release-Distributionen

Einmal installiert und mit kleinen Aktualisierung immer auf dem neuesten Stand der Software Entwicklung ist die Philosophie von Rolling Release Distributionen.

- **Arch Linux** bietet als Besonderheit den Rolling-Release-Zyklus. Einmal installieren und mit kleinen Aktualisierung immer wieder auf den neuesten Stand bringen, ist die Philosophie dahinter. Große Sprünge mit System-Upgrades des Gesamtsystems sind nicht nötig.

  Um Probleme bei Updates zu vermeiden, sollte man Rolling-Release-Distributionen oft und regelmäßig aktualisieren, damit Änderungen am Gesamtsystem klein bleiben.

- **Manjaro** ist die aufgehübschte Version von Arch Linux, die sich mit einem eleganten Desktop insbesondere an Windows-Umsteiger wendet.

[18] https://rpmfusion.org/Configuration
[19] https://spins.fedoraproject.org

- **Void Linux** ist ein komplett eigenständiges Projekt, das nicht als Abspaltung von einer anderen Distribution entstanden ist. Es ist ein schlankes Linux (ohne systemd). Die Live-Systeme (XFCE) kann man gefahrlos ausprobieren und dann installieren. Full Disk Encryption bietet der Installer nicht, dafür muss man das Full-Text-Adventure spielen.[20]

Um Probleme bei Updates zu vermeiden, sollte man Rolling Release Distributionen regelmäßig in kurzen Abständen aktualisieren, damit die Änderungen am Gesamtsystem klein bleiben.

Immutable (unveränderbare) Distributionen

Bei immutable (unveränderbaren oder unkaputtbaren) Distributionen wird das gesamte Betriebsystem als nicht modifizierbares Image read-only eingebunden. Updates werden ebenfalls als komplettes Image bereitgestellt. Zusätzliche Software installiert man in der Regel als Flatpak (GUI Programme) oder in Containern (Daemons und CLI Tools als Binärpakte). Es gibt auch Tools, um zusätzliche Software in die Systemimages einzubinden, aber davon wird abgeraten.

- **Silverblue** (GNOME) oder **Kinoite** (KDE) sind immutable Desktop Systeme auf Basis von Fedora. sind immutable Desktop Systeme auf Basis von Fedora. Neben Flatpaks werden Toolboxen[21] als Container unterstützt.
  - Ein Container ist keine abgeschlossene Umgebung wie eine virtuelle Maschine (VM). Ein neuer Container stellt anfangs die gleiche Umgebung wie der Host zur Verfügung. Man kann die Daten im Home-Verzeichnis aus dem Host-System lesen, aber Änderungen und neue Dateien sind nur innerhalb des Containers verfügbar.
  - In einem Container kann man Software ganz normal mit *dnf* installieren, compilieren, testen usw. Die zusätzliche Software steht nur im Container zur Verfügung.
- **Vanilla OS** ist ein immutable Desktop System auf Basis von Ubuntu, das einsteigerfreundlich sein möchte. Neben Flatpaks kann man zusätzliche Software via *apx* installieren.

Immutable Distributionen sind eine Basis für Software Entwickler und andere Bastler, die gern mit dem Gerät spielen und sich ärgern, wenn die Installation dabei kaputt geht.

Für besondere Sicherheitsanforderungen

- **Qubes OS** ist eine besondere Linux-Distribution. Alle Anwendungen laufen in mehreren getrennten, virtuellen Maschinen mit einem Xen-basierten Hypervisor, der die Gastsysteme überwacht und ihnen nur begrenzt Zugriff auf die Hardware lässt. Qubes OS bietet:
  - Schutz durch starke Isolation der einzelnen Anwendungen;
  - getrennten Netzwerkzugriff für jede der VMs;
  - Schutz gegen BadUSB-Devices durch eine Proxy-VM für USB-Geräte, mit der kontrolliert wird, welche USB-Geräte in den Arbeits-VMs zur Verfügung stehen;
  - umfangreiche graphische Integration der virtuellen Maschinen inklusive Farben zur visuellen Abgrenzung der VMs untereinander;

[20] https://docs.voidlinux.org/installation/guides/fde.html
[21] https://docs.fedoraproject.org/en_US/fedora-silverblue/toolbox

– Dateien aus unsicheren Quellen kann man in Disposable VMs anzeigen, bearbeiten oder in *trusted PDFs* konvertieren (Dieser Schutz ist aber nur effektiv, wenn man die Generierung von Thumbnails im Dateimanager abschaltet!).

QubesOS basiert auf Fedora, enthält aber auch Templates für Debian-VMs und Whonix (Tor Onion Router). In den Fedora-Templates von QubesOS ist die Nutzung der RPMfusion-Repositorys bereits vorbereitet, sie müssen nur aktiviert werden:

```
> sudo dnf config-manager --set-enabled rpmfusion-free
> sudo dnf config-manager --set-enabled rpmfusion-free-updates
```

Ein Nachteil von QubesOS ist der wesentlich höhere Speicherbedarf als andere Distributionen und eine Entschleunigung bei der Arbeit mit dem Computer.

Bei allen Linux-Distributionen erhält man nach einem einfachen Installationsprozess, der auch für Laien durchführbar ist, ein lauffähiges System mit wesentlich umfangreicherer Software als mit Windows oder MacOS. Gleichzeitig ist das System detailliert anpassbar und unter der Kontrolle des Anwenders, der *root* sein kann. Die bekannten Programme wird ein Umsteiger von Windows vergeblich suchen, es gibt kein Photoshop, keinen Windows-Explorer oder MS Office, dafür gibt es zahlreiche Alternativen.

20.3.1 Linux-taugliche Hardware

Man hat eigentlich kaum Probleme, moderne Linux Distributionen auf Standardhardware aus dem Großmarkt zu installieren. Trotzdem ein paar Hinweise auf besondere Perlen:

- Die deutsche Firma TUXEDO Computers bietet 100 % Ubuntu-kompatible Laptops und PCs in vielen Varianten, auch Notebooks im edlen Design. Andere Linux Ditributionen funktionieren auch, aber vorinstalliert gibt es nur eine Auswahl von Ubuntu Derivaten. Die Intel Management Engine ist im BIOS deaktivierbar.[22]
- Die niederländische Firma NovaCustom bietet Linux-taugliche Laptops mit Coreboot BIOS. Die Intel Management Engine kann abgeschaltet werden und verschiedene Linux Distributionen können beim Einkauf vorinstalliert geordert werden.[23]
- Die spanische Firma Slimbooks bietet edle Laptops mit Fedora an, die mit zwei SSD Festplatten bestückt werden können, die als RAID 1 zusammenarbeiten können.[24]
- Die Business-Laptops von Lenovo (X2x0, T4x0, T5x0) sind robust und kompatibel mit aktuellen Linux-Distributionen. Man kann sie auch gebraucht noch gut verwenden.

Hardware für besondere Sicherheitsanforderungen:

- Die **NitroPads** basieren entweder auf etwas älteren, robusten Thinkpad Business Laptops von Lenovo (X230, T430) oder modernen Laptops von NovaCustom (NS50, NV42).[25]

[22] https://www.tuxedocomputers.com
[23] https://laptopzusammenstellen.com/linux-laptops
[24] https://slimbook.es/en/store/special-editions?keyword=fedora
[25] https://shop.nitrokey.com/de_DE/shop

  - Die Integrität des Coreboot-BIOS, des TPM und des Kernels des Betriebssystems kann mit einem Nitrokey Pro oder Nitrokey Storage verifiziert werden, der vor dem Booten eingesteckt wird und grün blinkt, wenn alles Ok ist.
  - Die Laptops werden wahlweise mit einem vorinstalliertem Ubuntu LTS oder QubesOS als Betriebssystem ausgeliefert. Eine vollständige Verschlüsselung der Festplatte ist dabei eingerichtet – sofort startfertig. Man muss nur dass LUKS Passwort ändern und den PIN für den Nitrokey.
  - Die Intel Management Engine ist deaktiviert und die Ausstattung konfigurierbar.
  - Der 12,5 Bildschirm des X230 ist wirklich klein. Für ergonomisches Arbeiten sind ein zusätzlicher Monitor, Maus und Tastatur auf dem Schreibtisch empfehlenswert .

- Die **Purism Laptops** (Librem 14, Librem 15) und der **Purism Mini** bieten ebenfalls diese besonderen Sicherheitsfeatures:

  - Es kommt ein reduziertes Coreboot-BIOS zum Einsatz. Die Integrität des BIOS kann mit dem Librem Key verifiziert werden (BIOS-Tamper-Schutz).[26]
  - Der Librem Key kann auch als Schlüssel für die Full-Disk-Encryption verwendet werden. Es ist ein modifizierter Nitrokey, der als OpenPGP- oder SSH-Schlüssel, als Passwortspeicher und OTP-Token für Zwei-Faktor-Authentifizierung genutzt werden kann.
  - Hardware-Kill-Switches für Mikrofon, Kamera, Wi-Fi und Bluetooth schützen gegen Angriffe, die das Gerät in eine Spionage-Wanze verwandeln.[27]

  Das standardmäßig installierte Betriebssystem PureOS ist allerdings vernachlässigt. Es ist empfehlenswert, statt PureOS das gut gepflegte QubesOS zu installieren. Purism-Laptops sind voll kompatibel mit QubesOS 4.0. Das wäre eine ideale Kombination von Hardware und Software für hohe Sicherheitsanforderungen.[28]

20.3.2 Boot-Medium für die Linux Installation oder Live-DVD erstellen

Wenn man das ISO-Image für die Installation einer Linux-Distribution oder das Image eines Live-Systems wie TAILS oder ShredOS heruntergeladen hat, muss man daraus irgendwie ein Bootmedium für den Computer erstellen. Man hat die Wahl zwischen einer DVD oder einem USB-Stick.

Wenn man noch ein DVD-RW Laufwerk und eine beschreibbare DVD hat, dann könnte man das ISO-Image auf die DVD brennen und nach dem Neustart von der DVD booten.

Praktischer ist es, einen USB-Stick zu nutzen. Man schiebt das ISO Image auf den USB-Stick. Dabei gehen zwar alle Daten auf dem Stick verloren, aber man kann den USB-Stick danach neu formatieren und wieder als Datenträger verwenden.

- Für Windows gibt es den *Win32 Disk Imager*. (Vorsicht bei werbeverseuchten Downloads von Chip.de u. Ä.) Die Bedienung ist simpel. Das ISO-Image und den gewünschten USB-Stick wählen und auf den Button *Schreiben* klicken (Abb. 20.3).

[26] https://puri.sm/posts/the-librem-key-makes-tamper-detection-easy/
[27] https://puri.sm/learn/hardware-kill-switches/
[28] https://puri.sm/posts/qubes4-fully-working-on-librem-laptops

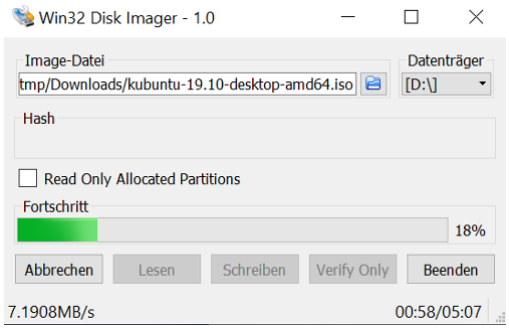


Abbildung 20.3: Win32 Disk Imager

- Linuxer können *gnome-disk* oder Disks verwenden. Falls das Tool nicht vorhanden ist, installiert man das Paket *gnome-disk-utility*. In der linken Sidebar des Hauptfensters wählt man zuerst den USB-Stick und dann im Disk-Menü den Menüpunkt *Restore Disk Image*. Man sollte nochmals prüfen, dass man WIRKLICH den USB-Stick gewählt hat, sonst zerstört man evtl. das System!!!

  Einige Distributionen bringen auch kleine, spezielle Tools mit, um bootfähige USB-Sticks zu erstellen. Man findet sie in der Regel in der Programmgruppe *System*.

- Liebhaber der Kommandozeile verwenden unter Linux gern *dd* (disk doubler), um ISO-Images auf USB-Sticks zu kopieren. Nach dem Anschließen des USB-Sticks benötigt man die Device-Kennung, die man quick and dirty mit *ls* ermitteln kann. Üblicherweise ist der zuletzt angeschlossene USB-Stick das letzte Device in der Liste.

  ```
  > ls /dev/sd?
  /dev/sda /dev/sdb /dev/sdc
  ```

  Dann schiebt man als root mit dd das ISO-Image auf den USB-Stick. Dabei werden alle(!) Daten und Partitionen auf dem Stick gelöscht.

  ```
  > sudo dd if=debian-live.iso of=/dev/sdc status=progress
  ```

20.4 NetBSD und OpenBSD

Diese beiden BSDs sind konsequent und ohne Kompromisse hinsichtlich Benutzbarkeit auf Sicherheit (OpenBSD) bzw. Portierbarkeit (NetBSD) optimiert. Wenn man mehrere Jahre Erfahrung mit einem UNIX-artigen System (z. B. Linux) gesammelt hat und hinreichend leidensfähig ist, dann kann man auch diese beiden Betriebssysteme einsetzen und sich an den Vorteilen erfreuen.

Die Optimierung auf Sicherheit gilt nur für das Betriebssystem, nicht für Anwendungen oder zusätzliche Bibliotheken. Gelegentlich werden Sicherheitsfeatures von Bibliotheken wie z. B. OpenSSL unterlaufen, denen das sichere Allozieren von Speicher bei NetBSD und OpenBSD zu langsam war und deren eigene Implementierung dann zum Heartbleed-Bug führte.

Anwendungen wie X11, Mozilla Firefox oder Thunderbird lassen sich in NetBSD nur installieren, wenn man in der Datei */etc/mk.conf* folgende Option setzt:

```
ALLOW_VULNERABLE_PACKAGES=yes
```

20.5 Risiko USB, Firewire und Thunderbolt

Die Nutzung der **USB**-Schnittstellen ist weit verbreitet und bedenkenlos werden Speichermedien (USB-Sticks oder USB-Festplatten), Kameras, Smartphones, Drucker und andere Peripheriegeräte an den Computer oder Laptop angeschlossen. Zunehmend wird die USB-Schnittstelle auch zum Aufladen von Geräten genutzt, die eigentlich keine Funktion in Zusammenhang mit dem Computer erfüllen.

Sogenannte BadUSB-Devices müssen kaum Sicherheitshürden überwinden und auch keine 0-Day-Exploits einsetzen. Sie können die vielfältigen technischen Features neu kombinieren, um unschöne Dinge anzustellen. USB-Geräte (z. B. USB-Sticks von Fremden) können neben der sichtbaren Funktion (z. B. als Speichermedium) weitere verdeckte Funktionen enthalten, die man nicht bemerkt. Sie können sich heimlich als USB-Tastatur ausgeben und Kommandos senden oder sich als Netzwerkkarten ausgeben und Daten umleiten.

- Auf der Blackhat 2014 haben K. Nohl und J. Lell von SRLabs in ihrem Vortrag *BadUSB – On Accessories that Turn Evil*[29] gezeigt, wie der Internet-Traffic für bestimmte Webseiten umgeleitet wird, ohne dass der User etwas merkt. Wenn man es einmal ausprobieren möchte, kann man sich das Script BadAndroid-v0.1.zip von SRLabs herunterladen. Das Archiv enthält eine README und ein Script, welches man auf ein gerootetes Android-Smartphone kopiert und dort startet. Dann schließt man das Smartphone an einen Computer an (Windows oder Linux) und ... eine nette Demo.
- Im November 2016 hat Samy Kamkar mit PoisonTap[30] ein weiteres BadUSB-Device vorgestellt. Wenn der Angreifer physischen Zugang zu einem Computer oder Laptop mit aktiviertem Passwortschutz hat (z. B. durch Bildschirmschoner) und auf dem Rechner noch ein Browser geöffnet ist, dann kann PoisonTab mit einigen kleinen Tricks die Online-Accounts (E-Mail, Twitter, Facebook usw.) des Targets übernehmen, die mit diesem Browser genutzt wurden. Der Angreifer muss nur *PoisonTab* am USB-Port anschließen und warten.
- Für interessierte Hacker gibt es getarnte BadUSB-Sticks zu kaufen, bei denen zahlreiche Schadfunktionen kombiniert oder selbst programmiert werden können. Bekannte Spielzeuge dieser Art sind MalDuino, Rubber Ducky, Teensy, USBNinja, Digispark oder Bash Bunny. Oft wird von diesen Geräten eine Tastatur simuliert, die nach dem Einstecken programmierte Tastensequenzen abfeuert. T. Scheible hat darüber eine nette Artikelserie geschrieben.[31]

Ein besonderes Risiko sind USB-Sticks oder USB-Festplatten, die man bedenkenlos an unterschiedlichen Computern in verschiedenen Netzen nutzt. Einige spektakuläre Beispiele aus den Medien zeigen, dass es im Cyberwar üblich ist, Malware auf einem USB-Stick in schwer zugängliche Netze zu transportieren. Dabei kann der USB-Stick extra präpariert werden oder man greift die schlecht gesicherten Rechner mehrerer Targets zuhause an und hofft, dass der Trojaner von einem Wirt in das gesicherte Netzwerk getragen wird.

- 2008 wurde ein niedlicher USB-Stick auf einer US-Militärbasis in Nahost platziert. Eine Knallcharge steckte den Stick in seinen Computer und infizierte das gesamte Kommunikationssystem des US-Militärs (klassifizierte und nicht klassifizierte Netzwerke) mit dem russischen Trojaner *agent.bz*. Es dauerte 14 Monate und kostete mehrere Mio. Dollar, die Netzwerke zu säubern.

[29] https://www.youtube.com/watch?v=nuruzFqMgIw
[30] https://www.schneier.com/blog/archives/2016/11/hacking_passwor.html
[31] https://scheible.it/rubber-ducky-badusb/

- *Stuxnet* wurde von einem Mossad-Agenten mit einem USB-Stick in die Uranaufbereitungsanlage im Iran gebracht.
- *Regin* ist ein hochentwickelter Spionage-Trojaner der NSA. Dieser Trojaner konnte 2014 ins Bundeskanzleramt gelangen und dann dort seine Aufgaben ausführen, weil eine Mitarbeiterin dienstliche Dokumente zuhause auf dem infizierten PC bearbeitete und mit dem USB-Stick ins Bundeskanzleramt brachte.

Bei **Firewire**(IEEE 1394)- und **Thunderbolt**-Schnittstellen ist das Risiko noch größer. Im Gegensatz zu USB wird bei diesen Schnittstellen keine Master-Slave-Kommunikation genutzt. Über Firewire und Thunderbolt haben angeschlossene Geräte via DMA (Direct Memory Access) vollen Zugriff auf den Hauptspeicher des PC und können z. B. eine Kopie auslesen.

- 2008 wurde demonstriert, wie man den Windows-Login mit einem Firewire-Gerät umgehen kann. Microsoft sah keinen Handlungsbedarf, da die Funktionalität der Firewire-Spezifikation entspricht. Es ist also kein Bug sondern ein Feature.
- Gegen Apples I/O-Technik Thunderbolt gab es von Anfang an Sicherheitsbedenken[32]. Dokumente von HBGary belegen, dass US-Behörden schon 2011 ein Framework nutzten, um Trojaner via Thunderbolt auf PCs und Laptops zu installieren.
- Die Datenverschlüsselung kann umgangen werden (für alle Produkte), da Keys aus dem Hauptspeicher ausgelesen werden können. Geheimdienste nutzen passende Tools routiniert, wenn sie physischen Zugriff auf den Zielrechner haben.

Hinweise zur Verbesserung der Sicherheit

1. Ein USB-Stick, der an einen unbekannten Computer angeschlossen wurde, oder ein USB-Stick von Dritten ist als potentiell verseucht zu betrachten. Man kann das Risiko verringern, wenn man eine Live-DVD nutzt.
2. Um Daten von USB-Sticks zu bearbeiten oder Fotos von der Digicam auf einer USB-Festplatte zu archivieren, kann man eine Live-DVD nutzen. Insbesondere sollte man eine Live-DVD nutzen, wenn man Daten aus der Firma zuhause bearbeiten und wieder mit in die Firma nehmen will.
3. Zum Aufladen von Geräten kann man USB-Ladegeräte nutzen. Man muss nicht alles, was wie ein USB-Stecker aussieht, in den Computer einführen. Das BSI warnt davor, E-Zigaretten via USB-Anschluss am Computer aufzuladen, und rät zu einem USB-Ladegerät, da einige chinesische Produkte im Hintergrund Malware installieren.[33]
4. *USBGuard* für Linux[34] zeigt dem Nutzer an, welcher Gerätetyp angeschlossen wird. Man kann dann das Gerät zulassen oder blockieren, noch bevor das zugehörige Modul des Linux-Kernels das Gerät anspricht und eine Verbindung aufbaut. Auch dauerhaftes Zulassen/Blockieren nach Geräteklasse oder ID kann konfiguriert werden.
5. Es gibt zahlreiche Freeware-Tools, um USB-Schnittstellen unter Windows zu sperren. (z. B. den USB-Blocker[35] von securityXploded.com)

[32] https://heise.de/-1198049
[33] https://heise.de/-3222811
[34] https://dkopecek.github.io/usbguard/
[35] http://securityxploded.com/windows-usb-blocker.php

6. Wenn man Firewire nicht nutzt, sollte man alle Firewire-Schnittstellen deaktivieren.

   - Für Windows stellt MS einen Support-Artikel bereit: *Blockieren des SBP-2-Treibers und des Thunderbolt-Controllers, um Bedrohungen für BitLocker zu reduzieren.*[36]
   - Unter Linux kann man prüfen, ob das System Firewire-Schnittstellen beim Booten erkannt hat:

     ```
     > lspci | grep -i Firewire
     ```

     Wenn der Rechner Firewire-Schnittstellen hat, dann kann man die Kernel-Module für diese Schnittstellen sperren. Man speichert eine Datei *firewire.conf* im Verzeichnis */etc/modprobe.d/* mit folgendem Inhalt:

     ```
     blacklist firewire-ohci
     blacklist firewire-sbp2
     ```

     Danach führt man folgende Kommandos aus:

     ```
     > sudo depmod -ae
     > sudo update-initramfs -u
     ```

USBGuard für Linux

USBGuard für reglementiert die Nutzung von USB-Geräten. Es dürfen nur USB-Geräte genutzt werden, die in einer Whiteliste freigegeben wurden. Alle anderen USB-Spielzeuge werden blockiert. Das Tool ist in allen aktuellen Linux Distributionen enthalten und kann mit dem bevorzugten Paketmanager installiert werden:

```
Debian: > sudo apt install usbguard
Fedora: > sudo dnf install usbguard
```

Nach der Installation muss man einen initialen Regelsatz erzeugen, der zumindest eine via USB angeschlossene Tastatur und Maus freigibt (sonst sperrt man sich aus). Es ist sinnvoll, auch weitere USB-Geräte anzuschließen, die man später nutzen möchte (Backup USB-Stick oder -Festplatte, Nitrokey usw.). Dann kann man mit folgendem Kommando die initiale Konfiguration erstellen, die alle angeschlossenen Geräte erlaubt und den Rest sperrt:

```
> sudo usbguard generate-policy > rules.conf
```

Die erstellte Konfiguration muss man dann in das Konfigurationsverzeichnis */etc/usbguard* kopieren und sichere Zugriffsrechte für die Datei setzen:

```
> sudo cp rules.conf /etc/usbguard/rules.conf
> sudo chmod 0600 /etc/usbguard/rules.conf
```

In der Konfiguration */etc/usbguard/usbguard-daemon.conf* sind kleine Anpassungen empfehlenswert, bevor man USBGuard verwendet:

[36] https://support.microsoft.com/kb/2516445/de

- Mit strengen Regeln wird sichergestellt, dass alle Regeln auch für USB Spielzeuge angewendet, die bereits vor dem Booten angeschlossen wurden:

  ```
  PresentDevicePolicy     = apply-policy
  PresentControllerPolicy = apply-policy
  ```

- Es kann allerdings vorkommen, dass man eine kaputte Tastatur mal austauschen muss. Mit strengen Regeln hat man sich dann ausgesperrt. Als etwas lockere Variante kann man alle Geräte zulassen, die beim Bootes des Rechners angeschlossen sind:

  ```
  PresentDevicePolicy     = allow
  PresentControllerPolicy = apply-policy
  ```

  Gegen *Evil Maid* Angriffe (jemand bootet den Rechner in Abwesenheit des Besitzers und nutzt ein BadUSB Device), schützt eine vollständige Verschlüsselung der Festplatte. Somit ist das Risiko durch etwas lockere Einstellungen überschaubar.

Danach kann man den USBGuard Daemon starten und für zukünftige Reboots aktivieren:

```
> systemctl start usbguard
> systemctl enable usbguard
```

Alle unbekannten USB-Geräte werden zukünftig blockiert. Wenn man ein ein neues USB-Spielzeug verwenden möchte, kann man es im Terminal freigeben. Dafür schließt man das Gerät an und lässt sich alle vorhandenen USB-Geräte anzeigen:

```
> sudo usbguard list-devices
...
29: block id 20a0:4107 serial "" name "Crypto Stick v1.2" hash "li65uJm8....
```

Die Nummer am Anfang der Zeile ist die ID, mit der man das Gerät freigeben kann:

```
> sudo usbguard allow-device 29
```

Wenn man das USB Spielzeug öfters verwenden möchte, kann man es dauerhaft freigeben, indem man die Option –permanent bzw. -p hinzufügt. Die Regel wird dann in die Datei */etc/usbguard/rules.conf* eingetragen:

```
> sudo usbguard allow-device --permanent 29
```

Mit dem folgenden Kommado kann man eine Freigabe widerrufen, solange das USB Spielzeug noch angeschlossen ist:

```
> sudo usbguard allow-device --permanent 29
```

Wenn man eine permanente Freigabe löschen möchte und das USB Spielzeug nicht angeschlossen ist, kann man sich die Regeln anschauen und die Regel löschen:

```
> sudo usbguard list-rules
...
> sudo usbguard remove-rule <ID>
```

Die umständliche Freigabe von unbekannten USB-Geräten auf der Kommandozeile und nur für den administrativen User ist etwas umständlich aber auch ein Sicherheitsfeature. Wer es etwas weniger streng haben möchte, kann auch anderen Nutzern die Modifikation der Regeln erlauben. Dafür ist folgende Option in der Konfigurationsdatei */etc/usbguard/usbguard-daemon.conf* anzupassen:

```
IPCAllowedUsers = root username1 username2 ...
```

Die in der Liste genannten User können das Kommando usbguard wie beschrieben nutzen, um neue USB-Geräte zu erlauben oder Freigaben aufzuheben.

20.6 Linux Firewall konfigurieren

Es gibt sicherheitsorientierte Linux Distributionen wie RHEL oder QubesOS, die standardmäßig eine Firewall und ein GUI zur Konfiguration installieren, welche erstmal alle Verbindungsversuche von außen blockiert. Viele Mainstream Distributionen wie Ubuntu(s), Linux Mint, ARCH Linux oder Manjaro/KDE verzichten bei der Standardinstallation auf eine Firewall oder aktivieren sie nicht automatisch nach der Installation.

20.6.1 Uncomplicated Firewall (UFW)

UFW ist eine einfach zu konfigurierende Firewall für Debian, Ubuntu(s), Linux Mint, ARCH Linux oder Manjaro, die man schnell installieren und in Betrieb nehmen kann. Linux Mint und Manjaro installieren die Firewall standardmäßig aber aktivieren sie nicht automatisch. In Debian und Ubuntu(s) erledigt man die Installation mit dem Kommando:

```
> sudo apt install ufw
```

Nachdem UFW installiert wurde, muss man die Firewall noch aktivieren:

```
> sudo ufw enable
```

Das Ergebnis ist eine Firewall, die alle Verbindungsversuche von außen blockiert aber für lokale Programme ist die Kommunikation nach außen ermöglicht. Für viele Anwender ist das wahrscheinlich ausreichend. Anpassungen sind möglich.

Man kann einzelne Dienste freischalten, die von außen erreichbar sein sollen:

```
> sudo ufw allow ssh
```

Das Löschen der Freigabe erfolgt, indem man ein *delete* einfügt:

```
> sudo ufw delete allow ssh
```

Die Liste der vordefinierten Dienste kann man sich mit folgendem Kommando anschauen:

```
> sudo ufw app list
```

Wenn keine passenden vordefinierten Dienste vorhanden sind, kann man auch Ports angeben. Für den I2P Router kann man bspw. den Port 8888 freischalten. Die Liste der vordefinierten Dienste kann man sich mit folgendem Kommando anschauen:

```
> sudo ufw allow 8888
```

Man kann einzelne Dienst wie CUPS nur für das lokale Netzwerk freigeben:

```
> sudo ufw allow proto tcp port 6331 from 192.168.1.0/24
```

Man kann ausgehende Protokolle sperren, die man nicht nutzen möchte:

```
> sudo ufw reject out telnet comment "Telnet ist unverschlüsselt"
```

Oder man könnte auch sehr restriktiv vorgehen, standardmäßig alle ausgehenden Dienste sperren und dann nur für einzelne Protokolle die Kommunikation nach außen erlauben:

```
> sudo ufw default reject outgoing
> sudo ufw allow out http
> sudo ufw allow out https
...
> sudo ufw allow out from any to X.X.X.X port 53
> sudo ufw allow out from any to Y.Y.Y.Y port 53
```

DNS Traffic sollte man nicht vergessen. Man kann mehrere DNS Server angeben.

Hinweis: Wenn man auch den HTTP Traffic blockiert und nur HTTPS erlauben möchte, dann sollte man im Browser den HTTPS-only-Mode aktivieren und die Validierung von TLS-Zertifikaten via OCSP-Server deaktivieren, um Problem zu vermeiden.

Den Status der Firewall kann man mit folgendem Kommando prüfen:

```
> sudo ufw status verbose
```

Es gibt ein grafisches Frontend GUFW, dass man mit dem bevorzugten Paketmanager installiert, wenn es noch nicht vorhanden ist, unter Debian/Ubuntu mit:

```
> sudo apt install gufw
```

GUFW kann mehrere Profile verwalten, wenn man auf dem Laptop zuhause andere Einstellungen verwenden möchte als unterwegs. Das Hinzufügen von Regeln ist einfach möglich, auch wenn die Regeln ein bisschen komplizierter sind.

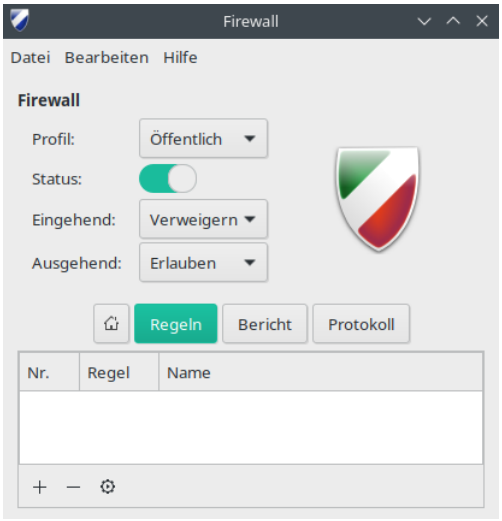


Abbildung 20.4: GUFW Hauptfenster

20.6.2 RHEL/Fedora firewalld

Bei RHEL und Fedora wird standardmäßig der *firewalld* installiert und kann als Systemdienst wie üblich gestartet, gestoppt, aktiviert und deaktiviert werden:

```
> sudo systemctl start|stop|enable|disable firewalld
```

firewalld unterscheidet zwischen verschiedenen Zonen. Den Zonen werden Netzwerkschnittstellen zugeordnet (ein Thema für IP-Profis). Standardmäßig gehören alle Netzwerkinterfaces zur Zone *public* und alle Kommandos ohne Angaben einer Zone werden auf *public* angewendet.

- Die Standardkonfiguration für die Zone *public* ist, dass alles blockiert wird, was von draußen rein will. Freigaben für bestimmte Services und Ports sind aber konfigurierbar.
- Die Standardkonfiguration für die Zone *Fedora Workstation* erlaubt eingehende Verbindungen von außen auf den nicht-priveligierten Ports > 1024.
- Wenn man keine Freigaben braucht, könnte man die Default Zone auf *drop* setzen:

  ```
  > sudo firewall-cmd --set-default-zone drop
  ```

firewalld unterscheidet zwischen einer temporären Runtime Konfiguration und einer permanenten Konfiguration. In der Runtime Konfiguration kann man die Firewall konfigurieren und testen.

- HTTPS Port für Incoming Traffic für die Zone *public* öffnen (Runtime):

  ```
  > sudo firewall-cmd --add-service=https
  ```

  Alternativ kann man auch Port + Protokoll angeben, wenn kein Service definiert ist:

  ```
  > sudo firewall-cmd --add-port=80/tcp
  ```

- ... oder alles wieder schließen:

```
> sudo firewall-cmd --remove-service=https
> sudo firewall-cmd --remove-port=80/tcp
```

- Etwas komplizierter wird es, wenn man einen lokalen Dienst (z. B. CUPS) nur für Rechner aus dem lokalen Netzwerk freigeben möchte:

```
> sudo firewall-cmd --add-rich-rule 'rule family="IPv4" source
↪  address="192.168.178.0/24" service name="cups" accept'
```

- Wenn alles getestet ist, speichert man die Runtime Konfiguration permanent:

```
> sudo firewall-cmd --runtime-to-permanent
```

- Eine Übersicht über alle aktiven Regeln erhält man mit dem Kommando:

```
> sudo firewall-cmd --list-all
```

Standardmäßig dürfen alle Programme die Firewallregeln ändern, die mit root Rechten laufen. Für Heimanwender ist das Ok. Für hohe Sicherheitsanforderungen kann man den Download Mode aktivieren. Dann dürfen nur Programme aus einer Whitelist die Firewallregeln modifizieren. Wenn die Whitelist leer ist, können keine Veränderungen an der Firewall vorgenommen werden. Den Lockdown Mode aktiviert und deaktiviert man mit folgenden Kommandos:

```
> sudo firewall-cmd --lockdown-on
> sudo firewall-cmd --lockdown-off
```

Die Konfiguration einer Lockdown Whitelist ist aber eher ein Thema für IT-Profis.

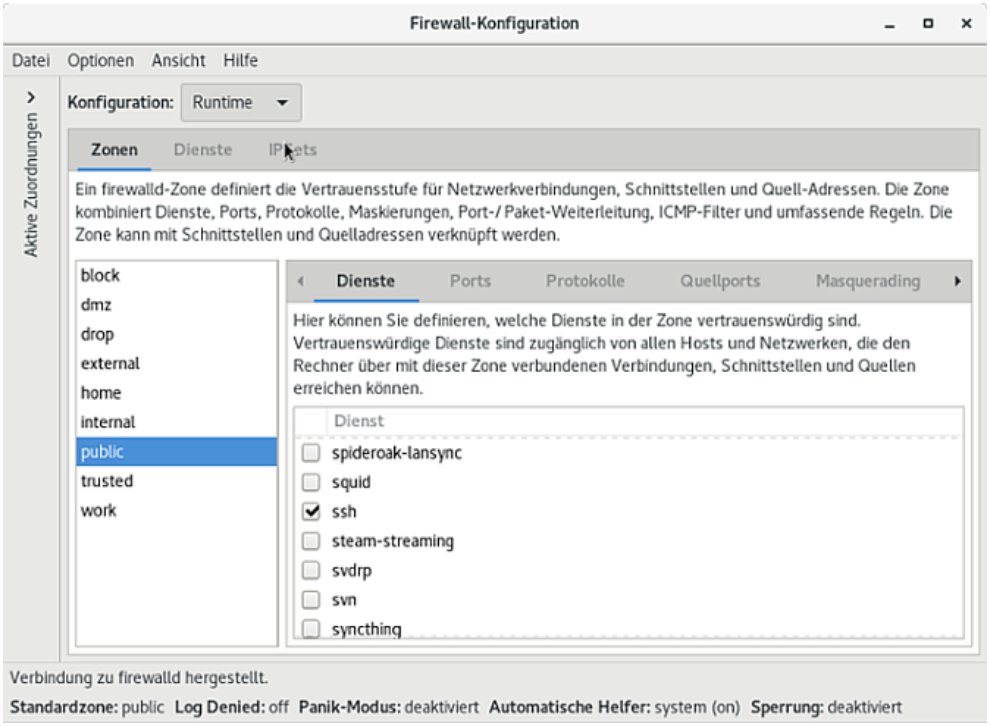


Abbildung 20.5: RedHat/Fedora Firewall Konfigurator GUI

20.6.3 QubesOS Firewall

QubesOS enthält standardmäßig eine Firewall, die in einer eigenen VM läuft. In der Default Konfiguration können die Dienste in den Arbeits-VMs nicht erreicht werden aber aus den Arbeits-VMs heraus sind alle Verbindungen möglich.

In den Einstellungen zu jeder einzelnen VM kann man den Datenverkehr komplett blockieren, indem man Networking deaktiviert. Außerdem kann man restriktivere Firewall Einstellungen anwenden, indem man nur für bestimmte Protokolle ausgehende Verbindungen zulässt (Abb. 20.6).

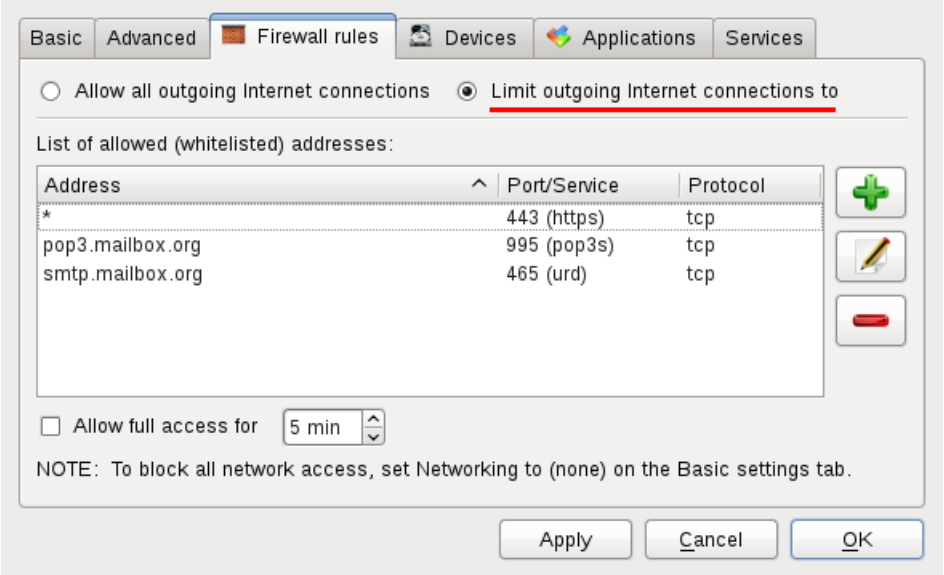


Abbildung 20.6: QubesOS: Firewall Konfiguration einer VM

20.7 WLAN Privacy Leaks

Wenn man mit dem Laptop unterwegs ist und WLANs in Internet Cafe's, am Flughafen, in der Firma oder im Hotel nutzt, dann bekommt man die Netzwerkkonfiguration (eigene IP-Adresse, DNS-Server...) via DHCP-Protokoll zugeteilt. Damit hinterlässt man auf dem DHCP-Server Spuren, die C. Huitema von der IETF in der Studie *Unique Identifiers in DHCP options enable device tracking*[37] zusammengefasst hat:

1. Die MAC-Adresse wird an den DHCP-Server übermittelt und ist eine weltweit eindeutige Kennung für die Hardware des Rechners (Netzwerkschnittstelle oder WLAN-Modul).

   - In IPv4 Netzen wird diese Kennung nur bis zum Router/Gateway übertragen. Im eigenen Home-Netz braucht man sich also keine Gedanken machen, aber in fremden WLANs (Hotel, Internetcafe', Flughafen) ist davon auszugehen, dass die MAC-Adressen der Nutzer protokolliert werden.
   - In IPv6 Netzen wird die MAC-Adresse Bestandteil der IP-Adresse, wenn die *Privacy Extension for IPv6* nicht aktiviert wurde. Damit wird die IP-Adresse zu einem personenbezogenen Merkmal und kann zur Wiedererkennung und zum Tracking genutzt werden.

[37] https://tools.ietf.org/html/draft-huitema-perpass-dhcp-identifiers-00

2. Die UUID/GUID des Intel Preboot eXecution Environment (PXE) wird an den DHCP-Server übermittelt, wenn PXE in den BIOS Einstellungen aktiv ist. PXE kann im BIOS deaktiviert werden.

3. Der konfigurierte Hostname und die DNS-Domain des Rechners wird an den DHCP-Server übermittelt.

Wenn man die automatische Anmeldung für die bevorzugte WLANs aktiviert hat, dann sendet der Laptop unterwegs (am Flughafen, im Hotel, in der U-Bahn...) ständig sogenannte *Probes*, um die Umgebung nach den bevorzugten WLANs zu scannen.

- Die *Probes* haben einen eindeutigen Fingerprint und können in gleicher Weise wie MAC-Adressen für das Tracking der Geräte verwendet werden, wie die Studie *Why MAC Address Randomization is not Enough* demonstrierte.[38]

- Mit den *Probes* auch eine Liste der bevorzugten WLANs gesendet, mit denen sich der Laptop automatisch verbinden würde (Prefered Network List, PNL). Diese Prefered Network List liefert Informationen über Orte, an denen sich der Besitzer des Laptops aufgehalten hat.

- Bei offenen WLANs ergibt sich ein weiteres Sicherheitsrisiko. Wenn man sich einmal mit einem offenen WLAN ohne Passwortschutz verbunden hat, wird die Verbindung in der Regel mit der Option *Automatisch verbinden wenn verfügbar* gespeichert.

  Ein Angreifer kann die *Probes* auswerten, die ein Laptop bei der Suche nach WLANs in der Umgebung sendet. Wenn er dabei die SSID eines bekannten, offenen WLANs findet, kann er mit einem Fake Hotspot diese SSID simulieren und der Laptop wird sich automatisch mit diesem WLAN verbinden. Damit sitzt der Angreifer in der Man-in-the-Middle-Position und könnte den Datenverkehr mitlesen und mit einigem Aufwand auch TLS Verbindungen angreifen.

  Die Security Firma Sensepost mit der Drohne Snoopy ein Gerät vorgestellt, das diesen Angriff automatisiert. In einer Demonstration wurde gezeigt, wie Snoopy die Login Credentials für PayPal, Yahoo! usw. abgreifen konnte.[39]

Um keine eindeutigen Spuren als Road-Warrior in Internet Cafe's oder am Flughafen zu hinterlassen, kann man die MAC-Adresse faken, automatische Anmeldung für alle WLANs deaktivieren, PXE Boot im BIOS des Rechners deaktivieren und nichtssagenden Hostnamen und DNS-Domain nutzen.

20.7.1 MAC-Adresse faken (Windows 10)

Windows 10 enthält alles, was man braucht, um die MAC-Adressen für WLAN-Verbindungen zu faken. Bevor(!) man sich unterwegs im Hotel, am Flughafen oder in der Berliner U-Bahn mit einem neuen WLAN verbindet, kann man die Randomisierung der MAC-Adresse aktivieren. Die Einstellungen werden alle in der Sektion *Netzwerk und Internet* auf dem Reiter *Wi-Fi* vorgenommen, siehe Bild 20.7.

1. Als erstes muss man unter *Manage Wi-Fi settings* die Randomisierung der MAC Adressen global einschalten, damit diese Funktion danach für einzelne WLANs konfiguriert werden kann. Außerdem wird immer eine zufällige MAC-Adresse für den Scan nach WLANs verwendet, wenn die Randomisierung global aktiviert wurde.

[38] http://papers.mathyvanhoef.com/asiaccs2016.pdf
[39] https://www.golem.de/news/drohne-snoopy-schnueffelt-im-vorbeiflug-1403-105329.html

2. Danach muss man das WLAN-Netzwerk wählen und unter *Advanced Options* für jedes Netzwerk einzeln den Modus für den Fake der MAC-Adresse auswählen. Man kann täglich eine neue MAC-Adresse generieren lassen oder den gleichen Fake immer wieder nutzen. Das ist z. B. für Wi-Fi Hotspots in Hotels sinnvoll, bei denen man für mehrere Tage bezahlt hat, oder wenn der Zugang zu einem Firmen-WLAN anhand der MAC-Adressen limitiert wird.

3. Die Option *automatisch Verbinden* sollte man für alle WLANs deaktivieren. Wenn die Option für ein oder mehrere WLAN Verbindungen aktiviert wurde, dann sendet der Rechner ständig sogenannte *Probes*, um aktiv nach diesen WLANs in der Umgebung zu suchen. Die *Probes* haben einen eindeutigen Fingerprint und können in gleicher Weise wie MAC-Adressen für das Tracking der Geräte verwendet werden.

4. Dann kann man sich mit dem WLAN verbinden.

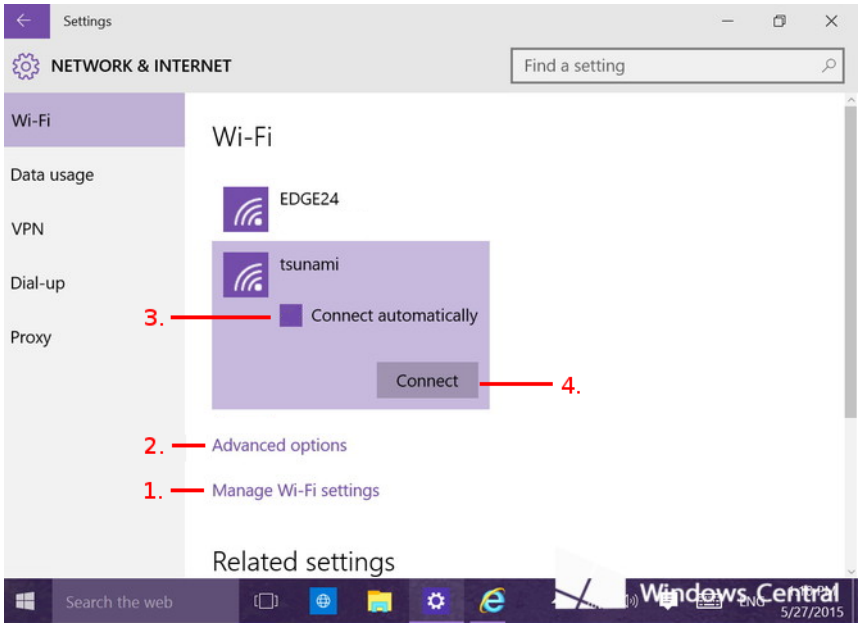


Abbildung 20.7: MAC-Adresse faken für Windows 10

20.7.2 MAC-Adresse faken (Linux)

Die MAC-Adresse ist eine weltweit eindeutige Kennung für jede Netzwerkschnittstelle. Jede Netzwerkkarte und jedes WLAN-Modul hat eine eigene, eindeutige Kennung. Wer oft mit dem Laptop unterwegs unterwegs ist, hinterlässt damit in allen WLANs eine eindeutige Spur.

Der NetworkManager enthält alle notwendigen Features, von WLAN Schnittstellen oder LAN Interfaces zu ändern (MAC Spoofing). Zusätzliche Tools sind nicht nötig.

Beim Verbindungsaufbau verwendet der Networkmanger standardmäßig die echte MAC-Adresse. In der Konfigurationsdate vom NetworkManager (*/etc/NetworkManager/NetworkManager.conf*) kann man das Standardverhalten in der Sektion [connection] anpassen. Oder man erstellt eine zus. Konfigurationsdatei *50-macchange.con* im Verzeichnis */etc/NetworkManager/conf.d/*.

Das MAC Spoofing für zukünftig erstellte Verbindungen aktiviert man mit folgenden Optionen:

```
[connection]
ethernet.cloned-mac-address=random
wifi.cloned-mac-address=stable
```

Für die Generierung der Fake MAC-Adressen gibt es folgende Möglichkeiten:

- **preserve:** die MAC Addresse wird nicht verändert, also kein Fake. (Default)
- **random:** es wird bei jedem Verbindungsaufbau eine neue Fake Adresse generiert. Diese Einstellung ist für WLANs mit vielen räumlich verteilten Access Points sinnvoll (WIFIonICE, HOTSPLOTS o.ä.), um an unterschiedlichen Orten nicht wiedererkannt zu werden.
- **stable:** es wird für ein WLAN immer der gleiche Fake verwendet aber für verschiedene WLANs unterschiedliche Fake Adressen. Das erleichtert meist den Login in bekannten Wi-Fi Hotspots, beispielsweise wenn man in einem Hotel immer die gleiche MAC Adresse verwenden muss. Es verhindert aber die Wiedererkennung anhand der MAC-Addr. in anderen WLANs.

In den Netzwerkeinstellungen kann man den Fake Mode anpassen und die *Duplizierte Adresse* vom oben konfigurierten Standardwert *stable* auf *random* setzen (Abb. 20.8).

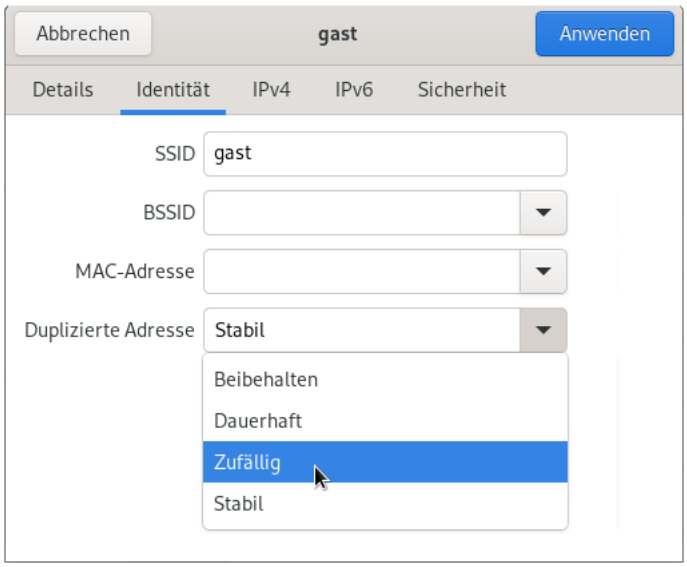


Abbildung 20.8: Fake Mode für MAC Adresse im NetworkManager anpassen

Man kann die Fake Methode für ein WLAN auch individuell auf der Kommandozeile anpassen. Das erste Kommando zeigt eine Liste der Netzwerke an und das zweite Kommando ändert die Fake Methode für das WLAN mit dem Namen WIFIonICE auf *random*:

```
> nmcli connection show
...
> nmcli connection modify "WIFIonICE" wifi.cloned-mac-address random
```

Scannen nach WLAN Access Points in der Umgebung

Aktuelle Versionen des NetworkManager scannen standardmäßig nach verfügbaren WLANs und senden dafür leere *Probe Request* ohne die SSIDs der bekannten Netzwerke.

Damit gibt es keine Probleme für die Privatsphäre durch *Probes*, die die Prefered Network List (PNL) verraten könnten. Außerdem werden standardmäßig randomisierte MAC Adressen für das Scannen nach WLAN Access Points genutzt. Warnungen zu dem Thema sind out-of-date.

Einzige Ausnahme: Wenn man ein verstecktes WLAN (ein *Hidden WiFi*) konfiguriert hat, werden *Probes* mit der SSID des WLANs gesendet, um das verstecktes WLAN zu einer Antwort zu überreden. Versteckte WLANs zu nutzen, ist aber keine gute Idee, wie T. Haller (Hauptentwickler des NetworkManagers) betont, weil es negative Implikationen für die Privatsphäre hat.

Hostname konfigurieren

Der Hostname eines Rechners kann bei der Installation des Betriebssystems festgelegt oder nachträglich geändert werden. Es gibt keine wirklich anonyme Empfehlung für diese Werte. Wir empfehlen den folgenden nichts aussagenden Wert: **host**.

Wenn man eine Linux Distribution mit *systemd* verwendet, kann man den Hostnamen nachträglich mit folgendem Kommando ändern:

```
> sudo hostnamectl set-hostname host
```

Bei Distributionen ohne *systemd* schreibt man den Hostnamen in die Datei */etc/hostname* und startet den Rechner neu, um die Änderung zu aktivieren.

Es gibt keinen allgemein gültigen Weg, um das Senden des Hostnamens via DHCP zu unterbinden. Die Entwickler der Linux Distributionen haben unterschiedliche Ansichten.

- Debian und Ubuntu senden standardmäßig bei jedem Aufbau einer Netzwerkverbindung via DHCP den Hostnamen an den DHCP-Server in der Hoffnung, dass damit der Rechner via DNS unter diesem Namen einfacher im Netz gefunden werden kann.

  Das kann praktisch sein, wenn man seine NextBox nur einschalten muss und sofort darauf zugreifen kann. Allerdings hinterlässt man damit in WLANs von ICE, Hotels o.ä. eine Spur.

  Der NetworkManager bietet die Möglichkeit, das Senden des Hostnamen für bestimmte Verbindungen nachträglich zu deaktivieren, nach dem die Verbindung angelegt wurde:

  ```
  > nmcli connection modify "WIFIonICE" ipv4.dhcp-send-hostname false
  > nmcli connection modify "WIFIonICE" ipv6.dhcp-send-hostname false
  ```

- Fedora und RedHat senden standardmäßig keinen Hostnamen via DHCP, aber man kann es in der Netzwerkkonfiguration für eine Schnittstelle aktivieren.

- QubesOS und TAILS senden keinen Hostnamen aufgrund der Privacyimplikationen.

Kapitel 21

Smartphones

> *Wenn mir früher jemand gesagt hätte, ich würde freiwillig eine Wanze mit mir herum tragen und sie auch noch selbst aufladen, hätte ich laut gelacht. Heute habe ich ein Smartphone.*

Braucht man das Ding wirklich oder ist es nur ein nettes Lifestyle-Gadget? Für den Berliner Philosophen und Medientheoretiker Byung-Chul Han sind Smartphones das wesentliche Element zur Kontrolle der Bevölkerung im Zeitalter der Psychomacht:

> *Jede Herrschaftstechnik bringt eigene Devotionalien hervor, die zur Unterwerfung eingesetzt werden. Sie materialisieren und stabilisieren die Herrschaft. [...] Das Smartphone ist eine digitale Devotionalie, ja die Devotionalie des Digitalen überhaupt. Es funktioniert wie der Rosenkranz. Beide dienen der Selbstprüfung und Selbstkontrolle. Like ist das digitale Amen. Das Smartphone ist nicht nur ein effizienter Überwachungsapparat, sondern auch ein mobiler Beichtstuhl. Facebook ist die Kirche, die globale Synagoge.*

(Für manche Leute ist es Facebook, für andere Instagram oder Twitter oder etwas Ähnliches – aber immer ist man online und auf der Jagd nach Likes.)

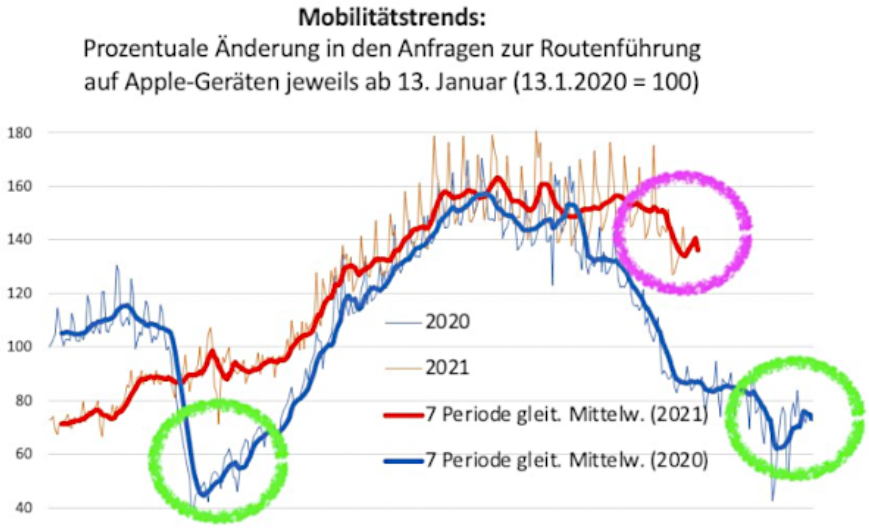
Mit der zunehmenden Verbreitung von Smartphones entstehen neue Gefahren für die Privatsphäre, die deutlich über die Gefahren durch Daten sammelnde Webseiten beim Surfen oder E-Mails-Scannen bei Mail-Providern wie Google hinaus gehen. Da wir die handliche Wanze immer mit uns umhertragen und unterwegs nutzen, ist es möglich, komplexe Bewegungsprofile zu erstellen und uns bei Bedarf zu lokalisieren. Greg Skibiski beschrieb 2009 im Interview mit Technology Review seine Vision von einer Zukunft mit breiter Auswertung der via Smartphone gesammelten Daten wie folgt:

> *Es entsteht ein fast vollständiges Modell. Mit der Beobachtung der Signale kann man ganze Firmen, ganze Städte, eine ganze Gesellschaft röntgen.*

Zehn Jahre später ist die Vision von Greg Skibiski Wirklichkeit. Bewegungsdaten von Smartphones wurden in den Corona-Jahren 2020/21 routiniert verwendet, um die Bevölkerung zu durchleuchten und mehr oder weniger interessante Informationen zu gewinnen:

- Das Statistische Bundesamt analysierte die Veränderungen der Fahrgastzahlen der Deutschen Bahn nicht anhand der Verkäufe von Fahrkarten und Platzkarten (was vielleicht naheliegend wäre) sondern anhand der Bewegungsdaten von Mobiltelefonen. Ergebnis: die Fahrgastzahlen waren 2020 um 50 % niedriger als im Vorjahr.

- Zu Weihnachten und Silvester 2020 führte das Statistische Bundesamt außerplanmäßige Sonderauswertungen der anonymisierten Mobilfunkdaten durch, um die Einhaltung der Corona-Beschränkung durch die Bevölkerung zu prüfen.
  - In Berlin registrierte man am 24.12.2020 eine Reduzierung der Mobilität von 8,4 % und am 26.12.2020 eine Reduzierung von 20 % gegenüber dem Vorjahr. Da Heiligabend überwiegend in der Familie verbracht wird, war die Reduzierung an diesem Tag erwartungsgemäß geringer als am 2. Weihnachtstag.
  - In München und Stuttgart wurde die Einhaltung der Ausgangssperre zu Silvester 2020/21 anhand der Mobilfunkdaten beobachtet. In beiden Städten war die Mobilität in der Silvesternacht um rund 80 % geringer als in den Vorjahren.
- In der vierten Corona-Welle im Herbst 2021 hatten die Menschen die Nase voll von den Reiseeinschränkungen. Die Auswertung der Navigationsanfragen von Apple-iPhones zeigte, dass sich die deutsche Bevölkerung in ihrer Reiselust im November 2021 nur wenig einschränkte.



- Der CSU-Politiker U. Brandl schlug in einem Interview vor, auf die Anonymisierung der Mobilfunkdaten zu verzichten und die Bewegungsdaten aller Bürger der Polizei zur Auswertung und zur Durchsetzung von Ausgangsbeschränkungen zur Verfügung zu stellen, insbesondere um die Einhaltung der 15-km-Regel durchzusetzen.[1]

  Wir müssen einfach mehr Mut haben, dass man die digitalen Möglichkeiten nutzt.

  Den Mut, die digitalen Möglichkeiten zu nutzen, hatte die NSA schon vor 20 Jahren.

Man könnte den braven Bürger simulieren und das Smartphone zuhause lassen, wenn es nicht so schwer fallen würde, für kurze Zeit auf das kleine Gadget zu verzichten.

[1] https://www.br.de/nachrichten/bayern/15-kilometer-regel-brandl-fordert-auswertung-von-handy-daten

21.1 Datensammlungen der Smartphone-Hersteller

Eine Beschreibung der Daten, die von Google und Apple via Smartphones gesammelt werden, liefert die Studie *Measuring The Data iOS and Android Send to Apple And Google* (2021).[2]

iPhones: In Apples Datenschutzbestimmungen räumt sich der Konzern das Recht ein, den Standort des Nutzers laufend an Apple zu senden. Apple wird diese Daten Dritten zur Verfügung stellen. Damit begann 2011 die heute allgegenwärtige Datensammlung im Gerät durch den Smartphone-Hersteller.

Während wir gegen die Vorratsdatenspeicherung bei E-Mails kämpften, übertrugen Apples Mobilgeräte seit iOS Version 8 automatisch die Call History der Telefonanrufe in die Apple Cloud (Telefonnummer, Datum/Uhrzeit, Dauer). Mit iOS Version 10 wurde diese Datensammlung auf Anrufe via Messenger (WhatsApp, Signal usw.) und verschlüsselten VoIP Telefonate (Skype usw.) ausgeweitet, was das Signal Team verärgerte und zu einer Warnung veranlasste.

Die Kommunikationsdaten wurden für 4 Monate im iCloud Konto des Benutzers gespeichert und konnten dort von Behörden abgegriffen und für die Kommunikationsanalyse genutzt werden. Die Firma Elcomsoft bot die nötigen Tools, um diese Daten zu erschließen.

Mit iOS Version 13 wurde die Call History in der iCloud verschlüsselt und seit Version 13.4 wird sie nicht mehr in die iCloud kopiert, was die Schnüffler und Elcomsoft verärgert.[3]

Ein aktuelles iPhone sendet durchschnittlich alle 5min folgende Daten an Apple:

- Telefonnummer und SIM-Kartennummer,
- Gerätenummer (IMEI) und Seriennummer des Gerätes,
- Lokale IP-Adresse und Standortdaten,
- bei WLAN-Verbindung die MAC-Adressen aller Geräte im gleichen WLAN.

Google Android: die tief im System verankerte Google-Play-Service-App sendet alle 20 Minuten folgende Daten an Google:

- Telefonnummer und SIM-Kartennummer,
- Gerätenummer (IMEI) und Seriennummer des Gerätes,
- WLAN-MAC-Adresse und IP-Adresse,
- Andoid-ID (E-Mail-Adresse des Google Kontos),
- Standort (wenn die *Standortverfolgung* aktiv ist).

Die Genauigkeit der Standortverfolgung von Google zeigte das FBI bei Gerichtsverfahren gegen militante Gruppen, die an der Erstürmung des Capitol im Januar 2021 beteiligt waren (Abb. 21.1). Bei dieser Aktion verwendeten einige militante Gruppen Wegwerf-Smartphones für die Kommunikation. Das FBI identifizierte 300+ von diesen Wegwerf-Phones mit anonym gekauften SIM-Karten und verfolgte deren Weg durch das Captitol. Die Identifizierung der Personen erfolgte durch Abgleich mit den Bildern der Videoüberwachung.

Mit Android 10 hat Google für Apps den Zugriff auf eindeutige Hardwarekennungen wie IMEI, SIM, Seriennummer, MAC Adressen usw. allgemein verboten und nur für eine restriktiv gepflegte Liste von Ausnahmen zugelassen. Apps sollen die Werbe-ID für

[2] https://www.scss.tcd.ie/doug.leith/apple_google.pdf
[3] https://blog.elcomsoft.com/2020/04/macos-ios-and-icloud-updates-forensic-consequences

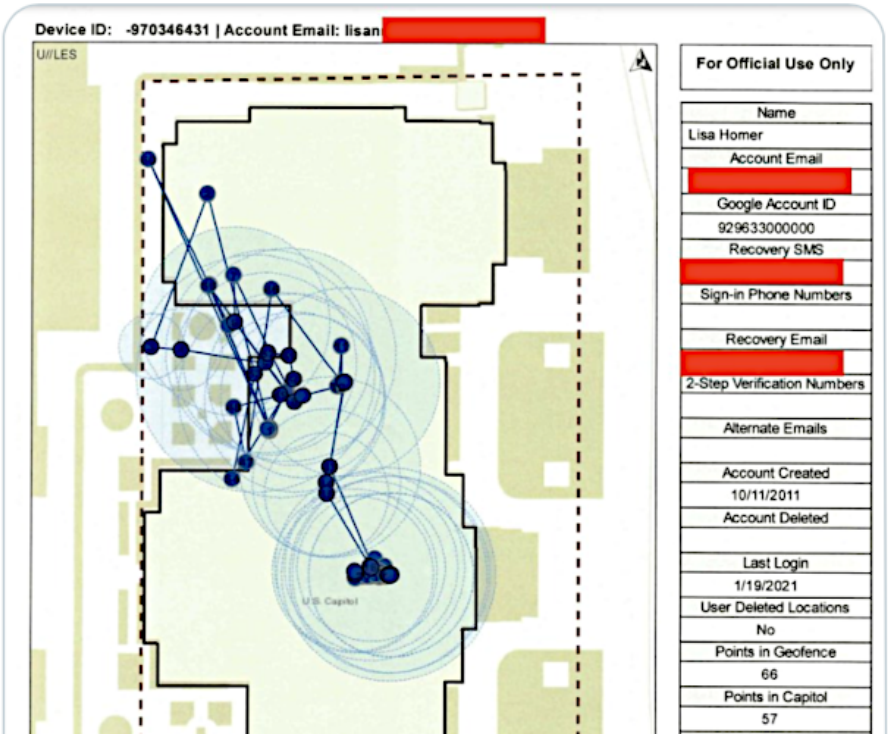


Abbildung 21.1: FBI-Dokument zeigt Genauigkeit des Google-Standort-Trackings

das Tracking nutzen, die der Nutzer neu auswürfeln oder löschen kann. Den Zugriff auf eindeutige Hardwarekennungen beansprucht Google exklusiv für sich.

Auch Googles Smartphones übertragen seit April 2016 die gesamte Call History (Telefonnummer, Datum/Uhrzeit, Dauer). Zur Call History gehören auch die Metadaten verschlüsselter Anrufe mit Messenger Apps wie Signal, Telegram, Elements oder Videokonferenzen via Zoom App. In Googles Datenschutzbestimmungen steht:[4]

> *Wenn Sie unsere Dienste nutzen, um Anrufe zu tätigen und zu erhalten oder um Nachrichten zu senden und zu empfangen, erheben wir möglicherweise Anruf- und Nachrichteninformationen wie Ihre Telefonnummer, die Anrufernummer, die Nummer des Angerufenen, Weiterleitungsnummern, die E-Mail-Adressen von Sender und Empfänger, das Datum und die Uhrzeit von Anrufen und Nachrichten, die Dauer von Anrufen, Routing-Informationen und die Art und Anzahl von Anrufen und Nachrichten.*
>
> *Die in Ihrem Konto gespeicherten Aktivitätsdaten können Sie sich in Ihrem Google-Konto ansehen und sie dort auch verwalten.*

Die Call History wird wie alle anderen Daten für die Optimierung der Werbung verwendet und auch an Werbepartner weitergegeben. Anhand der Daten werden Vermutungen über sexuelle Vorlieben, politische Orientierung und andere Themen erstellt. Die Privacy Policy von Google beschreibt es als gaaaanz harmlos:

> *Diese Daten verwenden wir beispielsweise, um Ihnen ein YouTube-Video zu empfehlen, das Ihnen gefallen könnte.*

[4] https://policies.google.com/privacy?hl=de

Da Google seit 2009 Partner im PRISM-Spionageprogramm der NSA ist, kann man wohl davon ausgehen, dass ...

Neben Google können auch Apps die Call History absaugen, wenn sie die Berechtigung *Reading SMS and Call Logs* haben. Die Facebook-App[5] nutzte natürlich diese Möglichkeit und sammelte die Call History von Smartphones ein, auf denen die App installiert war. Seit 2019 hat Google diese Berechtigung für Apps etwas eingeschränkt. Apps benötigen eine Erlaubnis von Google für den Zugriff auf die Call History.[6]

Es ist manchmal verwunderlich, wenn Leute seit 20 Jahren gegen die gesetzliche Verpflichtung zur Vorratsdatenspeicherung (bzw. Mindestspeicherpflicht) kämpfen und bei ihren Lieblings-Lifestyle-Gadgets keine Probleme damit haben, wenn Apple oder Google die Kommunikationsdaten freiwillig auf Vorrat sammeln und Behörden zur Verfügung stellen.

HarmonyOS (Huawei): Aufgrund der US-Sanktionen gegen Huawei werden die aktuellen Smartphones des chinesischen Konzerns ohne Google-Dienste und Zugriff auf den Playstore ausgeliefert. Google-freie Huawei-Phones übertragen keine Call History in die Cloud. Ein Backup der Call History kann auf einen Datenträger erfolgen und dann auf ein neues Smartphone übertragen werden (wenn gewünscht).

Es werden nur die Standortdaten an Server von Huawei übertragen, wenn man Apps aktiv nutzt, die auf den Standort zugreifen und dabei Informationen über WLANs in der Umgebung zur Verbesserung der Genauigkeit verwenden.

21.2 Datenschutzfreundliche Alternativen für Android

Für Android-Smartphones gibt es neben dem Google-OS einige Open-Source-Alternativen:

GrapheneOS ist eine Google-freie Alternative, die konsequent auf Sicherheit und Privatsphäre optimiert ist und nur für Phones der Google-Pixel-Serie zur Verfügung steht.

Die Liste der Sicherheitsfeatures von GrapheneOS ist lang: besonderer Speicherschutz, Tamper Protection, Verified Boot, Scrambled-PIN-Eingabe, Isolierung des Baseband-Prozessors, DANE/TLSA für alle TLS-Verbindungen des OS usw. Nach Einschätzung von Viktor Chebyshew (Sicherheitsexperte bei Kaspersky) ist es deutlich schwieriger, ein Smartphone mit GrapheneOS zu hacken als ein normales Android-Phone. Auch Edward Snowden lobt GrapheneOS als eine sichere Lösung.

Ein verschlüsseltes Backup der Daten kann man auf einen USB-Datenträger ablegen oder in einer (eigenen) Nextcloud. Es wird keine Google-Cloud verwendet. Die Backup-Funktionen findet man in den Einstellungen unter *System* → *Sicherung*.

Man kann GrapheneOS selbst auf ein unterstütztes Phone flashen. Alternativ bietet die Nitrokey GmbH mit NitroPhone ein Google-freies Pixel mit GrapheneOS als Betriebssystem im Online Shop an. Optional kann man zusätzlich das Mikrofon entfernen lassen und nur via Headset telefonieren, um die Nutzung als Wanze zur akustischen Raumüberwachung zu verhindern.[7]

GrapheneOS kommt mit einer spartanischen Softwareausstattung, die man sich nach eigenen Wünschen erweitern muss. Dabei kann man unterschiedlich vorgehen:

[5] https://www.theverge.com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android
[6] https://android-developers.googleblog.com/2019/01/reminder-smscall-log-policy-changes.html
[7] https://shop.nitrokey.com/de_DE/shop/product/nitrophone-1-199

1. Für die Kommunikation in der *Danger Zone* mit hohen Sicherheitsanforderungen (z. B. als Drogendealer, als den Staat delegitimierender Corona-Leugner o. Ä.) verzichtet man auf die Installation eines App Store und vermeidet so Probleme wie Kill-Switch oder Frontdoor. Die benötigten Messenger wie Threema, Signal App, Session, Briar oder aTox kann man sich von den Webseiten der Entwickler herunterladen und installieren.
2. Wenn man Google-frei bleiben will, aber mehr Apps braucht, kann man sich den F-Droid Store[8] installieren und findet dort ein breites Angebot. Die fehlende Navigations-App kompensieren OrganicMap (mit einfacher Bedienung) oder OSMand (mit vielen Features für Poweruser), für E-Mails gibt es K9Mail, es gibt (fast) alle Messenger, VPN-Apps und vieles mehr...
3. Wenn man GrapheneOS zum vollwertigen Spielzeug aufrüsten will, kann man die gesandboxten Google Play Services & Store installieren, die man in den Graphene-Apps findet. Dann sind dem Spieltrieb keine Grenzen gesetzt.
   Lediglich bei einigen Banking-Apps kann es zu Problemen kommen.

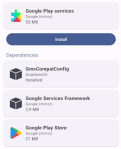


Abbildung 21.2: Installation der Google Services in GrapheneOS

4. GrapheneOS unterstützt die Aufteilung in mehrere Bereiche, die gegeneinander abgeschottet sind. In den Einstellungen kann man unter *System* → *Mehrere Nutzer* weitere Accounts zusätzlich zum Administrator anlegen. Man könnte einen Account mit dem Google-Play-Stuff als Spielwiese, einen für berufliche Kommunikation, einen für private Kommunikation usw. verwenden.

CalyxOS kann man auf den Google-Pixel-Smartphones, dem Fairphone 4 und dem Xiaomi Mi A2 installieren. Es fokussiert als (fast) Google-freie Alternative ebenfalls auf Sicherheit, ist aber nicht so restriktiv vorkonfiguriert und gehärtet wie GrapheneOS.

CalyxOS ist standardmäßig großzügiger mit Apps[9] ausgestattet als GrapheneOS. Organic Map, K9Mail, Signal App, Briar, TorBrowser u. a. m. sind standardmäßig vorhanden. F-Droid ermöglicht die Installation von Open-Source-Apps und der Aurora App Store bietet Zugriff auf die Apps bei Google Play. Die microG Suite bietet Push-Benachrichtigungen via Google Cloud Services (FCM). Wenn man ein Google-freies Phone möchte, kann man microG deaktivieren.

Auf der Webseite findet man Anleitungen, um ein Smartphone selbst zu flashen.[10]

iodéOS ist ein Fork des LineageOS-Projekts mit einigen Verbesserungen für die Privatsphäre. F-Droid ist als App Store vorinstalliert, ein standardmäßig aktiver Werbeblocker funktioniert auch mit VPNs. microG für Google Cloud Services (FCM) kann man optional installieren oder Google-frei leben.

Man kann iodéOS selbst auf ein Samsung-, Xiaomi- oder Sony-Smartphone flashen.

Im Shop gibt es iodéOS vorinstalliert auf einem neuen Terracube und Fairphone-3 oder auf gebrauchten, aufbereiteten Smartphones von Samsung, Xiaomi oder Sony.[11]

[8] https://f-droid.org/de/
[9] https://calyxos.org/docs/guide/apps
[10] https://calyxos.org/install/
[11] https://iode.tech/en/#new-phones

ShiftPhones kann man nicht im Großmarkt kaufen sondern nur auf der Webseite des deutschen Herstellers. Die Smartphones sind modular aufgebaut und einfach reparierbar.[12]

Mit ShiftOS-Light gibt es eine Google-freie Android Version für diese Smartphones direkt vom Hersteller. Es ist der F-Droid Store installiert und man kann keine Apps verwenden, die unbedingt darauf bestehen, die Google Cloud Services (FCM) für Push Benachrichtigungen zu nutzen. Das betrifft beispw. einige Apps für das Online Banking oder Netflix.[13]

/e/ Android ist eine Alternative für ältere Smartphones.

Um ältere Hardware zu unterstützen, die von Herstellern nicht mehr unterstützt wird, kommt ein etwas angestaubter Linux-Kernel in /e/ zum Einsatz. Auch die Apps im /e/ Store sind oft veraltet. Deshalb sollte man als erstes den F-Droid Store installieren und weitere Apps von dort.

/e/ ist Google-frei, verwendet standardmäßig keine Cloud-Dienste und überträgt keine Daten an die /e/ Foundation. Um Cloud-Funktionen zu nutzen, kann man einen Account bei der /e/ Cloud erstellen oder eine beliebige andere Nextcloud-Instanz nutzen.

Erfahrene Nutzer können das Custom ROM von /e/ auch auf einem vorhandenen Google-Smartphone installieren und damit Google rauswerfen. Es werden aktuell 93 Android-Smartphones unterstützt (Stand Oktober 2020).

Man kann Phones mit vorinstalliertem /e/ im Shop der /e/ Foundation kaufen.[14]

21.3 Datensammlungen mit Smartphone Apps

Standortdaten: Tausende Apps sammeln überflüssigerweise Standort- und Bewegungsdaten der Nutzer. Der ehemalige Bundesdatenschutzbeauftragte erwähnt bspw. eine App, die das Smartphone zur Taschenlampe macht und dabei den Standort an den Entwickler der App sendet (vielleicht lustig bis harmlos?).

Weniger lustig wird es, wenn die *Muslim Prayer App* mit mehr als 98 Mio. Nutzern weltweit, die nur an das Gebet erinnert und die Richtung nach Mekka anzeigt, oder die populäre *Muslim Dating App* Standortdaten sammeln und an die Firma Locate X senden. Die Daten werden vom US-Militär gekauft und zur Planung von gezielten Tötungen mit Drohnen genutzt. Außerdem kauft das U.S. Special Operations Command (USSOCOM) diese Daten zur Planung und Unterstützung von verdeckten Special-Forces-Einsätzen. Secret Service und US Customs and Border Protection (CBP) sind weitere Kunden, die die Datensammlung von Locate X abonniert haben.[15] [16]

US Customs and Border Protection (CBP) zahlt jährlich fast eine halbe Million Dollar an die Firma Venntel für den Zugriff auf die Standort- und Bewegungsdaten. Auch die US-Immigrationspolizei (ICE) gehört zu den Kunden von Venntel. Die Firma kauft Daten von harmlosen Wetter-Apps, Navigationsapps, der Starbucks-App u. Ä. sowie von Spielen und bereitet sie auf.[17]

Fog Date Sience LLC ist ein Outlet von Venntel, dass die Standortdaten an US-Polizeien verkauft. Um geltende Gesetze zum Datenschutz zu umgehen, werden die Standortdaten

[12] https://www.shiftphones.com
[13] https://www.shift.eco/hilfe_faqs/was-ist-shiftos-l
[14] https://esolutions.shop/
[15] https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x
[16] https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street
[17] https://www.vice.com/en/article/k7qyv3/customs-border-protection-venntel-location-data-dhs

anhand der Advertizing ID übermittelt, die aber leicht einem konkreten Smartphone und Besitzer zugeordnet werden kann. Die Polizeibehörden können mit dem Tool von Fog Date Sience LLC ohne richterlichen Beschluss laufend den Standort von 250 Mio. US-Amerikanern bestimmen.

Der norwegische Journalist M. Gundersen hat in einer Recherche die Datensammlung der Firma Venntel genauer analysiert. Im Februar 2020 installierte er auf einem neuen Smartphone 160 Apps und trug es ständig bei sich. Keine der 160 Apps nannte die Firma Venntel in ihren Datenschutzklauseln.[18]

Im August forderte er von Venntel Einsicht in die Daten, welche die Firma über ihn gesammelt hatte. Zur Identifizierung übergab er die Advertising-ID des Smartphones. Als Antwort erhielt er 75.406 Datenpunkte mit Location- und Zeitstempel, die in den 6 Monaten gesammelt wurden. Anhand der Daten konnten sein Wohnort, seine Arbeitsstelle, seine Wanderungen in der Freizeit sowie jede Bank nachvollzogen werden, auf der er sich während der Wanderung ausgeruht hatte. Abb. 21.3 zeigt den Ausschnitt von 36 Minuten aus einer Wanderung mit einer Rast.

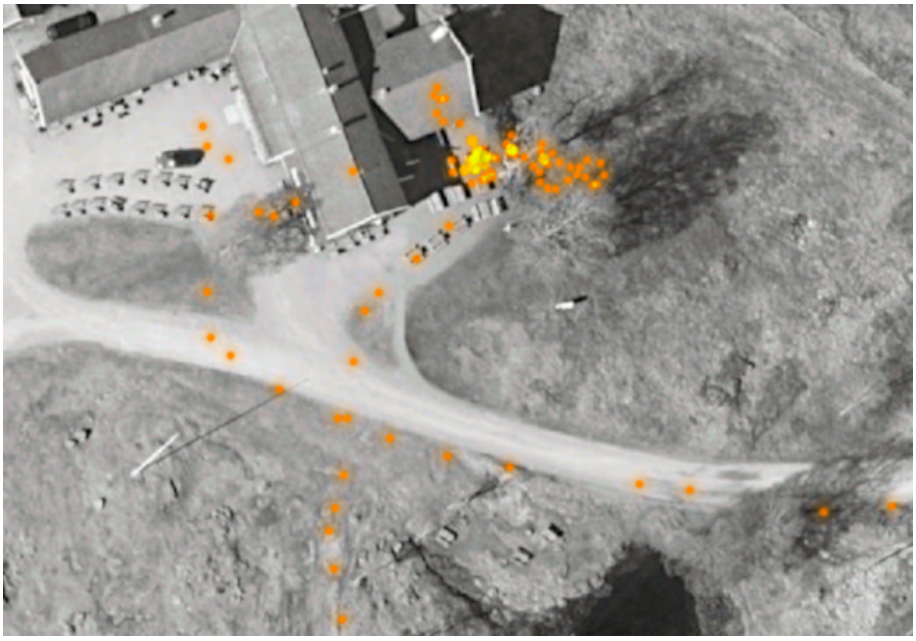


Abbildung 21.3: Illustration: Harald K. Jansson/Norge i bilder

Venntel informierte M. Gundersen auch darüber, dass seine Daten an die zahlenden Kunden der Firma weiterverkauft wurden, nannte aber keine Namen von Kunden.

In weiteren Recherchen konnte M. Gundersen ermitteln, das Venntel die Daten u. a. von der französischen Firma Predicio und von der US-Firma Complementics kauft. Ein großer Teil der ortsbezogenen Daten stammt außerdem von dem slowakischen Unternehmen Sygic, das ein Portfolio von 70 Apps anbietet.

Neben Locate X und Venntel ist die Firma Anomaly Six (A6) ein weiterer Baustein bei der Sammlung von Standort- und Bewegungsdaten für US-Behörden und Geheimdienste. Das SDK der Firma Anomaly Six wird in Apps eingebaut und die Entwickler werden dafür bezahlt. Diese Apps senden damit laufend die Standortdaten von einigen hundert

[18] https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants/

Mio. Nutzern an das US-amerikanische Unternehmen und von dort aus weiter an US-Geheimdienste.[19]

Laut Eigenwerbung verfolgt Anomaly Six täglich 230 Mio. Smartphones und sammelt pro Jahr 280 TeraByte Standortdaten (Stand 2022). In einer Demonstration zeigte Anomaly Six, wie der Weg von NSA-Mitarbeitern vom Hauptsitz in Fort Meade nach Jordanien oder der Einsatz von russischen Wagner-Söldnern verfolgt werden kann.[20]

Für den Daten- und Überwachungsforscher Wolfie Christl hat diese Form der Überwachung eine völlig neue Qualität:

> *Ich habe das Gefühl, dass viele nicht verstehen, dass dies völlig beispiellos ist und anders als das ist, was Edward Snowden im Jahr 2013 aufdeckte.*
>
> *Statt kompliziertem Schnüffeln im Traffic ist die US-Regierung jetzt ein weiterer Marktteilnehmer in einer bestehenden kommerziellen Trackingwirtschaft.*

Fun Fact: Die NSA forderte im August 2020 die Mitarbeiter in der Spionage-Community auf, auf den privaten Smartphones die Nutzung von Apps mit Standortverfolgung stark einzuschränken, weil auch andere Staaten diese Möglichkeiten nutzen.

IP-Adressen werden im Post-Cookie-Zeitalter wieder zu einem wichtigen Merkmal. Bei Smartphones ist es aber nicht so einfach, einzelne Geräte zu verfolgen, da man zwischen WLAN und mobiler Verbindung wechselt und bei jedem Wechsel eine neue IP-Adresse erhält.

Die belgische Firma Utiq SA/NV[21] kooperiert mit der Telekom, Vodafone, Telefónica und Orange, um Smartphones anhand von wechselnden IP-Adressen im mobilen Netzwerk (WWAN) zu verfolgen. Das Verfahren wird auch als *Netzwerk-Cookies* bezeichnet und funktioniert wie folgt:

1. Wenn ein Surfer eine verseuchte Webseite besucht, sendet der Webserver die IP-Adresse und die aufgerufene Webseite zu Utiq.
2. Utiq ermittelt den Telekommunikationsprovider und schickt die IP dorthin.
3. Der Telekommunikationsprovider weiß, welchem Smartphone (SIM Karte) diese IP-Adresse aktuell zugeteilt ist und liefert eine pseudonyme ID zurück, die für diese SIM Karte konstant bleibt, auch wenn die IP-Adresse wechselt.
4. Utiq sendet die ID an eine Marketingplattform, die dann die passende Werbung liefert.
5. Der Webserver baut diese individualisierte Werbung in die ausgelieferte Webseite ein.
6. Die angezeigte Werbung könnte man mit irgendwelchen Werbeblockern wie uBlock Origin o. ä. blockieren, aber das Tracking verhindert man damit nicht.

Im Juni 2023 hat Utiq SA/NV erste Ergebnisse dieser neuen Trackingmethode vorgestellt. Das Tracking anhand der IP-Adresse in Kooperation mit Telcos kann 4x mehr Surfer verfolgen als es mit Third-Party-Cookies möglich ist und ist um 25% besser als Tracking mit First-Party Cookies.

Auf der Webseite Utiq consenthub[22] kann man dieser Form des Tracking widersprechen. Möglicherweise wird es aber zukünftig mehrere Firmen geben, die das anbieten und dann sollte man sich vielleicht daran gewöhnen, immer ein VPN auf dem Smartphone zu nutzen.

[19] https://www.wsj.com/articles/u-s-government-contractor-embedded-software-in-apps-to-track-phones-11596808801
[20] https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-zignal-surveillance-cia-nsa/
[21] https://utiq.com
[22] https://consenthub.utiq.com

Metadaten der Kommunikation werden von den standardmäßig auf den Android-Smartphones installierten Apps für SMS (Google Messaging App) und Telefonie (Google Dailer App) gesammelt.

> When an SMS message is sent/received the Google Messages app sends a message to Google servers recording this event, the time when the message was sent/received and a truncated SHA256 hash of the message text. The latter hash acts to uniquely identify the text message. The message sender's phone number is also sent to Google, so by combining data from handsets exchanging messages the phone numbers of both are revealed.
>
> When a phone call is made/received the Google Dialer app similarly logs this event to Google servers together with the time and the call duration.

Das Logging der Daten entspricht der Vorratsdatenspeicherung, gegen die wir viele Jahre gekämpft haben, die wir aber jetzt bei den Smartphones akzeptieren.

Um die Datensammlung etwas zu reduzieren, kann man **Silence**[23] oder den **Fossify SMS Messenger**[24] installieren. Bei der Installation der Apps oder in den Einstellungen unter *Apps* → *Default Apps* → *SMS App* kann man auswählen, welche App sich um die SMS kümmert. *Silence* kann SMS auch verschlüsseln, wenn beide Seiten die App nutzen. Der Silence Warrant Canary wird regelmäßig aktualisiert und signalisiert damit auch, dass das Projekt weiterhin betreut wird, auch wenn die aktuelle Version schon einige Jahre alt ist.

Adressbücher: Viele Apps beschränken sich nicht auf die Sammlung von Standortdaten und Anzeige von Werbung. Die folgenden Apps lesen die Kontaktdaten aus dem Adressbuch und senden sie ohne Freigabe durch den Nutzer an den Betreiber:

- die Social Networks *Facebook*, *Twitter* und *Path*;
- die Location-Dienste *Foursquare, Hipster* und *Foodspotting*;
- die Fotosharing-App *Instagram*;
- die VoIP-Software *Viper* sowie verschiedene Messaging Dienste;
- usw.

Politisch brisant können diese Datensammlungen werden, wenn z. B. Twitter alle Daten von Wikileaks-Unterstützern an die US-Behörden herausgeben muss. Damit geraten auch die Freunde von Wikileaks-Unterstützern als potentiell suspekte Individuen ins Visier von US-Behörden, was u. U. unerwünschte Konsequenzen haben kann.

Browserverlauf: Die Spiele der Hersteller iApps7 Inc, Ogre Games und redmicapps gehen in ihrer Sammelwut so weit, dass sie von Symantec als Malware eingestuft werden. Die Spiele-Apps fordern folgende Rechte um Werbung einzublenden:

- ungefährer (netzwerkbasierter) Standort,
- genauer (GPS-)Standort,
- uneingeschränkter Internetzugriff,
- Browserverlauf und Lesezeichen lesen,
- Browserverlauf und Lesezeichen erstellen,
- Telefonstatus lesen und identifizieren,

[23] https://f-droid.org/packages/org.smssecure.smssecure/
[24] https://f-droid.org/packages/org.fossify.messages

- Automatisch nach dem Booten starten.

Auch Spiele von Disney verlangen sehr weitreichende Freigaben, so dass sie nur als Spionage-Tools bezeichnet werden können.

Analytics: Viele Smartphone-Apps enthalten Daten sammelnde Bibliotheken von Dritten. Führend sind dabei Google (in 50 % aller Apps) und Facebook (in 30 % aller Apps). Die in den Apps enthaltenen Bibliotheken sammeln fleißig Daten über jede Interaktion des Nutzers mit der App oder Standortdaten usw. und schicken sie an die großen Datensammler. Als Gegenleistung bekommen die Entwickler Analysedaten über das Nutzerverhalten ihrer App, Crashreports und Einnahmen durch Werbung.

Die Datenkonzerne werten die Daten natürlich parallel auch für ihre eigenen Interessen aus. So sammelt Facebook bspw. über diesen Weg große Mengen an Daten über Nichtmitglieder, die in sogenannten Schattenprofilen geführt werden.

Die Webseite **Exodus Privacy**[25] hat 52.000+ Android-Apps analysiert und sammelt weiterhin Analysen von Apps. Die Übersicht der Tracker zeigt, dass am häufigsten Google-Tracking-Bibliotheken verwendet werden und dass Facebook an zweiter Stelle steht. Bibliotheken für Werbung und Analytics werden besonders gern verwendet, da sie jede Aktion des Nutzers protokollieren und an Google, Facebook o. a. senden.

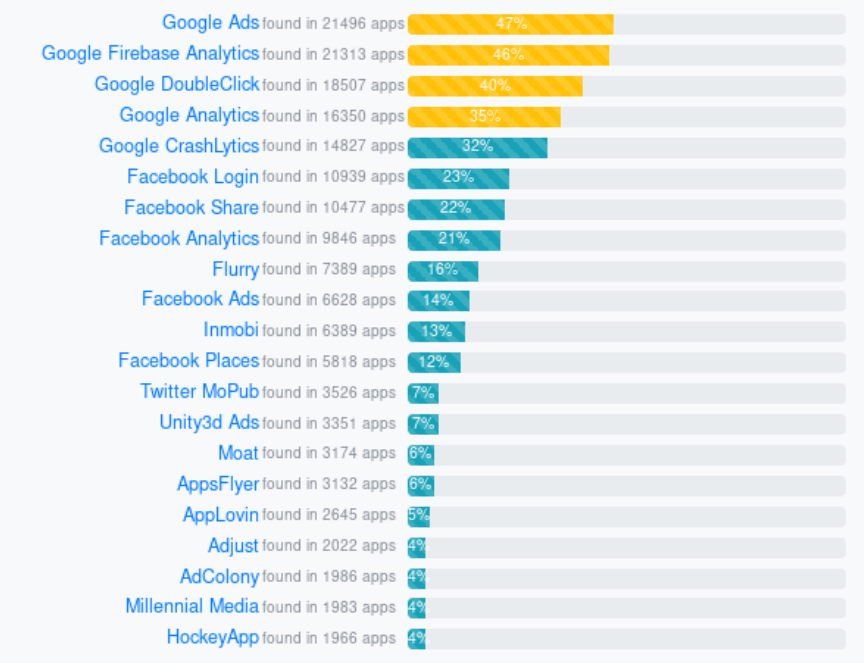


Abbildung 21.4: Die häufigsten Tracking-Bibliotheken in Android Apps

Neben den negativen Beispielen mit mehr als 30 Tracking-Bibliotheken in einzelnen Apps findet man auf Exodus Privacy auch positive Beispiele ohne Tracker[26]. Wenn man eine App für eine bestimmte Aufgabe sucht, findet man dort Alternativen ohne Tracker (wobei ich Crash-Reporting-Bibliotheken als unkritisch einstufen würde).

Hinweis: man muss nicht immer für jeden Anwendungsfall eine App nutzen. Viele Dienste bieten eine Smartphone-taugliche Webseite im Responsive-Design, die mit einem datenschutzfreundlichen Browser (z. B. Firefox Klar) genutzt werden kann.

[25] https://reports.exodus-privacy.eu.org/en/
[26] https://reports.exodus-privacy.eu.org/en/reports/?filter=no_trackers

Passwörter: Einige E-Mail-Apps übertragen bei Einrichtung eines E-Mail-Accounts die E-Mail-Adresse und das Passwort für den Account an den Hersteller der App. Hey – das nennt man Phishing und nicht Service!

Die Server der App-Hersteller verwenden die Login-Credentials, um sich bei dem externen E-Mail-Account einzuloggen und nach neuen E-Mails zu suchen. Sie laden die Mails auf den eigenen Server, beschnüffeln sie manchmal ein bisschen und benachrichtigen den Nutzer dann per Google Push Service über neue E-Mails.

- Prominentes Beispiel ist die *MS-Outlook-App für iOS und Adroid*. Das EU Parliaments IT Department (DG ITECS) hat deshalb die Nutzung der MS-Outlook-App verboten.[27] In dem Privacy-Statement findet man den Hinweis, dass die Login-Credentials für E-Mail-Accounts (Username, Passwort) von Microsoft gesammelt werden und dass sich Microsoft die E-Mails von den Providern holt und verarbeitet:

  > *Email Credentials: We collect and process your email address and credentials to provide you the service.*
  > *Email Data: We collect and process your email messages and associated content to provide you the service. [. . .]*

- M. Kuketz nennt in seinem Blog mit den E-Mail-Apps *BlueMail, TypeMail Mail.Ru, myMail* u. a. m. weitere Beispiele. Mit der Einrichtung des E-Mail-Accounts in der BlueMail-App gibt man der Firma das Recht, in dem Mail-Account zu schnüffeln:

  > *When you link your email accounts (provided by third parties) to Blue Mail, you give Blue Mail permission to securely access your information contained in or associated with those accounts.*

  Außerdem beschnüffelt der BlueMail-Server die E-Mails und wertet z. B. die Geolocation-Tags in versendeten Fotos aus. Wer das nicht möchte, soll eine Kamera verwenden, die keine Geolocation-Informationen in den Fotos speichert. Auch diese Schnüffelei wird juristisch korrekt im Privacy Statement benannt.

Vertrauenswürdige Alternativen für E-Mail-Apps sind **K9Mail**[28] oder **FairEmail**.[29] Nach dem Wechsel auf eine vertrauenswürdige App sind die Passwörter für die betroffenen E-Mail-Accounts zu wechseln!

21.4 Überwachung

Auch Strafverfolgungsbehörden und Geheimdienste nutzen die neuen Möglichkeiten zur *Durchleuchtung der Gesellschaft*:

- Die NSA sammelt täglich rund 5 Milliarden Standortdaten von Mobiltelefonen weltweit im Rahmen des Programms STORMBREW. Nahezu jeder Handynutzer ist betroffen. Das Analyse-Programm *Co-Traveler* sucht anhand der Standortdaten nach Verbindungen zu Zielpersonen. Wer sich zufällig mehrmals am gleichen Ort wie eine Zielperson aufgehalten hat oder zufällig im gleichen Zug saß, kann auch als Unschuldiger ins Netzwerk der Spionage geraten. Außerdem wird nach Verhaltensmustern gesucht, die auf ein erhöhtes Sicherheitsbewusstsein hindeuten.

[27] https://www.scmagazineuk.com/eu-parliament-blocks-microsoft-outlook-apps-over-privacy-fears/article/537584/
[28] https://k9mail.app
[29] https://email.faircode.eu

- NSA/GCHQ sammeln täglich fast 200 Millionen SMS mit dem Programm DISHFIRE. Anhand der Datensammlung werden Kontaktbeziehungen (Identifizierung neuer Zielpersonen), Reisedaten, Finanztransfers (Konto- und Kreditkartennummern) u. a. m. analysiert.
- Das FBI nutzt das Tracking von Smartphones seit mehreren Jahren, wie Danger Room berichtete. Muslimische Communitys werden systematisch analysiert, ohne dass die Personen im Verdacht stehen, eine Straftat begangen zu haben.[30]
- Im Iran werden mit Hilfe der Funkzellenauswertung die Teilnehmer von Demonstrationen in Echtzeit ermittelt. Die Technik dafür wird von westlichen Unternehmen entwickelt, beispielsweise von Siemens/Nokia und Ericsson. Nachdem die Unterstützung von Siemens/Nokia für die Überwachung bekannt wurde und ein Boykottaufruf zu mehr als 50 % Umsatzeinbruch im Iran führte, wurde die Überwachungstechnik bei Siemens/Nokia in eine Tochtergesellschaft ausgelagert: Trovicor. Zu den Kunden von Trovicor zählen auch Bahrain, Katar und ähnliche Diktaturen.
- In der Ukraine wurden die Geofencing-Daten von Handys bereits im Januar 2014 zur Einschüchterung von Demonstranten genutzt. Teilnehmer einer Demonstration gegen den damals amtierenden Präsidenten bekamen eine SMS mit dem Inhalt:[31]

  Sehr geehrter Kunde, sie sind als Teilnehmer eines Aufruhrs registriert.

Auch in Deutschland wird die Lokalisierung von Smartphones mittels Funkzellenauswertung zur Gewinnung von Informationen über politische Aktivisten genutzt:

- Die flächendeckende Auswertung von Handydaten im Rahmen der Demonstration GEGEN den (ehemals) größten Nazi-Aufmarsch in Europa in Dresden im Februar 2011 hat erstes Aufsehen erregt. Obwohl die Aktion von Gerichten als illegal erklärt wurde, werden die gesammelten Daten nicht gelöscht und weiterhin für die Generierung von Verdachtsmomenten genutzt.[32]
- Seit 2005 wird diese Methode der Überwachung auch gegen politische Aktivisten eingesetzt. So wurden beispielsweise die Aktivisten der Anti-G8-Proteste per groß angelegter Funkzellenauswertung durchleuchtet.[33] Die Überwachung der Handys der Aktivisten begann bereits zwei Jahre vor dem G8-Gipfel in Heiligendamm.
- Die breite Funkzellenauswertung in Berlin zur Aufklärung von Sachbeschädigungen wird als gängige Ermittlungsmethode beschrieben. Auf Anfrage musste die Polizei zugeben, dass diese Methode bisher NULL Erfolge gebracht hat.
- Die Nutzung der Stillen SMS zur Lokalisierung von Personen boomt gerade beim Verfassungsschutz:
  - 1. Halbjahr 2013: 28.500 Stille SMS versendet;
  - 1. Halbjahr 2014: 53.000 Stille SMS versendet;
  - 2. Halbjahr 2014: 142.000 Stille SMS versendet.

  Gleichzeitig stagniert die Nutzung der Stillen SMS bei Strafverfolgern (Polizei, BKA usw.) oder geht zurück. Man kann jetzt darüber spekulieren, was die Gründe für diese Aktivitäten des Verfassungsschutzes sind.

[30] https://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims/
[31] https://www.heise.de/-2095284
[32] https://www.heise.de/tp/artikel/34/34973/1.html
[33] https://www.heise.de/tp/artikel/35/35043/1.html

21.5 Aktivierung als Abhörwanze

Dass Strafverfolger und Geheimdienste ein Handy/Smartphone remote als Abhörwanze aktivieren können, ist seit 2006 bekannt. Das FBI nutzte damals die Handys der Mafiabosse Ardito und Peluso remote zur akustischen Raumüberwachung, um Beweise zu sammeln.[34]

Bereits 2007 hat das BSI deshalb empfohlen, bei Gesprächen mit sensiblen Inhalten keine Handys mitzuführen. Das schützt natürlich nur, wenn sich alle Beteiligten daran halten.

> *Aus Sicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die effektivste Schutzmaßnahme ein Vermeiden des Mitführens von Handys bei Gesprächen mit sensitivem Inhalt, die Detektion jedweder Mobilfunkaktivität im Raum durch den vom BSI entwickelten Mobilfunkdetektor MDS sowie das Deaktivieren sämtlicher drahtloser Schnittstellen von Mobilfunkgeräten.*

Der Missbrauch eines Smartphones als Abhörwanze ist nicht auf potente Geheimdienste beschränkt. Angreifer können auch Apps mit verdeckten Funktionen verwenden. Dafür gab es in der Vergangenheit bereits mehrere Beispiele:

- Die offizielle App der spanischen Fußballliga *La Liga* aktivierte während der Ausstrahlung der Fußballspiele im TV das Mikrofon der Smartphones zur Raumüberüberwachung, um in Kombination mit den GPS-Standortdaten nach der unlizenzierten öffentlichen Übertragung von Ligaspielen zu fahnden. Die App hat ca. 10 Mio. Nutzer in Spanien.[35]
- Die Hamas hat anlässlich der WM ebenfalls eine App für Fußballfans in der israelischen Armee entwickelt und außerdem mehrere Dating-Apps für israelische Soldaten (Heart Breaker), die der Spionage dienten, inklusive akustischer Raumüberwachung und Zugriff auf die Kamera. Ein Sicherheitsoffizier der IDF kommentierte:[36]

  > *Whatever you can do with your phone, a malicious app can do too.*

Aktuelle Smartphone-Betriebssysteme machen es App-Entwicklern etwas schwerer, das Mikrofon unbemerkt zur Raumüberwachung zu nutzen (wenn man weiß, worauf man achten muss).

Bei iOS 14+ leuchtet ein kleiner gelb-oranger Punkt über der Anzeige der Signalstärke der Netzwerkverbindung, wenn die App im Vordergrund das Mikrofon verwendet. Der Punkt wird rot, wenn eine App im Hintergrund das Mikrofon verwendet und bei gesperrten iPhones sollten alle Apps keinen Zugriff mehr auf das Mikrofon haben.

In Android 12+ wurde eine ähnliche Anzeige bei Zugriff auf Mikrofon und Kamera intergriert.

[34] http://news.cnet.com/2100-1029-6140191.html
[35] https://heise.de/-4075636
[36] https://www.rt.com/news/431663-hamas-dating-app-idf-israel

21.6 WLAN und Bluetooth ausschalten, wenn nicht genutzt

Alle Smartphones (und Laptops!) haben ein WLAN-Modul. Es ist bequem, wenn man nach Hause kommt oder wenn das Smartphone am Arbeitsplatz automatisch das WLAN nutzt statt der teuren Datenverbindungen des Mobilfunk-Providers.

nn man mit aktiviertem WLAN Modul und automatischem Login für die bevorzugte WLANs unterwegs ist, dann ergeben sich einige Implikationen für die Privatsphäre und die Sicherheit:

1. Auf der re:publica 2013 wurde ein kostenfreies WLAN bereitgestellt. Dieses WLAN verfolgte alle WLAN-fähigen Geräte (Laptops und Smartphones) der Besucher, unabhängig davon, ob die Geräte das WLAN nutzten oder nicht. Das Projekt *re:log - Besucherstromanalyse per re:publica W-LAN* visualisiert die Daten.[37]

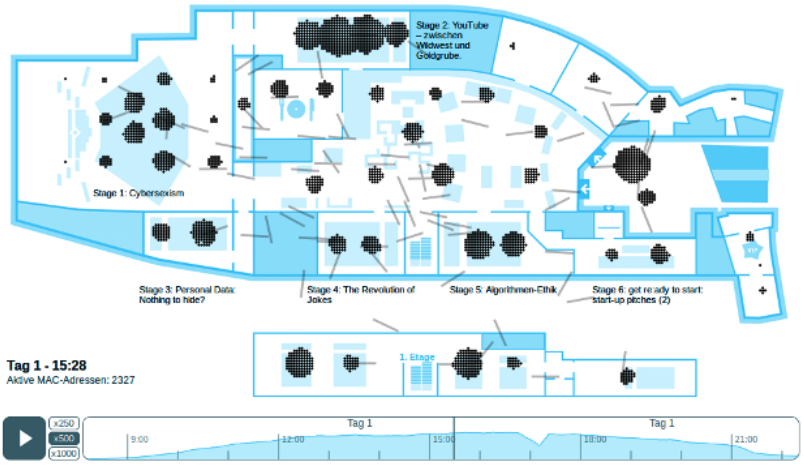


Abbildung 21.5: WLAN-Tracking auf der re:publica 2013

   Die Werbefirma Renew wollte dieses Prinzip kommerziell ausbauen und stellte zu den Olympischen Spielen 2012 in London 200 Abfallbehälter auf, die mit einem integrierten WLAN-Access-Point die Fußgänger anhand der MAC-Adressen der Smartphones verfolgten. Innerhalb einer Woche wurden über 4 Mio. Geräte durch die Londoner City verfolgt.

   > *We will cookie the street.* (K. Memari, chief executive of Renew)

   Mit aktuellen Smartphones ist diese Verfolgung der Bewegungen der Smartphones anhand der MAC Adressen der WLAN Module **nicht mehr möglich** (wenn man das WLAN nicht aktiv nutzt), da für WLAN Scans jetzt randomisierte MAC Adressen verwendet werden.

2. Die Berliner Verkehrsbetriebe haben in Zusammenarbeit mit HOTSPLOTS auf den U-Bahnhöfen kostenfreies Wi-Fi zur Verfügung gestellt. *We will cookie the subway.* wäre ein guter Slogan, aber *Unser Loggmittel...* ist echt gut und passend.

   Die Nutzung ist ganz einfach. Wenn man beim Warten auf die U-Bahn noch schnell mal ... wählt man das *BVG Wi-Fi* und ruft eine Webseite auf. Nachdem man die Nutzungsbedingungen bestätigt und die erste Werbeseite gesehen hat, kann man kostenfrei Surfen usw. Es werden kein Name und keine E-Mail-Adresse abgefragt.

[37] http://apps.opendatacity.de/relog/

Zukünftig meldet sich das Smartphone bei jedem Ein- und Aussteigen und bei jeder Durchfahrt durch den Bahnhof automatisch bei dem BVG-Access-Point an. In den Nutzungsbedingungen ganz unten (runterscrollen) findet man die Daten, die bei jedem (automatischen) Connect gespeichert werden:

- die eindeutige MAC-Adresse des Gerätes,
- die zugewiesene IP-Adresse,
- Zeitstempel des Login und Logout.

Die Daten werden gemäß TKG und Vorratsdatenspeicherung (neudeutsch: Mindestspeicherfristen) gespeichert. Außerdem werden sie von HOTSPLOTS ausgewertet und der BVG für statistische Auswertungen zur Verfügung gestellt. Diese Daten ermöglichen eine Verfolgung von Bewegungen in der realen Welt, wie es anhand der Besucherströme auf der republica 2013 demonstriert wurde.

Da aktuelle Smartphones beim Verbindungsaufbau zu einem bekannten WLAN standardmäßig immer den gleiche Fake der MAC Adresse verwenden kann mit dem automatischen Connect der Weg von Fahrgästen verfolgt werden, die das WLAN einmal (aus Neugier?) genutzt haben.

Ähnliche Datenspuren hinterläst man im WLAN im ICE oder bei einigen Kaffeehausketten.

3. Auf der Blackhat Asia 2014 wurde mit Snoopy ein aktiver Abgriff vorgestellt. Diese Drohne kann häufig benutzte SSIDs von WLANs ohne Anmeldepasswort simulieren. In Deutschland wären dafür WiFiOnICE oder HOTSPLOTS (15.000 Access Points) gut geeigenet.

   Die Smartphones meldet sich gutgläubig im Hintergrund automatisch bei der Drohne an. Der Internet Traffic läuft über die Drohne und kann dort analysiert und modifiziert werden.

   Es wurde auf der Konferenz demonstriert, wie Snoopy Login Credentials von PayPal, Yahoo! usw. abgreifen konnte, Name und Wohnort der Nutzer ermitteln konnte und die Smartphones über einen längeren Zeitraum tracken konnte.

   Hinweis: Wenn man WLANs ohne Passwortschutz nutzt, sollte man Autologin für diese WLANs deaktivieren oder offene WLANs nach der Benutzung auf dem Phone löschen.

4. Smartphones senden ständig sogenannte *Probe Requests*, um nach WLAN Access Points in der Umgebung zu suchen. Bei älteren Phones sendeten die *Probes* eine Liste aller WLAN SSIDs, die das Smartphone kennt (die Prefered Network List, PNL).

   Es gab mehrere Studien, die analysiert haben, wie man Smartphone Nutzer anhand der PNL deanonymisieren oder angreifen kann. Zuletzt wurde von der Universität Hamburg eine Studie publiziert, laut der im Jahr 2021 noch 23% der Smartphones in einer belebten Fußgängerzone aktiv *Probe Requests* mit den SSIDs der ihnen bekannten WLANs sendeten.

   Jetzt würde das Ergebnis wahrscheinlich nahe Null liegen, da aktuelle Smartphones nur dann die SSIDs bekannter WLANs mit den *Probe Requests* versenden, wenn sie als versteckte WLANs konfiguriert wurden. Sogenannte *versteckte WLAN Accesspoints* sind nicht unsichtbar, aber sie senden ihre SSID nicht aktiv, so dass man sie direkt ansprechen muss, wenn man sich mit ihnen verbinden will - ist ein sehr exotisches Feature, das man nicht nutzen sollte.

Obwohl sich hinsichtlich Privatsphäre bei den WLAN Schnittstellen in den letzten Jahren vieles verbessert hat, ist es trotzdem empfehlenswert, WLAN abzuschalten, wenn man sie nicht braucht.

Bluetooth wird in gleicher Weise für das Tracking genutzt. Außerdem erhöht jede Funktion die Angriffsfläche. Die Webseite mobilsicher.de empfahl bereits 2015:

Ein ausgeschaltetes Bluetooth-Gerät kann niemand angreifen oder sich heimlich damit verbinden. Daher sollte die Funktion bei Smartphone oder Tablet nur an sein, wenn sie auch genutzt wird.

Dass diese Warnung berechtigt war, zeigt der Angriff BlueBorn, der im September 2017 publiziert wurde. Über mehrere Sicherheitslücken in Bluetooth können Angreifer Smartphones exploiten und eigenen Code auf dem Gerät ausführen. Android- und Linux-Geräte können komplett übernommen werden.[38]

2023 publizierte Kapersky einen Angriff, mit dem es möglich ist, eine Tastatur via Bluetooth zu registrieren. Der Angreifer kann dann ohne weitere Authentifizierung als legaler Nutzer Befehle mit dieser Tastatur auf dem Gerät ausführen. Betroffen waren neben Smartphones auch PCs.[39]

Schlussfolgerung: Bluetooth abschalten, wenn man es nicht braucht.

21.7 Push Services oder Polling nutzen

Es gibt viele Apps, bei denen man erwartet, dass man zeitnah über Neuigkeiten von einem Server informiert wird. E-Mail-Clients und Messenger sollen neu eingetroffene Nachrichten anzeigen, Banking-Apps sollen über Finanztransaktionen informieren usw. Gleichzeitig soll der Energieverbrauch der Apps und das Datenvolumen minimiert werden.

Push-Services wurden von Google und Apple entwickelt, um diese Anforderungen zu erfüllen. Sie funktionieren folgendermaßen:

1. Eine Smartphone App, die von einem Server über Neuigkeiten benachrichtig werden möchte, fordert von den Push Services APN (Apple), FCM (Google) oder von einem eigenen, App-spezifischen Push Service (nur bei Android möglich) ein sogenanntes Push Token an.
2. Dann registriert die App dieses Push-Token bei dem Server, der die App bei Neuigkeiten benachrichtigen soll (Messenger, Mailserver o. Ä.), und legt sich wieder schlafen. Der Server weiß damit, über welchen Push Service er dem User eine Nachricht schicken kann.
3. Wenn der Server eine Neuigkeit an die Smartphone-App senden will, nimmt er das Push-Token und schickt es zusammen mit einer kurzen (verschlüsselten) Information an den Push-Service APN (iOS) oder FCM (Android). In der Regel wird nur die Info *New Message here* gesendet.
4. Die Push-Services leiten die Nachricht anhand des Push-Tokens an das Smartphone.
5. Das Smartphone empfängt die Nachricht, weckt die passende App auf und übergibt ihr den (verschlüsselten) Inhalt der Push-Nachricht. Alles weitere übernimmt die App.

Für Android Apps gibt es Projekte (vor allem Messenger), die eigene Push Services entwickeln, die unabhägig von Google funktionieren und keine Daten beim Datenkraken hinterlassen. Bei iPhones ist man aber immer auf APN von Apple angwiesen. Es gibt in iOS keine anderen Möglichkeiten.

[38] https://heise.de/-3830319
[39] https://www.kaspersky.de/blog/bluetooth-vulnerability-android-ios-macos-linux/30750/

Polling ist eine Alternative zu Push-Services. Statt auf eine Benachrichtigung zu warten, fragt die Smartphone App alle 10–20 Minuten bei dem Server nach, ob es Neuigkeiten gibt.

Beim Polling sind keine zusätzlichen Services von Apple oder Google notwendig, nur die Apps und Server sind in die Kommunikation involviert. Nachteilig ist vor allem ein höherer Energie- und Datenverbrauch.

Implikationen von FCM (Google) und APN (Apple) für die Privatsphäre

- Bei Verwendung von Push-Benachrichtigungen kann der Push-Service (APN oder FCM) protokollieren, wie viele Benachrichtigungen ein Nutzer für eine bestimmte App bekommt, also wie intensiv die App genutzt wird. Die Inhalte der Nachricht sind i. d. R. verschlüsselt.
- Accounts, die nicht an eine Telefonnummer gebunden sind, können mit den Push-Token deanonymisiert werden, da Google oder Apple diese Accounts anhand der Push-Token mit einer Telefonnummer, der Geräte IMEI oder Kontodaten verknüpfen können.
- Behörden zur Strafverfolgung und Geheimdienste haben gemäß Bestandsdatenauskunft in DE des Recht, alle Informationen abzufragen, die ein Provider (E-Mail, Messenger, Cloud usw.) im Rahmen der Bereitstellung des Dienstes über einen Nutzer gespeichert hat. Dazu zählen auch die Push-Token, die von einem Nutzer auf dem Server registriert wurden.

  Mit diesen Push-Token könnten sich die Behörden an Google oder Apple wenden und dort weitere Informationen zum dem Smartphone abrufen, welches das Token registriert hat: Telefonnummer, IMEI, und MAC- und IP-Adressen, SIM-Nummern usw.

  iPhones senden außerdem alle 5min die MAC Adressen aller Geräte im gleichen WLAN an Apple. Das ermöglicht u. U. erweiterte Auswertungen der sozialen Kontakte.

  Mit den Daten von Google/Apple könnten sich die Behörden an die Mobilfunkprovider wenden und bekommen dort die echten Namen, Adressen, Kontonummern. . . der gesuchten Personen (falls Google/Apple diese Daten nicht gleich mitliefern konnten).

  Mit Push-Token können ALLE Anonymisierungsversuche ausgehebelt werden. Es schützt kein VPN, kein Tor Onion Router und ein Threema-Account ist dann auch nicht mehr anonym. Die Kombination vieler Daten ist der Tod der Anonymität.

  Bei der Verfolgung eines Klima-Aktivisten, gegen den wegen Diebstahl und Wohnungseinbrüchen ermittelt wurde, verlangten französische Behörden via Europol vom E-Mail-Provider ProtonMail im September 2021 neben einem Logging der IP-Adressen vermutlich auch die Herausgabe der Push-Token.

Konfiguration von Push oder Poll in den Smartphone-Apps

- Auf dem iPhone verwenden alle Messenger immer Push-Nachrichten via APN, es gibt keine Alternative. Somit ist man auch bei der Verwendung eines Messengers ohne Telefonnummer auf iPhones nicht wirklich anonym.
- Für Android gibt es einige Messenger, die ohne Google Services arbeiten können:
  - In Threema 4.71+ kann man unter *Einstellungen* → *Über Threema* → *Fehlerbehebung* → *Threema Push benutzen* auf den eigenen Push Service von Threema umschalten.
  - Signal bietet auf der eigenen Webseite eine Version zum Download für Nutzer mit hohen Sicherheitsanforderungen, die keine Google Services nutzt.[40]

[40] https://signal.org/android/apk/

  - Telegram FOSS aus dem F-Droid Store verwendet keine Google Services.[41]
  - Im Session-Messenger kann man Google Push deaktivieren und statt dessen Polling aktivieren. Dann kann man aber nicht mehr angerufen werden.

  Messenger funktionieren ohne Google Push (FCM) nur, wenn man den Apps *Hintergrundaktivität* und *Hintergrunddatenverkehr* erlaubt! Bei einigen Smartphones muss man zusätzlich die Option *für Akku Betrieb nicht einschränken* für diese Apps aktivieren.

  enn man Wert auf Anonymität legt und nicht möchte, dass sein Messenger Account mit einer Telefonnummer verknüpft wird (Threema, Session Messenger o ä.), muss man nach der Deaktivierung von FCM Push auch einen neuen Account erstellen. Der alte Account, der mit FCM genutzt wurde, ist verbrannt. Google kann ihn mit einer Telefonnummer usw. verknüpfen und stellt diese Information auch den *Diensten* zur Verfügung.

- E-Mail-Server müssen nicht unbedingt Push-Services unterstützen. Deshalb bieten alle E-Mail-Apps für die allgemeine Verwendung die Möglichkeit, *Polling* für jeden Server zu konfigurieren.

- Bei speziellen E-Mail-Apps für einen besonderen Dienst ist es bei Android unterschiedlich. Tutanota verwendet keine Push-Servcies für die Android-App. Die Protonmail-App verwendet ausschließlich Googles FCM Push-Services und bietet keine Alternative.

- Banking-Apps, die man für das Online-Banking benötigt, verwenden i. d. R. Push-Services, da man sich nicht die Mühe der Implementierung einer Alternative macht.

- Google-freie Alternativen für das Android-Betriebssystem wie das auf Sicherheit und Privatsphäre optimierte GrapheneOS für Pixel-Smartphones unterstützen standardmäßig keine Google-Services-FCM. (Damit sind einige Apps auf diesen Systemen nicht nutzbar.)

21.8 Tracking blockieren

Auf dem Desktop-PC installiert man einen AdBlocker im Browser. Auf einem Smartphone ist das Blockieren von Tracking kompliziert, da fast jede App Trackingdienste einbindet. Einige Apps verwenden bis zu 40 Trackingdienste, die die Nutzung beobachten.[42]

Die Verbindungen zu Tracking- und Werbeservern könnte man auf DNS-Ebene blockieren. Aus technischer Sicht handelt es sich dabei um die klassische Zensur. Der Nutzer zensiert den Zugriff auf Trackingserver, indem er die DNS-Namensauflösung blockiert.

Seit Herbst 2020 funktioniert diese Form der Filterung immer schlechter und wird löchrig. Die Trackingdienste nutzen Anti-Zensur-Techniken, um die Filterung zu umgehen:

- Apple unterstützt die Trackingdienste dabei mit der Implementierung von DNS-over-TLS oder DNS-over-HTTPS in iOS Version 14+. Apps haben die Möglichkeit, via DoT oder DoH mit wenig Code einen eigenen, unzensierten DNS-Server statt des Servers zu verwenden, der in den Systemeinstellungen konfiguriert wurde, und damit die Zensur durch den Nutzer zu umgehen. Ein Video erklärt die Schritte.[43]

[41] https://f-droid.org/de/packages/org.telegram.messenger/
[42] https://reports.exodus-privacy.eu.org
[43] https://developer.apple.com/videos/play/wwdc2020/10047/

- Android Nutzer beschweren sich seit September/Oktober 2020 in diversen Foren immer häufiger, dass ihnen in Spielen usw. nach kurzer Verzögerung beim Start Werbung angezeigt wird, obwohl Tracking- und Werbeserver auf DNS-Ebene blockiert wurden.

  Auch hier kommt ein eigener DNS-Server in der App zum Einsatz, der via DNS-over-TLS oder DNS-over-HTTPS die Blockade umgeht und das VPN durchtunnelt.

Wenn Anti-Zensur-Techniken entwickelt werden, dann müssen wir uns nicht wundern, wenn auch die Trackingbranche diese Techniken verwendet, um Blockaden zu umgehen.

Für weniger hochentwickelte Apps funktioniert die Zensur auf DNS-Ebene weiterhin. Für aktuelle Varianten von Andoid und iOS ist die Variante (2) empfehlenswert.

(1) Man könnte die Apps **Blokada** (Andoid, iPhone) oder **DNSCloak** (iPhone) installieren und als Trackingblocker nutzen. Beide Apps registrieren sich als VPN-Dienst, sodass andere Apps den Traffic über diese Filter-Apps schicken. Die Apps übernehmen die Auflösung der DNS-Namen und blockieren Verbindungen zu vielen Tracking- und Werbeservern. Blokada verwendet lokale Blacklisten für das Blockieren der DNS-Namen. DNSCloak überlässt die Filterung dem DNS-Server, den man auswählen kann.

Nachteilig bei diesen Lösungen ist, dass man kein anderes VPN mehr nutzen kann.

(2) Aktuelle Android- und iOS-Versionen unterstützen die Konfiguration eines DNS-over-TLS- oder DNS-over-HTTPS-Servers in den Systemeinstellungen. Wenn man einen DNS-Server mit Blocklisten für Tracking und Werbung auswählt, werden Tracking- und Werbungsserver auf DNS-Ebene zensiert und man kann gleichzeitig ein VPN nutzen.

Android unterstützt seit Version 9 (Pie) DNS-over-TLS. Die Option heißt *Privates DNS* und verbirgt sich in den erweiterten Einstellungen für *Netzwerk & Internet*.

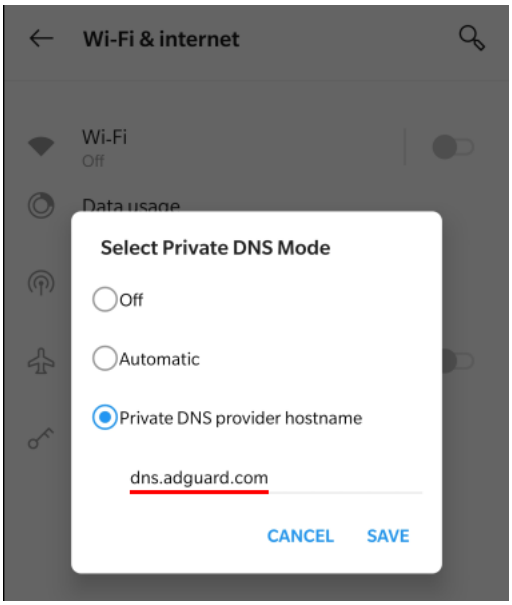


Abbildung 21.6: DNS-over-TLS-Server in Android konfigurieren (Privates DNS)

Es ist der Hostname eines DNS-over-TLS-Servers einzutragen, der Trackingdienste und Werbung blockiert. Die initiale Ermittlung der IP-Adresse des DoT-Servers erfolgt mit dem DNS-Server, der via DHCP zugeteilt wurde. Nach dem Captive Portal Check wird auf DNS-over-TLS umgeschaltet.

iPhones unterstützen verschlüsseltes DNS seit iOS Version 14. Die Konfiguration ist ein bisschen umständlicher als bei Android, aber machbar:

1. Man muss sich ein Konfigurationsprofil für den DNS-Server herunterladen. Es gibt mehrere Webseiten, die Profile für einige DNS-Server bereitstellen. Es ist aber empfehlenswert, ein signiertes Profil direkt vom Anbieter herunterzuladen, z. B. vom bekannten russischen DNS-Anbieter AdGuard.[44]
2. Dann ist das Konfigurationsprofil zu installieren (*Einstellungen → Profil geladen*) und die Warnung zu bestätigen, dass DNS-Einstellungen modifiziert werden.
3. Standardmäßig ist das zuletzt installierte Profil automatisch aktiv. Wenn man mehrere Profile für DNS-Server installiert hat, kann man in den Einstellungen unter *Allgemein → VPN & Netzwerk → DNS* das aktive Profil auswählen.

21.9 Zugriff auf Standortdaten einschränken

Im Dezember 2020 hat der norwegische Journalist M. Gundersen eine Recherche veröffentlicht, die demonstrierte, das viele Apps Standortdaten sammeln und an irgendwelche Firmen im Wilden Westen verkaufen, die aus den aggregierten Daten detaillierte Bewegungsprofile erstellen. Das muss man aber nicht einfach so akzeptieren.

iPhones bieten in den Einstellungen unter *Datenschutz → Ortungsdienste* die Möglichkeit, für jede App festzulegen, ob und wann sie den Standort abfragen darf (Abb 21.7).

Abbildung 21.7: Zugriff auf Standortdaten für iPhone-Apps konfigurieren

- Wenn kein Grund erkennbar ist, warum der Zugriff auf den Standort für die Funktionalität der App nötig sein sollte, dann wird der Zugriff gesperrt.
- Wenn man sich nicht sicher ist, ob es u. U. einmal sinnvoll sein könnte, der App Zugriff auf den Standort zu geben, wählt man *Nächstes Mal fragen* (z. B. Messenger).

[44] https://adguard.com/en/blog/encrypted-dns-ios-14.html

- Für Navigations-Apps u. Ä. ist es natürlich sinnvoll, dass die App während der Benutzung auf den genauen Standort zugreifen darf.
- Für Wetter-Apps u. Ä. wäre es hilfreich, wenn die App bei der Benutzung zumindest grob den Standort mit einer Genauigkeit von +/- 3km kennen würde. Für diese Apps kann man die Option *Genauen Standort* deaktivieren.

Um trotz dieser Einschränkungen den genauen Standort ermitteln zu können, sind Trackingfirmen wie Huq Industries[45] dazu übergegangen, das Standorttracking vor allem in Apps einzubauen, die einen exakten Standort benötigen (bspw. in Apps zur Warnung vor Radarfallen u. Ä.) und die MAC Adressen der WLANs der Umgebung auszuwerten, um anhand dieser Daten den Standort selbst zu berechnen. Es ist also nicht davon auszugehen, dass der eingebaute Schutz gegen Standorttracking zu 100 % funktioniert.

21.10 Browser Konfiguration

In den App Stores gibt es unendlich viele Apps, die nur wenig Mehrwert zum smartphonetauglichen Angebot der gleichnamigen Webseiten bieten aber im Hintergrund personalisiertes Tracking des Nutzers implementieren (Youtube, Tagesschau, Bahn.de... usw.) Außerdem gibt es Apps mit allgemein wenig Mehrwert. (Ich erinnere mich an eine App, die 2021/22 populär war und nichts weiter gemacht hat, als einen QR-Code zu scannen und diesen QR-Code bei Bedarf anzuzeigen).

Auf viele Apps kann man verzichten und statt dessen die Webseiten mit einem privacy-freundlich konfigurierten Browser in Kombination mit einem Passwortmanager (z.B. KeepasDX für Android oder Strongbox für iPhones) aufrufen. Man braucht nur wenige Klicks (Fingertipps) mehr für einen Login bei Bahn.de oder ähnlichen Webseiten und man wird weniger beobachtet.

Es gibt mehrere gute Browser für Smartphones, das Thema kann man endlos diskutieren.

Hier gibt es einen Vorschlag für die Konfiguration von **Fennec** (oder **Mull**) für Android. Beide Browser können via F-Droid Appstore installiert werden und basieren auf Firefox, wobei proprietäre Bestandteile und die Telemetrie entfernt wurden. Mulls enthält die arkenfox-user.js.

Trackingschutz

- Beim Beenden des Browser kann man alle Daten löschen, um langfristiges Tracking anhand von Cookies und Evercookies zu verhindern. Standardmäßig werden Cookies nicht gelöscht. Die Optionen findet man in den Einstellungen unter *Browserdaten beim Beenden löschen*. HINWEIS: Die Daten werden aber nur gelöscht, wenn man den Browser wirklich im Menü beendet! Sie werden nicht gelöscht, wenn man den Browser mit einer Wischgeste wegschiebt.

  Wenn man sich nicht daran gewöhnen kann, den Browser über das Menü zu beenden und ihn immer mit einer Wischgeste wegschiebt, kann man auch den Private Browsing Mode dauerhaft verwenden und die Links von anderen Apps im Private Browsing Mode öffnen.

- Den Werbe-und Trackingblocker uBlock Origin kann man in den Einstellungen unter *Add-ons* aktivieren und eine vorbereitete Konfiguration vom PrHdb importieren.[46]

- Zum Schutz gegen Fingerprinting des Browser kann man *resistFingerprinting* unter *about:config* aktivieren.

[45] https://blog.appcensus.io/2021/10/25/what-the-huq/
[46] https://www.privacy-handbuch.de/handbuch_21d2.htm

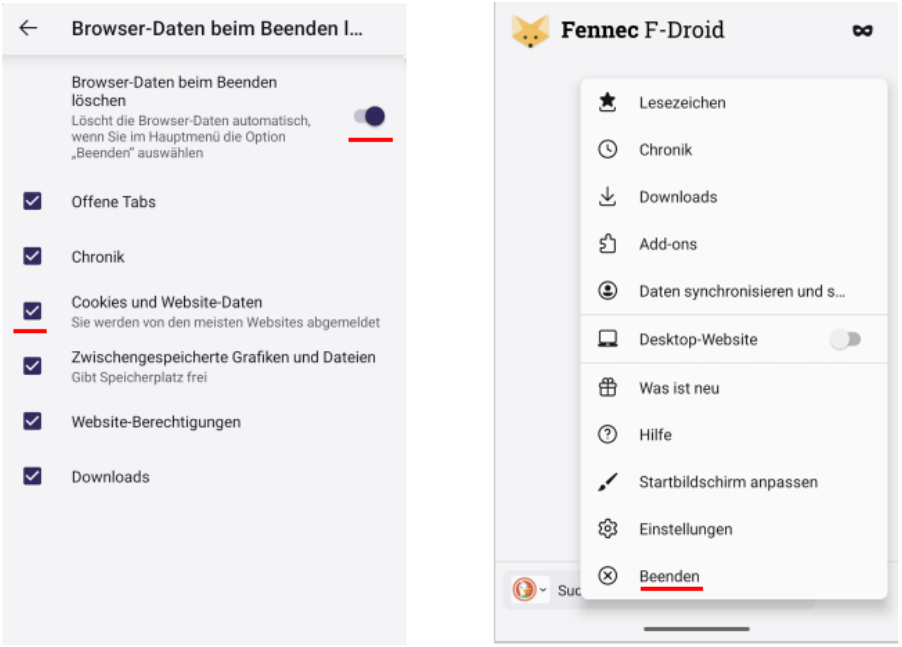


Abbildung 21.8: Fennec/Mull: alle Daten beim Beenden des Browsers löschen

```
privacy.resistFingerprinting = true
```

(Im Gegensatz zur Desktop Version von Firefox wird damit kein User-Agent Fake als Windows Browser aktiviert und kein seltsamer Fake der Bildschirmgröße.)

- Die Einstellung für das Senden des Referers kann man unter *about:config* anpassen:

```
network.http.referer.XOriginPolicy = 1
```

- Um Pricacy-Leaks via WebRTC zu vermeiden, sollte man folgende Einstellungen setzen:

```
media.peerconnection.ice.default_address_only = true
media.peerconnection.ice.no_host              = true
```

- Damit der Browser nicht bei jedem Start den Server *location.services.mozilla.com* angepingt, kann man folgenden Parameter unter *about:config* setzen:

```
browser.region.update.enabled = false
```

- Der Captive Portal Check ist in Fennec standardmäßig deaktiviert. Für den Login bei WiFi-Hotspots muss man den Standardbrowser des Systems nehmen.

HTTPS Sicherheit

- Den Nur-HTTPS-Mode kann man für alle Webseiten in den Einstellungen aktivieren.
- Zusätzlich kann man unter *about:config* folgende Optionen aktivieren:

```
security.ssl.require_safe_negotiation           = true
security.ssl.treat_unsafe_negotiation_as_broken = true
security.mixed_content.upgrade_display_content  = true
security.cert_pinning.enforcement_level         = 2
```

Passwortpeicher

Um die Risiken bei der Verwendung des integrierten Passwortspeichers zu minimieren, kann man den Passwortspeicher des Browsers abschalten und statt dessen KeepassDX nutzen.

Damit Login Credentials in Formulare übernommen werden können, muss KeepassDX im Hintergrund gestartet und die passende Passwortdatenbank geöffnet werden.

Telemetrie

Das Senden der Telemetriedaten deaktiviert man unter *about:config* mit folgenden Optionen:

```
datareporting.policy.dataSubmissionEnabled = false
datareporting.healthreport.uploadEnabled   = false
```

Telemetrie

- Nach Beobachtung des Google Sicherheitsteams nimmt seit 2021 die Bedrohung durch Zero-Day-Exploits, die Schwachstellen in Media-Codecs ausnutzen, kontinuierlich zu.

  Um Angriffe mit korrupten Mediadateien zu erschweren, kann man das automatische Abspielen von Medien abschalten. Videos startet man dann mit einem zusätzlichen Tippen:

  ```
  media.autoplay.default         = 5
  media.autoplay.blocking_policy = 2
  ```

- Die Javascript JIT Compiler kann man deaktivieren, um die Angriffsfläche zu reduzieren:

  ```
  javascript.options.baselinejit   = false
  javascript.options.ion           = false
  javascript.options.native_regexp = false
  ```

- Die Vibrator-API kann in Kombinationen mit anderen Mechanismen die Privatsphäre gefährden, wie das W3C in den Security and Privacy Considerations schreibt, deshalb:

  ```
  dom.vibrator.max_vibrate_ms = 0
  ```

21.11 Fake-Handy-Nummern

Immer öfter muss man bei vielen Gelegenheiten eine Telefonnummer angeben. Man möchte z. B. einen Tisch in einem Restaurant reservieren (online oder im Restaurant) und das Restaurant möchte unbedingt eine Telefonnummer haben.

Man ist sich aber sicher, dass man nicht angerufen werden möchte, und fragt sich, in welchen Datensammlungen diese Informationen später ausgewertet oder verknüpft werden könnten. Man könnte einfach eine Fakenummer angeben, aber man möchte Dritte dabei nicht belästigen.

1. Die Bundesnetzagentur hat die *Drama-Nummern* für die Verwendung in Medienproduktionen gesperrt. Diese Nummern dürfen ohne Genehmigung verwendet werden:

```
(0)152 28817386
(0)152 28895456
(0)152 54599371
(0)171 39200-00 bis -99
(0)172 9925904
(0)172 9968532
(0)172 9973185
(0)172 9973186
(0)172 9980752
(0)174 9091317
(0)174 9464308
(0)176 040690-00 bis -99
```

Für das Festnetz gibt es folgende Drama-Nummern:

```
(0)30 23125 000 bis 999 (Berlin)
(0)69 90009 000 bis 999 (Frankfurt am Main)
(0)40 66969 000 bis 999 (Hamburg)
(0)89 99998 000 bis 999 (München)
(0)221 4710 000 bis 999 (Köln)
```

2. Für hartnäckige Fälle gibt es das Projekt *Frank-geht-ran*, wo wirklich jemand ans Telefon geht und den Anrufer abwimmelt oder SMS ungelesen entsorgt werden:

```
(0)163 1737743  (Mobil)
(0)521 16391643 (Festnetz)
```

Es ist praktisch, wenn man ein paar Fake-Nummern im Adressbuch hat. Alternativ speichert man sich ein Lesezeichen für dramanumbers.github.io, wo man bei Bedarf schnell eine zufällige Nummer abrufen kann. Wichtig ist, dass man bei Bedarf schnell eine passende Nummer findet.

Es kann (in seltenen Fällen) vorkommen, dass auch die Gegenseite diese Fake-Nummern kennt und nicht akzeptiert. Funktioniert nicht zu 100 % überall aber sehr oft.

OpenPGP-Verschlüsselung von E-Mails

Für die vertrauliche Kommunikation haben sich in den letzten Jahren Messenger etabliert. E-Mails werden nur noch für viele Belanglosigkeiten eingesetzt, sind aber bei der privaten Kommunikation auf dem Rückzug. Wer es unbedingt möchte, kann dennoch auch auf dem Smartphone OpenPGP für die E-Mail-Verschlüsselung nutzen. Aber:

> *Never store your private PGP key on your mobile phone. [...] Mobile phones are inherently insecure.* (Mike Cardwell)

Wenn der private Schlüssel auf einer OpenPGP-Smartcard gespeichert wird, verlässt er diese Umgebung nie und landet nie auf dem Smartphone. Die PIN zur Freigabe des Schlüssels wird zusammen mit den zu entschlüsselnden oder zu signierenden Daten an die Smartcard gesendet und das Ergebnis der Kryptooperation zurück an das Smartphone.

1. Auf dem Andoid-Smartphone benötigt man folgende Software, die man aus dem Google Play Store oder F-Droid Store installieren kann:

   - **OpenKeychain** kümmert sich um Ver-/Entschlüsselung und die Verwaltung der Schlüssel. Seit Mai 2015 wird der Yubikey via NFC als OpenPGP Smartcard unterstützt. Nitrokeys werden seit Februar 2017 von OpenKeychain via USB OTG nterstützt.
   - Die E-Mail-Programme **FairEmail** oder **K9mail** können direkt mit OpenKeychain zusammenarbeiten und integrieren Buttons zum Verschlüsseln bzw. Entschlüsseln von E-Mails.

2. Den Nitrokey bzw. Yubikey bereitet man am einfachsten auf einem PC vor (siehe GnuPG-Smartcards nutzen). Die OpenPGP-Smartcard-Funktion ist freizuschalten, die PIN und Admin-PIN ist zu ändern und die Schlüssel sind zu generieren.

3. Das neu erstellte Schlüsselpaar kann man auf dem PC in eine Datei exportieren (geheimen + öffentlichen Schlüssel!). Der geheime Schlüssel in dieser Datei enthält praktisch nur einen Verweis, welche Smartcard genutzt werden muss.

4. Diese Schlüsseldatei ist auf das Smartphone zu übertragen und in OpenKeychain zu importieren.

5. Außerdem muss man noch die öffentlichen Schlüssel der Kommunikationspartner in OpenKeychain auf dem Smartphone importieren. Diese Schlüssel kann man ebenfalls aus Enigmail exportieren, wenn sie dort vorhanden sind. Alle benötigten Schlüssel können markiert werden (STRG-Taste drücken, wenn der Schlüssel mit der Maus markiert wird) und in eine Datei zusammen gespeichert werden. Diese Datei wird ebenfalls auf das Smartphone übertragen und in OpenKeychain importiert.

21.12 Kill-Switch und Frontdoor

Eine Warnung: Jede kryptografische Anwendung braucht einen vertrauenswürdigen Anker. Üblicherweise geht man davon aus, dass der eigene PC oder das eigene Laptop ein derartiger vertrauenswürdiger Anker ist, über den man volle Kontrolle hat. Bei Smartphones kann man nicht davon ausgehen, dass der Nutzer volle Kontrolle über die Software hat.

1. Mit dem Kill-Switch[47] hat Google die Möglichkeit, auf Android-Handys beliebige Apps zu deinstallieren, zu installieren oder auszutauschen. Das iPhone[48] und Windows Phone[49] haben ebenfalls einen Kill-Switch. Jede Krypto-Anwendung aus den Markets muss also als potentiell kompromittiert gelten. Sie kann genau dann versagen, wenn man den Schutz am nötigsten braucht.

2. Im Rahmen des Crypto War 3.0 haben Conztanze Kurz (Sprecherin des CCC) und Konstantin v. Notz (Grüne) im November 2019 den Vorschlag unterstützt, dass Anbieter von Messaging Diensten eine modifizierte Version der App bereitstellen könnten, in der die Ende-zu-Ende-Verschlüsselung zugunsten der Strafverfolgung kompromittiert wurde. Diese Version könnte in Kooperation mit Google/Apple via Play/App Store auf den Smartphones der Zielpersonen verteilt werden.

[47] https://mashable.com/2011/03/06/android-kill-switch
[48] https://www.telegraph.co.uk/technology/3358134/Apples-Jobs-confirms-iPhone-kill-switch.html
[49] https://www.heise.de/-1131297

Diese *Frontdoor* genannte Option hätte einige Vorteile gegenüber einer *Backdoor*, die die Krypto aller Messaging Apps kompromittiert, oder gegenüber staatlichen Trojanern, die den Schwarzmarkt für Exploits anheizen und auch an nicht-staatliche Akteure verkauft werden.

3. Außerdem gibt es einige Frameworks, die die Sicherheit kompromittieren können:
   - Der Sicherheitsexperte C. Mulliner hat das *Dynamic Dalvik Instrumentation Framework for Android* entwickelt, mit dem man jegliche Kryptografie komplett aushebeln kann. In seinem Blogartikel weist C. Mulliner darauf hin, dass er zum Deployment des Frameworks nichts schreiben muss, weil für dieses Problem genügend Lösungen publiziert wurden.
   - Auch das *Xposed Framework* kann mit einem ähnlichen Trick Kryptografie komplett aushebeln oder die Datenschutzeinstellungen verschärfen (je nach Intention).

21.13 Angriffe mit (Staats-) Trojanern erschweren

Der in den Medien derzeit bekannteste Staatstrojaner ist die Pegasus-Suite der israelischen NSO Group. Mehr als 50.000 Opfer wurden mit diesem Trojaner ausspioniert (Stand: Sommer 2021). Dazu gehörten Menschenrechtsaktivisten, Journalisten (auch in europäischen Ländern wie Griechenland, Polen, Ungarn), aufsässige Politiker (Katalonien), EU-Politiker, US State Department, die Krypto-Handys des spanischen Regierungschefs und seiner Verteidigungsministerin usw.

Die Pegasus-Spionagesoftware ist in mehreren Preisstufen verfügbar:

- Einsteigerversion: bietet nur 1-Klick-Exploits zur Infektion von Smartphones. Das Target muss auf einen Link klicken o. Ä. um das Smartphone zu kompromittieren.
- Advanced Version: bietet nicht-persistente 0-Klick-Remote-Exploits für Smartphones.
- High End Version: bietet persistente 0-Klick-Remote-Exploits, die auch einen Reboot auf dem Smartphone überstehen.

Alternativen zu Pegasus sind der Trojaner Predator der griechischen Firma Intellexa oder Graphite von Paragon Solutions mit ähnlichen Fähigkeiten. Predator spielte im griechischen Abhörskandal 2022 eine wesentliche Rolle und wurde auf den Smartphones von hochrangigen Politikern und Journalisten nachgewiesen. BKA und Zitis interessieren sich für den Kauf von Predator.

Neben den staatlich organisierten Hackern gibt es auch Freiberufler auf dem Gebiet, die man im anheuern kann (*Hire a Hacker*). Diese Subjekte möchten gern anonym bleiben und bieten deshalb ihre Dienste meist im Darknet auf Tor Onion Sites an. Es kostet zwischen $500 bis $2.000 ein Smartphone hacken zu lassen. Man sendet dem anonymen Hacker via Kontaktformular die Telefonnummer der Zielperson (keine hochrangigen Politiker), überweist Geld als Bitcoins oder in Monero und bekommt innerhalb 24-72h eine Archiv mit dem Inhalt aller Daten des Zielphones oder einen Remotezugriff auf Phone wie mit der Pegasus Spyware, um das Opfer zu belauchen und sich Kontakte, Fotos, Chats usw. selbst herunterzuladen. (ABER Vorsicht: nicht alle Angebote im Darknet sind seriös und manche werden als Honeypots vom FBI betrieben.)

Es gibt keinen 100%igen Schutz gegen einen Angreifer, der nahezu unbegrenzte finanzielle Mittel zur Verfügung hat. Dennoch kann man Angriffe deutlich erschweren.

Die Sicherheitsfirma Kaspersky hat einige Tipps zum Schutz gegen Pegasus und andere Trojaner veröffentlicht. Das Team von GrapheneOS und wir vom PrHdb haben ein paar kleine Ergänzungen hinzugefügt:

Allgemein (für alle Smartphones)

- Immer die aktuellen Updates zeitnah einspielen (System und Apps).
- Nicht auf Links in Nachrichten klicken. (Nicht alle Kunden von Pegasus kaufen die teuren Versionen, die 0-Klick-Remote-Infektionen bieten.)
- Immer ein vertrauenswürdiges VPN nutzen, da TK-Provider seit 2020 staatliche Behörden beim Rollout von Staatstrojanern unterstützen müssen. Man sollte VPN-Provider wählen, die keine persönlichen Informationen abfragen.

  Statt der Apps der VPN-Provider sollte man native VPN-Apps wie Wireguard o. Ä. bevorzugen (sagt das Kaspersky Team). Die bevorzugte VPN-App sollte *Netzwerk-Kill-Switch* (Android) bzw. *Always-On-VPN* (iPhones) unterstützen.
- Das Smartphone öfters rebooten, da persistente Exploits teurer sind und selten genutzt werden. Ein persistenter 0-Click-Exploit für Android kostet bis zu 2,5 Mio. Dollar. Das nutzt man vorsichtig und spart es für wichtige Ziele auf. Für einige Trojaner wie zum Beispiel den iPhone Trojaner *TriangleDB* gibt es keine persistente Version.
- Gelegentlich sollte man den Smartphone-Akku auch vollständig entladen lassen (*phone dies the natural death*) um es von NoReboot-Trojanern zu reinigen.[50]
- Man kann die Zielerkennung erschweren, indem man Messenger verwendet, die nicht an Telefonnummern gebunden sind (Threema, Session), und nicht die Telefonnummern weitergibt. Man kann mit Threema oder Session Messenger auch telefonieren.
- Man sollte nicht den mitgelieferten Standardbrowser verwenden, sondern Firefox Focus (sagt Kaspersky) oder Mull Browser (für Android, Empfehlung vom PrHdb), was nicht generell unknackbar ist, aber viele Standardangriffe ins Leere laufen lässt.
- Auch ein standardmäßig mitgeliefertes E-Mail-Programm sollte man meiden und statt dessen Alternativen nutzen, um Angriffe ins Leere laufen zu lassen. Über einen 0-Click-Exploit in Apple Mail wurden bspw. die iPhones von Journalisten und Promis kompromittiert. Dieser Bug in Apple Mail existierte von iOS 3.1.3 bis 13.4.1 über einen Zeitraum von 10 Jahren.[51]

  Alternativen sind FairEmail bzw. K9Mail (Thunderbird) für Android oder Canary Mail für iPhones. Die E-Mail Apps sollte man so konfigurieren, dass Anhäge und Bilder nicht automatisch angezeigt werden, dass keine Vorschaubilder von Anhängen automatisch generiert werden und keine externen Elemente automatisch geladen und angezeigt werden.
- Ein gehärtetes Smartphone-OS verwenden (GrapheneOS legt die Latte höher).

Android (Kleinigkeiten insbesondere für Android-Phones)

- Die standardmäßig für SMS genutzte Google Messages App sollte man schon aus Datenschutzgründen durch *Silence* oder *Fossify SMS Messenger* ersetzen.
- Das Smartphone nicht rooten und eine Sicherheitssuite installieren, die warnt, wenn ein Jailbreak erkannt wird.

GrapheneOS (Kleinigkeiten zu Verringerung der Angriffsfläche)

- Um die Angriffsfläche auf das Hidden OS zu verringern, kann man *LTE only* für mobile Daten aktivieren und die veralteten Protokolle 2G + 3G sowie das neue 5G

[50] https://www.kaspersky.com/blog/what-is-noreboot-attack-and-how-to-protect-your-smartphone/43292/
[51] https://www.derstandard.de/story/2000117062213/angriffe-auf-journalisten-und-promis-schwere-luecke-auf-iphones-und

deaktivieren. *LTE only* kann man in GrapheneOS in den Einstellungen unter *Netzwerk & Internet → SIM Karten → Bevorzugter Netzwerktyp* aktivieren.

- Wenn man den *HTTPS-only Mode* im Standardbrowser Vanadium aktiviert, erschwert man das Einschleusen von bösartigem Zeugs in Webseiten. Außerdem kann man den JIT-Compiler für Javascript abschalten, um die Angriffsfläche zu verringern. Diese beiden Optionen kann man in den Einstellungen des Browsers Vanadium in der Sektion *Datenschutz und Sicherheit* aktivieren.

iPhones *iOS security is fucked!* (Sagte der CEO von Zerodium, 2020).

Bereits seit 2019 hat Apple einige signifikante Sicherheitsprobleme und es kursieren viele Exploits für iPhones auf dem Markt:

> *In den letzten Monaten haben wir einen Anstieg der Zahl der iOS-Exploits beobachtet, vor allem von Safari und iMessage-Ketten, die von Forschern aus der ganzen Welt entwickelt und verkauft werden. Der Zero-Day-Markt ist so überflutet von iOS-Exploits, dass wir kürzlich begonnen haben, einige von ihnen abzulehnen.*

- Apple hat die Zeichen der Zeit erkannt und in iOS 16 einen Blockiermodus (engl: lock down mode) implementiert, der in iMessages keine Dateien außer Bildern darstellt, Facetime-Anrufe von Unbekannten blockiert, den JIT-Compiler in Browsern deaktiviert, die USB-Schnittstelle abschaltet, Installation von Profilen blockiert u. a. m. Damit wird die Angriffsfläche deutlich verkleinert.

  Den *Blockiermodus* kann man in den Einstellungen unter *Datenschutz & Sicherheit* aktivieren. Man wird mehrfach darauf hingewiesen, dass man es wirklich nur in ganz besonderen Ausnahmefällen braucht, nur wenn wirklich ein Risiko besteht, dass man zu einer Zielgruppe für Hackerangriffe gehört usw. Aber wer weiß das schon, bevor man gehackt wurde?

- Kaspersky empfiehlt, iMessages und Facetime zu deaktivieren, da diese am häufigsten angegriffen werden. Da es für Apple keine Alternative für SMS-Versand und Empfang gibt, muss man damit auf SMS verzichten.

  (P.S. Nachdem die iPhones von Kaspersky Mitarbeiter bei der Operation Triangulation gehackt wurden, hat Kaspersky begonnen, alle beruflichen iPhones auszurangieren.)

Trojanerinfektion erkennen mit MVT (iPhones)

Mit dem Mobile Verification Toolkit (MVT) kann man Trojaner wie Pegasus oder Predator erkennen und auch von der CIA(?) seit 2019 großflächig in Russland, Israel und China eingesetzten Trojaner für die Operation Triangulation. Die Signaturdateien werden ständig erweitert.

Mit den öffentlich verfügbaren Trojaner-Signaturen kann man viele (Staats-) Trojaner erkennen. Aber diese Datenbanken sind nicht geeignet für den belastbaren Beweis, dass das Phone wirklich *sauber* ist. Ein negatives Ergebnis der Untersuchung ist eindeutig, aber ein positives Ergebnis (*kein Trojaner gefunden*) bedeutet nicht unbedingt, dass sich wirklich kein Trojaner auf dem Smartphone versteckt. Für eine halbwegs belastbare Aussage, ob das Phone sauber ist, benötig man Zugang zu nicht-öffentlichen Signaturdaten und Spezialwissen im Umgang mit dem Toolkit.

Mit MVT kann man iPhones und Android Smartphones hinsichtlich Trojanerinfektion untersuchen. Allerdings sind die Möglichkeiten unter Android limitiert. iPhones bieten mehr Informationen zur Analyse und daher bessere Möglichkeiten zur Erkennung von Trojanern.

Eine kleine Minimal-Anleitung, wie man mit MVT Trojanern auf iPhones erkennt:

1. Es ist keine gute Idee, ein möglicherweise infiziertes Smartphone (diese Möglichkeit muss man einkalkulieren, sonst würde man es ja nicht testen) mit seiner Arbeitsumgebung auf dem PC oder Laptop zu verbinden. Man braucht also erstmal eine Testumgebung, mindestens eine eigene VM in QubesOS oder extra Hardware.

   Es gibt Trojaner, die sich aggressiv weiterverbreiten wollen. Ich habe einen solchen Trojaner schon einmal in Aktion gesehen. Im Auto sitzend sagte meine Beifahrerin, dass sich ihr iPhone rasant entleert und sie mit dem Laden garnicht hinterher kommt. Bevor ich reagieren konnte, hatte sie das USB Ladekabel in die passende Buchse gesteckt, der Navi machte nochmal kurz Nöff und war dann erstmal tot.

2. Das iPhone Backup kann man unter MacOS im Finder erstellen, unter Windwos benötigt man iTunes und Linuxer können die Toolsammlung *libimobiledevice* verwenden.

   Unter Linux könnte man am einfachsten die Pakete aus den Repositories probieren:

   ```
   Ubuntu: > sudo apt install libimobiledevice-utils
   Fedora: > sudo dnf install libimobiledevice-utils
   ```

   Da das iPhone (hoffentlich) auf dem aktuellen Stand ist, sind die Pakete aus den Linux Repos oft zu alt und man muss die aktuelle Version von Github selbst kompilieren.[52]

   Wenn alles vorbereitet ist, schließt man das iPhone via USB an die Testumgebung an und erstellt ein verschlüsseltes(!) Backup. Das verschlüsselte Backup enthält mehr Daten und erleichtert somit die Analyse. Unter Linux setzt man zuerst ein Passwort:

   ```
   > idevicebackup2 -i encryption on
   ```

   ... und erstellt dann das verschlüsselte Backup vom iPhone:

   ```
   > idevicebackup2 backup --full /path/to/backup/
   ```

3. Das MVT Toolkit holt man sich von Github und Linuxer komplilieren es selbst:

   ```
   > sudo apt install git python3 python3-pip sqlite3
   > git clone https://github.com/mvt-project/mvt.git
   > cd mvt
   > pip3 install .
   ```

   Wie bei Virenscannern gibt es Listen mit Indikatoren, die auf eine Infektion hinweisen. Es gibt Indikatoren für Pegasus, Predator u. a. m. Die Listen aktualisiert man mit:

   ```
   > mvt-ios download-iocs
   ```

   Das iPhone Backup ist für die Analyse mit dem MVT Toolkit zu entschlüsseln:

   ```
   > mvt-ios decrypt-backup -d /path/to/decrypted /path/to/backup
   ```

   Dann startet man die Untersuchung des Backups mit folgendem Komando:

   ```
   > mvt-ios check-backup --output /path/to/output/ /path/to/decrypted
   ```

[52] https://github.com/libimobiledevice/libimobiledevice

Im Outputverzeichnis findet man die Ergebnisse der Analyse, die man abschließend mit den Listen der Indikatoren zur Erkennung von Infektionen abgleichen kann:

```
> mvt-ios check-iocs --iocs ~/iocs/pegasus.stix2 /path/to/output/
> mvt-ios check-iocs --iocs ~/iocs/cytrox.stix2 /path/to/output/
> mvt-ios check-iocs --iocs ~/iocs/malware.stix2 /path/to/output/
> mvt-ios check-iocs --iocs ~/iocs/wyrmspy_dragonegg.stix2 /path/to/output/
...
```

Der Parameter *–iocs* kann mehrfach in einem Kommando verwendet werden, so dass man das alles auch in ein Kommando packen könnte.

iPhone Spyware Analyzer von iMazing

Das Mobile Verification Toolkit (MVT) ist ein Kommandozeitentool für Spezialisten. Der *iPhone Spyware Analyzer* von iMazing[53] (für MacOS und Windows verfügbar) bietet eine grafische Oberfläche für Mäuschenschubser, die die Nutzung vereinfacht und im Hintergrund MVT instrumentalisiert.

Der iPhone Spyware Analyzer nutzt die öffentlich verfügbaren Trojaner-Signaturen und kann damit auch hochentwickelte Staatstrojaner wie Pegasus, Predator oder Operation Triangulation erkennen. Allerdings ist die Erkennung der Staatstrojaner auf Basis der öffentlich verfügbaren Signaturen nicht perfekt. Wenn kein Trojaner gefunden wird, ist es es kein Beweis, dass wirklich kein Trojaner auf dem Smartphone ist. Staatstrojaner jagen bleibt eine Aufgabe für Spezialisten.

Hauptanwendung für den Spyware Analyzer ist das Identifizieren kommerzieller Stalker- und Watchware, die heimlich (ohne Wissen des Nutzers) auf dem iPhone installiert werden und die auch bei Privatpersonen populär sind. Eltern versuchen damit, ihre Kinder heimlich zu überwachen, misstrauische Ehepartner installieren sich das Zeugs... usw.

Wenn man Stalker- und Watchware auf dem iPhone gefunden hat, könnten man versuchen, mit der Person zu reden, die es installiert hat, man könnte selbst versuchen, die Stalker-App zu identifizieren und zu deinstallieren oder man macht Tabula rasa (Rücksetzen auf Werkseinstellungen).

Trojanerinfektion erkennen mit TinyCheck

TinyCheck[54] ist ein OpenSource Tool von Kaspersky, dass den aus- und eingehenden Datenverkehr eines Smartphones analysiert und auf verdächtige Muster scannt. Es erkennt in erster Linie Stalking Trojaner, Trojaner die von bekannten Botnetzen gesteuert werden und ähnliches Zeugs.

Um TinyCheck zu nutzen, benötigt man einen Rasberry Pi Minicomputer mit einem aktuellen Debian Linux als Betriebssystem. Dieser Rasberry Pi benötigt zwei Netzwerkschnittstellen:

1. Ein WLAN Interface als Accesspoint für die zu testenden Smartphones.
2. Ein WLAN oder kabelgebundenes Netzwerk mit Verbindung zum Internet (zum Router).

Ideal, wenn der Pi einen kleinen Touchscreen hat, um TinyCheck im Kiosk Mode zu nutzen.

Die Installation von TinyCheck ist nicht schwer. Man holt sich den Quellcode von Github und ruft das Script zu Installation auf. Das Script fragt einige Einstellungen ab (welche Netzwerkschnittstelle als Accesspoint zu nutzen ist und welche für die Internetverbindung... usw.)

[53] https://imazing.com/de/spyware-analyzer
[54] https://github.com/KasperskyLab/TinyCheckb

```
> cd /tmp/
> git clone https://github.com/KasperskyLab/TinyCheck
> cd TinyCheck
> sudo bash install.sh
```

Nach der Installation kann man im Browser die Adresse *https://tinycheck.local* aufrufen, Tinycheck konfigurieren und die Trojanersignaturen (IOCs) importieren.

Die zu testenden Smartphones verbinden sich via WLAN mit dem Accesspoint des Rasberry Pi. Der mobile Datenverkehr via Mobilfunkprovider ist dabei zu deaktivieren (einige Trojaner bevozugen Mobilfunk, auch wenn ein WLAN vorhanden ist, um die Erkennung zu erschweren).

Dann sollte man auf dem Phone einige Aktionen ausführen wie SMS schreiben, Anrufe annehmen, Messages schicken... um einen evtl. vorhandenen Trojaner zu Reaktionen zu provozieren.

Nachdem man ca. 10min auf dem Phone rumgespielt hat, kann man sich das Ergebnis der Analyse des aus- und eingehenden Datenverkehrs auf dem Rasberry Pi anschauen.

Hinweis: Wenn TinyCheck bei einem Test keine Hinweise auf suspekten Datenverkehr findet, ist das kein Beweis, dass das Smartphone wirklich *sauber* ist. Es wurde nur im Testzeitraum keine seltsame Kommunikation festgestellt, was ein gutes Zeichen ist, aber kein Beweis.

Hilfe für Journalisten

Nachdem bekannt wurde, dass mehr als 200 Journalisten mit dem Pegasus-Trojaner angegriffen wurden, hat *Reporter ohne Grenzen* im Juli 2022 das *Digital Security Lab* in Berlin eröffnet. Dort schauen drei IT-Spezialisten sich die Smartphones und Computer von Journalisten an, die die Vermutung haben, dass sie gehackt wurden. Das Team kann pro Woche ca. 10 Handys analysieren. Kontaktadressen findet man auf der Webseite.[55]

21.14 Juice-Jacking-Angriffe

Juice Jacking nennt man Angriffe, die von USB-Ladestationen ausgehen. Kriminelle können öffentliche Ladestationen mit USB-Anschluss oder vergessene Ladekabel nutzen, um ein Smartphone zu komromittieren und Malware zum Datenklau zu installieren.

In Deutschland sind diese Angriffe kaum bekannt, weil es nur wenige öffentliche Ladestationen gibt. International ist man schon weiter bei der Bereitstellung öffentlicher Ladestationen an Flughäfen, in Hotels, in Verkehrsmitteln und anderen öffentlichen Plätzen.

Die Behörden von Los Angeles (USA) haben im November 2019 eine dringende Warnung vor öffentlichen Ladestationen für Smartphones mit USB-Anschluss veröffentlicht.[56]

Im April 2023 hat das FBI diese Warnung via Twitter für die gesamte USA ausgesprochen.

> *Travellers should avoid using public USB power charging stations in airports, hotels and other locations because they may contain dangerous malware.*

Moderne Smartphones haben einen Softwareschutz gegen diese Angriffe (in Android deaktivierbar). Das Smartphone sollte den Nutzer erst fragen, ob der Gegenüber vertrauenswürdig ist, wenn

[55] https://www.reporter-ohne-grenzen.de/hilfe/digital-security-lab
[56] http://da.lacounty.gov/community/fraud-alerts/juice-jacking-criminals-use-public-usb-chargers-steal-data

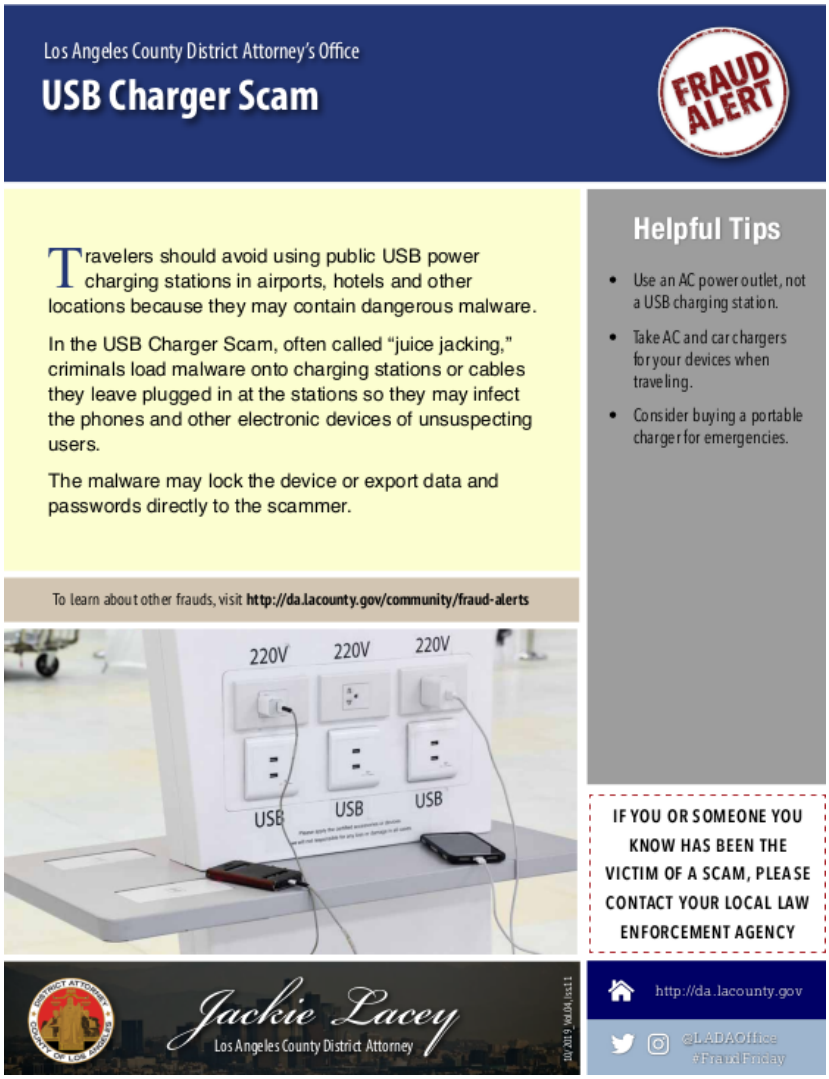


Abbildung 21.9: Warnung vor USB-Charger-Scam

eine Datenverbindung initiiert wird. Allerdings scheinen die Behörden von LA wenig Vertrauen in diesen Schutz zu haben.

Man kann natürlich seinen AC-Charger nutzen oder (wenn der Stecker mal nicht passt) eine Powerbank, die man via USB auflädt, um damit dann das Smartphone zu laden.

Außerdem gibt es das *USB Condom* oder *USB Data Blocker*. Das sind kleine Adapter für USB-Stecker, in denen nur die Kontakte für die Energieversorgung verbunden sind, aber nicht die Kontakte für Datenleitungen. Im deutschen Fachhandel gibt es diese Dinger noch nicht, aber man kann sie bei Amazon oder ähnlichen Händlern mit internationaler Lieferung bestellen.

21.15 IMSI-Catcher

Im Mobilfunknetz verbindet sich ein Smartphone mit einer Basisstation den Mobilfunkproviders. Das Samrtphone nutzt dabei in der Regel die Station mit dem stärksten Signal in der Nähe.

IMSI-Catcher simulieren eine Fake-Basisstation der Mobilfunkprovider und versuchen, die Smartphones in der Umgebung dazu zu überreden, die echten Stationen zu ignorieren und sich direkt

mit dem IMSI-Catcher zu verbinden. In Abhängigkeit vom Mobilfunkstandard (2G ... 5G) kann der IMSI-Catcher die Kommunikation beobachten, blockieren oder modifizieren.

- 2G ist ein veralteter, unsicherer Mobilfunkstandard, bei dem auch Inhalte der Kommunikation (Telefonie, SMS) ungeschützt gegenüber einem IMSI-Catcher sind. Telefonate können abgehört werden und SMS abgefangen oder modifiziert werden. IMSI-Catcher versuchen deshalb öfters ein Downgrad zu 2G zu erzwingen, indem sie die 3G/4G/5G Funkkanäle mit Jamming stören.
- Im 3G und 4G Standard wurde die Sicherheit etwas verbessert, aber es wurden mehrere Sicherheitslücken identifiziert, die eine Manipulation von Traffic ermöglichen könnten.
- Bei allen Mobilfunkstandards ist es möglich, Smartphones anhand der EMEI (2/3/4G) oder SUCI (5G) zu identifizieren, individuell die Position zu verfolgen oder es zu blockieren.
- Außerdem können IMSI-Catcher via Baseband angreifen und das Hidden OS exploiten.

Das BKA nutzte im Jahr 2022 insgesamt 38x IMSI-Catcher. Außerdem kommen IMSI-Catcher beim Schutz höchstrangiger Politiker zum Einsatz und unterschiedliche Akteure nutzen sie zu Spionage (beispw. in der Umgebung von Botschaften und Regierungsgebäuden).

- In Washington DC wurden 18 IMSI-Catcher in der Umgebung des White House und US Capitol sowie in der Nähe von Botschaften mit einem GSMK Cryptophone aufgespürt. [57]
- Auch in Oslo wurden IMSI-Catcher im Regierungsviertel gefunden. Journalisten einer Zeitung machten die norwegische Spionageabwehr darauf aufmerksam.[58]

In Sicherheitskreisen vermutet man, das die IMSI-Catcher in den Regierungsvierteln in erster Linie der Beobachtung dienen, wer in den verschiedenen Einrichtungen ein- und ausgeht.

Apps zur Erkennung von IMSI-Catchern (IMSI-Catcher-Catcher)

- Das GSMK CryptoPhone hat einen gut funktionierenden IMSI-Catcher-Catcher onBoard.
- Für Android gibt es keine aktuelle Software. *SnoopSnitch* u. ä. Apps sind veraltet.
- Auf dem 37C3 wurde im Vortrag What your phone won't tell you mit der App *CellGuard* ein IMSI-Catcher-Catcher für iPhones angekündigt. Die App soll 2024 veröffentlicht werden.

Schutzmaßnahmen gegen IMSI-Catchern

Die Nutzung des unsicheren 2G Mobilfunkstandards kann man in Android in den Einstellungen der Mobilfunkverbindung deaktivieren. Bei iPhones wird 2G abgeschaltet, wenn man den Blockiermodus (engl: lock down mode) unter *Datenschutz & Sicherheit* aktiviert.

Wenn man den Verdacht hat, dass sich das Phone mit einem IMSI-Catcher verbindet, weil eine IMSI-Catcher-Catcher App warnt oder weil man plötzlich mitten in einer modern ausgebauten Stadt statt der üblichen 5G nur noch LTE (4G) Verbindungen sieht oder gar UMTS (3G, was eigentlich flächendeckend abgeschaltet wird), dann bleibt als einzige Verteidigung, die Mobilfunkverbindung abzuschalten und ein (vertrauenswürdiges) WLAN zu suchen oder temporäre Nichterreichbarkeit in Kauf zu nehmen (Phone AUS).

[57] https://rt.com/usa/189116-washington-dc-spying-phone/
[58] https://www.zeit.de/digital/datenschutz/2014-12/norwegen-spionage-oslo

21.16 Das Hidden OS im Smartphone

In jedem Smartphone steckt neben dem End-User-Betriebssystem (Android, iOS, Windows Phone) und dem Linux-Kernel ein weiteres, verstecktes Betriebssystem. Dieses Hidden OS läuft auf dem Baseband-Prozessor und bearbeitet die Kommunikation mit den Mobilfunkstationen in Echtzeit. Es handelt sich dabei um ein Real-Time-Betriebssystem. Der Markt wird von Qualcomm mit AMSS dominiert, die Software ist Closed-Source.

Im Betrieb hat das Hidden OS die volle Kontrolle über die gesamte Hardware incl. Mikrofon und Kamera. Linux-Kernel und End-User-Betriebssysteme laufen als Slaves unter der Kontrolle des Hidden OS.

Die implementierten Sicherheitsstandards des Hidden OS stammen aus dem vergangenen Jahrhundert. Die Daten der Mobilfunkstationen werden z. B. ungeprüft als gültig übernommen. Security-Analysen sind schwierig, da jede Analyse zuerst ein Reverse-Engineering der Closed-Source-Software erfordert. Trotzdem stellen Sicherheitsexperten seit Jahren immer wieder gravierende Mängel vor:

- Weinmann stellte auf der DeepSec 2010 mit *All Your Baseband Are Belong To Us* einen Angriff vor, der mit einem nur 73 Byte großem Remote-Code-Execution-Exploit eine Backdoor öffnete und das Smartphone in eine Abhörwanze verwandelte.[59]
- Mit den *Hexagon challenges* wurde auf der PacSec 2013 ein verbesserter Angriff auf das Hidden OS von Rals Phillip Weinmann vorgestellt.[60]
- Forscher der TU Berlin demonstrierten auf dem *22nd USENIX Security Symposium* einen Angriff auf das Hidden OS, der nur geringe Ressourcen erforderte. Mit einigen manipulierten Smartphones wurden andere Smartphones in der Umgebung kompromittiert und der Empfang von Anrufen und SMS blockiert.[61]
- Das GSMK-Team demonstrierte 2013 einen Over-the-Air-Angriff auf Smartphones, bei dem zuerst das Hidden OS des Baseband-Prozessors durch ein *Over-the-Air-Update* kompromittiert und dann das Smartphone-OS (iOS und Android) angegriffen wurde. Alle verfügbaren Smartphones wurden erfolgreich kompromittiert.[62]

  > *Compromised phones can then be used to record conversations or gain access to sensitive data. It would also be possible to monitor content being accessed through pawned smartphones.*

  Der Angriff ist relativ aufwändig und wird daher wahrscheinlich selten eingesetzt, da es einfachere Möglichkeiten durch Verteilung kompromittierter Apps via Play Store o. Ä. gibt.

21.17 Smartphones löschen

Bevor man alle Daten auf dem Smartphone löscht, sollte man sich davon überzeugen, dass man die Daten auf ein neues Phone übertragen hat oder ein Backup der Daten hat.

- **iPhones** haben eine integrierte Löschfunktion, die alle (verschlüsselten) Daten wegputzt. Man findet sie in den Einstellungen unter *Allgemein* → *Zurücksetzen*.

[59] http://www.securitytube.net/video/5372
[60] http://pacsec.jp/speakers.html
[61] http://phys.org/news/2013-08-firmware-tweak-block-subscriber-berlin.html
[62] https://www.theregister.co.uk/2013/03/07/baseband_processor_mobile_hack_threat/Malware-flingers%20can%20pwn%20your%20mobile%20with%20over-the-air%20updates

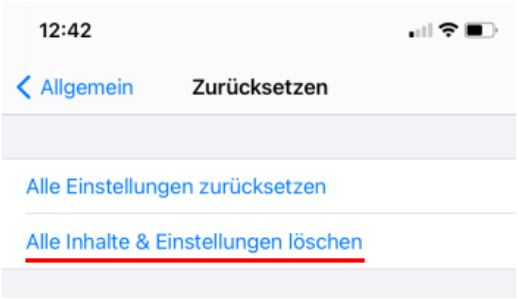


Abbildung 21.10: iPhone zurücksetzen und Daten löschen

- **Android** Smartphones sind ein bisschen komplizierter vollständig zu reinigen, wenn die Verschlüsselung der Daten nicht aktiviert wurde.

  1. Alle Accounts auf dem Smartphone löschen und in allen Apps abmelden.
  2. Das Smartphone auf Werkszustand zurücksetzen. Den Menüpunkt findet man üblicherweise in den Einstellungen unter *sichern und zurücksetzen*. Bei einigen Androids findet man es auch unter *System* → *Zurücksetzen*.
  3. Mit einem neuen Account im Google Playstore anmelden und die kostenlose Variante der App iShredder[63] oder die App Extiprater[64] aus dem F-Droid Store installieren.
  4. Die App iShredder bzw. Extiprater starten und die Datenspeicher löschen.
  5. Die App iShredder wieder deinstallieren und vom Playstore abmelden.
  6. Das Smartphone nochmals auf Werkszustand zurücksetzen.
  7. Die SD-Karte entfernen und an einem Computer neu formatieren.

  Wenn man die Datenverschlüsselung auf dem Android Smartphone aktiviert hatte, ist das Löschen mit iShredder oder Extiprater nicht nötig. Dann gibt es nach dem Zurücksetzen auf Werkszustand nur kryptischen Datenmüll auf den Datenträgern.

[63] https://play.google.com/store/apps/details?id=com.projectstar.ishredder.android.standard
[64] https://f-droid.org/packages/us.spotco.extirpater