

Privacy-Handbuch

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

9. Mai 2022

Inhaltsverzeichnis

| | | |
|----------|--|-----------|
| 1 | Scroogled | 7 |
| 2 | Angriffe auf die Privatsphäre | 17 |
| 2.1 | Big Data - Kunde ist der, der bezahlt | 18 |
| 2.1.1 | Google | 18 |
| 2.1.2 | Weitere Datensammler | 24 |
| 2.2 | Techniken der Datensammler | 26 |
| 2.3 | Tendenzen auf dem Gebiet des Tracking | 31 |
| 2.4 | Crypto War 3.0 | 34 |
| 2.5 | Fake News Debatte | 37 |
| 2.5.1 | Der Kampf gegen Fake News | 38 |
| 2.5.2 | Fake News Beispiele | 39 |
| 2.5.3 | Medienkompetenztraining | 43 |
| 2.5.4 | Fake News oder Propaganda - was ist der Unterschied? | 44 |
| 2.6 | Geotagging | 44 |
| 2.7 | Kommunikationsanalyse | 47 |
| 2.8 | Überwachungen im Internet | 49 |
| 2.9 | Terrorismus und der Ausbau der Überwachung | 55 |
| 2.10 | Ich habe doch nichts zu verbergen | 59 |
| 3 | Digitales Aikido | 63 |
| 3.1 | Nachdenken | 64 |
| 3.2 | Ein Beispiel | 67 |
| 3.3 | Schattenseiten der Anonymität | 68 |
| 3.4 | Wirkungsvoller Einsatz von Kryptografie | 69 |
| 4 | Spurenarm Surfen mit Firefox | 71 |
| 4.1 | Mozilla Firefox installieren | 72 |
| 4.2 | Datensparsame Suchmaschinen | 74 |
| 4.2.1 | Suchmaschinen in Firefox hinzufügen | 78 |
| 4.2.2 | Vorschläge bei Eingabe einer URL reduzieren | 80 |
| 4.3 | Cookies und EverCookies | 80 |
| 4.4 | Surf-Container | 85 |
| 4.5 | Werbung, HTML-Wanzen und Social Media | 86 |
| 4.5.1 | Tracking-Filter für Firefox | 88 |
| 4.5.2 | Tracking Protection in Firefox | 88 |
| 4.5.3 | uBlock Origin für Firefox | 90 |
| 4.6 | JavaScript | 92 |
| 4.6.1 | Browserfingerprinting mit Javascript | 92 |
| 4.6.2 | Sicherheitsbedenken bei Javascript | 97 |
| 4.7 | iFrames | 100 |
| 4.7.1 | iFrames allgemein blockieren | 100 |
| 4.7.2 | Integrierte Videos mit Click-2-Play laden | 101 |
| 4.7.3 | Googles reCAPTCHA und hCaptcha von Cloudflare | 101 |
| 4.8 | URL-Parameter | 102 |
| 4.9 | Zugriff auf lokale URLs blockieren | 103 |

| | | |
|----------|---|------------|
| 4.10 | Firefox activity-stream | 106 |
| 4.11 | Contextual Feature Recommender (CFR) | 109 |
| 4.12 | Browsercache und Surf-Chronik | 110 |
| 4.13 | Referer | 112 |
| 4.14 | Risiko Plugins | 113 |
| 4.14.1 | Media Plug-ins für Video und Audio | 113 |
| 4.14.2 | Anzeige von PDF Dokumenten | 114 |
| 4.15 | HTTPS-Verschlüsselung erzwingen und härten | 115 |
| 4.15.1 | Anzeige der HTTPS Verschlüsselung | 118 |
| 4.15.2 | Vertrauenswürdigkeit von HTTPS | 118 |
| 4.15.3 | SSL-Zertifikate via OCSP validieren | 120 |
| 4.15.4 | Tracking via TLS Session | 121 |
| 4.15.5 | Tracking via HTTP Strict Transport Security (HSTS) | 121 |
| 4.15.6 | Tracking Risiko durch seltsame Auswahl der SSL/TLS Cipher | 122 |
| 4.16 | Installierte Schriftarten verstecken | 122 |
| 4.17 | Hardware Fingerprinting | 124 |
| 4.18 | WebRTC mit Firefox | 125 |
| 4.19 | DNS-over-HTTPS mit Firefox | 128 |
| 4.20 | Sonstige Maßnahmen | 131 |
| 4.21 | Firefox Profile | 137 |
| 4.22 | Zusammenfassung der Einstellungen | 138 |
| 4.23 | Snakeoil für Firefox (überflüssiges) | 139 |
| 4.24 | Der Unsinn vom Spoofen der User-Agent Kennung | 142 |
| 5 | Spurenarm Surfen mit Librewolf | 145 |
| 5.0.1 | Installation | 145 |
| 5.0.2 | Anpassungen der Konfiguration | 145 |
| 6 | Passwörter und 2-Faktor-Authentifizierung | 147 |
| 6.1 | Hinweise für Passwörter | 148 |
| 6.1.1 | Firefox build-in Passwortspeicher | 150 |
| 6.1.2 | Passwortspeicher | 151 |
| 6.2 | Zwei-Faktor-Authentifizierung | 153 |
| 6.3 | Phishing Angriffe | 158 |
| 7 | Bezahlen im Netz | 160 |
| 7.1 | Anonyme Online-Zahlungen vor dem Aus? | 163 |
| 7.2 | Bargeld | 164 |
| 7.3 | Bitcoin | 166 |
| 8 | E-Mail Kommunikation | 168 |
| 8.1 | E-Mail Provider | 168 |
| 8.2 | ProtonMail und Tutanota | 170 |
| 8.3 | Mozilla Thunderbird | 172 |
| 8.3.1 | Begriffserklärungen: SMTP, POP3, IMAP, STARTTLS | 173 |
| 8.3.2 | Konfiguration des Assistenten zur Account Erstellung | 175 |
| 8.3.3 | Lesen von E-Mails | 177 |
| 8.3.4 | Sichere Konfiguration als E-Mail Client | 179 |
| 8.3.5 | Sichere Optionen für TLS-Verschlüsselung | 182 |
| 8.3.6 | Datenverluste vermeiden | 184 |
| 8.3.7 | Wörterbücher installieren | 184 |
| 8.3.8 | Spam-Filter aktivieren | 185 |
| 8.3.9 | Spam vermeiden | 185 |
| 8.3.10 | RSS-Feeds | 189 |
| 8.3.11 | Filelink | 190 |
| 8.4 | Private Note | 191 |

| | | |
|-----------|--|------------|
| 9 | E-Mails verschlüsseln | 193 |
| 9.1 | E-Mails verschlüsseln mit Thunderbird | 195 |
| 9.1.1 | Eigenen OpenPGP Schlüssel erstellen oder importieren | 196 |
| 9.1.2 | Eigenen OpenPGP Schlüssel mit GnuPG verwenden | 196 |
| 9.1.3 | Den eigenen öffentlichen Schlüssel verteilen | 197 |
| 9.1.4 | Fremde Schlüssel importieren | 198 |
| 9.1.5 | Fremde Schlüssel akzeptieren bzw. verifizieren. | 199 |
| 9.2 | Gedanken zum Mailvelope Browser Add-on | 199 |
| 9.2.1 | Mailvelope mit GnuPG nutzen | 201 |
| 9.2.2 | Mailvelope und Autocrypt | 201 |
| 9.3 | Einige Ergänzungen zum Thema GnuPG | 202 |
| 9.3.1 | Gedanken zur Auswahl und Stärke von Schlüsseln | 204 |
| 9.3.2 | GnuPG Smartcards nutzen | 204 |
| 9.3.3 | Adele - der freundliche OpenPGP E-Mail-Roboter | 207 |
| 9.3.4 | Memory Hole Project | 208 |
| 9.3.5 | Autocrypt | 209 |
| 9.3.6 | Verschlüsselung in Webformularen | 210 |
| 9.3.7 | OpenPGP-Verschlüsselung für Kontaktformulare | 211 |
| 9.3.8 | OpenPGP Keyserver | 214 |
| 9.3.9 | Web des Vertrauens (WoT) | 215 |
| 9.4 | Verschlüsselte Dokumente per E-Mail senden | 218 |
| 10 | Instant Messaging und Telefonie | 219 |
| 10.1 | Verschlüsselte Telefonie | 222 |
| 10.1.1 | SRTP/ZRTP Verschlüsselung | 223 |
| 10.1.2 | Verschlüsselt chatten und telefonieren mit qTox | 224 |
| 10.1.3 | Skype??? | 227 |
| 10.2 | Instant Messaging | 228 |
| 10.2.1 | Messenger Threema | 234 |
| 10.2.2 | Messenger Signal App | 236 |
| 10.2.3 | Messenger Telegram | 241 |
| 10.2.4 | Messenger basierend auf [matrix] | 248 |
| 10.2.5 | Chatten mit Jabber/XMPP | 250 |
| 10.2.6 | Messenger Wire | 252 |
| 10.2.7 | Einige weitere Messenger (unvollständig) | 253 |
| 10.3 | Videokonferenzen mit Jitsi Meet und BigBlueButton | 255 |
| 11 | Anonymisierungsdienste | 257 |
| 11.1 | Gedanken zur Anonymität | 257 |
| 11.2 | Was können Anonymisierungsdienste wie Tor? | 258 |
| 11.3 | Tor Onion Router | 260 |
| 11.3.1 | Security Notes | 263 |
| 11.3.2 | Anonym Surfen mit dem TorBrowserBundle | 264 |
| 11.3.3 | TorBrowser für Android Smartphones | 271 |
| 11.3.4 | OnionBrowser für iPhones | 271 |
| 11.3.5 | Sicherheitskonzept für hohe Ansprüche | 272 |
| 11.3.6 | Anonyme E-Mail Accounts | 275 |
| 11.3.7 | Anonym Bloggen | 277 |
| 11.3.8 | Anonymes Instant-Messaging | 278 |
| 11.3.9 | Gajim (Linux) und Tor Onion Router | 280 |
| 11.3.10 | Dateien anonym tauschen via Tor | 281 |
| 11.3.11 | Tor Onion Services | 283 |
| 11.3.12 | Tor Bad Exit Nodes | 287 |
| 11.3.13 | Tor Good Exit Nodes | 291 |
| 11.4 | Finger weg von unseriösen Angeboten | 293 |

| | |
|--|------------|
| 12 Anonyme Peer-2-Peer Netzwerke | 295 |
| 12.1 Invisible Internet Project (I2P) | 297 |
| 12.1.1 Installation des I2P-Routers | 297 |
| 12.1.2 Konfiguration des I2P-Router | 299 |
| 12.1.3 Anonym Surfen mit I2P | 300 |
| 12.1.4 I2P Mail 1 (Susimail) | 302 |
| 12.1.5 I2P Mail 2 (Bote) | 304 |
| 12.1.6 I2P IRC | 307 |
| 12.1.7 I2P BitTorrent | 308 |
| 12.2 DSL-Router und Computer vorbereiten | 310 |
| 13 Virtual Private Networks (VPNs) | 311 |
| 13.1 VPN Dienste als Billig-Anonymisierer | 314 |
| 13.2 Empfehlenswerte VPN-Provider | 315 |
| 13.3 IPsec/IKEv2 VPN Client mit Windows 10 | 317 |
| 13.4 Verschiedene VPN Lösungen für Linux | 318 |
| 13.4.1 OpenVPN mit Linux | 318 |
| 13.4.2 Wireguard mit Linux | 321 |
| 13.4.3 Firewall Kill-Switch-Konfiguration für VPNs mit UFW | 325 |
| 13.5 Das VPN Exploitation Team der NSA | 327 |
| 14 Domain Name Service (DNS) | 329 |
| 14.1 DNSSEC Validierung | 330 |
| 14.2 Verschlüsselung des DNS Datenverkehr | 330 |
| 14.3 Vertrauenswürdige DNS-Server | 332 |
| 14.4 DNS-Server der Big Player der IT Branche | 334 |
| 14.5 Konfiguration der DNS-Server | 335 |
| 15 Daten verschlüsseln | 338 |
| 15.1 Konzepte der vorgestellten Tools | 339 |
| 15.2 Gedanken zur Passphrase | 340 |
| 15.3 Dokumente verschlüsselt speichern | 343 |
| 15.4 Quick and Dirty mit GnuPG | 344 |
| 15.5 dm-crypt/LUKS für Linux | 345 |
| 15.5.1 Linux System komplett verschlüsseln | 345 |
| 15.5.2 Für Genießer in der Konsole mit cryptsetup | 346 |
| 15.5.3 Hardware Token verwenden (FIDO2, Nitrokeys, Yubikeys) | 350 |
| 15.5.4 LUKS-Nuke - hinterhältige Datenzerstörung | 355 |
| 15.6 zuluCrypt für Linux | 355 |
| 15.7 Backups verschlüsseln | 357 |
| 15.7.1 Schnell mal auf den USB-Stick | 357 |
| 15.7.2 Online Backups | 360 |
| 16 Daten löschen | 362 |
| 16.1 Dateien in den Papierkorb werfen | 362 |
| 16.2 Dateien sicher löschen (Festplatten) | 362 |
| 16.3 Dateireste nachträglich beseitigen | 363 |
| 16.4 Dateien sicher löschen (SSDs) | 364 |
| 16.5 Gesamten Datenträger säubern (Festplatten) | 365 |
| 16.6 Gesamten Datenträger säubern (SSDs) | 365 |
| 16.7 Datenträger zerstören | 366 |
| 17 Daten anonymisieren | 367 |
| 17.1 Fotos und Bilddateien anonymisieren | 368 |
| 17.2 PDF-Dokumente säubern | 368 |

| | |
|---|------------|
| 18 Daten verstecken | 371 |
| 18.1 Allgemeine Hinweise | 372 |
| 18.2 steghide | 372 |
| 18.3 stegdetect | 373 |
| 19 Betriebssysteme | 375 |
| 19.1 Microsoft Windows | 375 |
| 19.1.1 Telemetrie in Windows 10 | 376 |
| 19.1.2 Virescanner sind Snakeoil | 378 |
| 19.2 Apple MacOS | 379 |
| 19.3 Linux Distributionen | 380 |
| 19.3.1 Linux-taugliche Hardware | 382 |
| 19.3.2 Boot-Medium für die Linux Installation erstellen | 383 |
| 19.4 NetBSD und OpenBSD | 384 |
| 19.5 Risiko USB, Firewire und Thunderbolt | 384 |
| 19.6 Linux Firewall konfigurieren | 388 |
| 19.6.1 Uncomplicated Firewall (UFW) | 388 |
| 19.6.2 RHEL Firewall | 389 |
| 19.6.3 QubesOS Firewall | 390 |
| 19.7 WLAN Privacy Leaks | 390 |
| 19.7.1 MAC-Adresse faken (Windows 10) | 392 |
| 19.7.2 MAC-Adresse faken (Linux) | 392 |
| 19.7.3 Automatische Anmeldung für bevorzugte WLANs deaktivieren | 394 |
| 19.7.4 Hostname und DNS-Domain konfigurieren | 394 |
| 20 Smartphones | 396 |
| 20.1 Kommerzielle Datensammlungen | 397 |
| 20.1.1 Datensammlungen der Smartphone Hersteller | 397 |
| 20.1.2 Privacy-freundliche Alternativen für Android | 400 |
| 20.1.3 Datensammlungen mit Smartphone Apps | 401 |
| 20.2 Überwachung | 405 |
| 20.3 Aktivierung als Abhörwanze | 406 |
| 20.4 WLAN ausschalten, wenn nicht genutzt | 407 |
| 20.5 Push Services oder Polling nutzen | 410 |
| 20.6 Tracking blockieren | 411 |
| 20.7 Zugriff auf Standortdaten einschränken | 412 |
| 20.8 Krypto-Apps | 413 |
| 20.9 Stille SMS und IMSI-Catcher erkennen | 415 |
| 20.10 Angriffe mit Staatstrojanern erschweren | 416 |
| 20.11 Juice Jacking Angriffe | 417 |
| 20.12 Das Hidden OS im Smartphone | 417 |

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 entstieg, 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 wurde 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 war, dass er nun daheim herumsaß 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 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 aufnahmen; es hatte einen Tag lang Aufruhr in der Blogosphäre gegeben, während die Leute mit dem neuen Allesseher zu spielen begannen und an diverse Rotlichtviertel heranzoomten, 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 einzuschließen. 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 präsentieren, 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 anfangen, machen 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 roten, 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. Als 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 Hände 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 son Zeug. Ob sie es nun wollten oder nicht, Google hat inzwischen das Gleiche aufgezo-

“Greg, kommst du nun?”

Er blickte die Hände 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 wartete. 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 war 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 Fahrradständen 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 zogen. 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 Wöhrle 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 webseitenübergreifend zu erfassen.

Verglichen mit dem Beispiel *Zeitungslesen* 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...

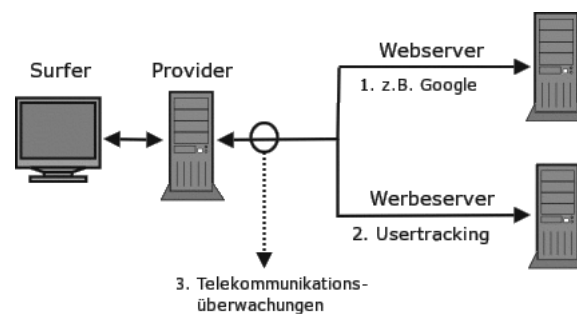


Abbildung 2.1: Möglichkeiten zur Überwachung im WWW

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)

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

Das weitere Wachstum des Imperiums scheint langfristig gesichert.

Zu spät hat die Konkurrenz erkannt, welches enorme Potential 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 wieder zu erkennen.

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 Websitebetreibern 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! (Reppesgaard: Das Google Imperium, 2008) Jeder Aufruf einer derart präparierten Website wird bei Google registriert, ausgewertet und einem Surfer zugeordnet. Neben kommerziellen Verkaufs-Websites, 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-Werbe-Programm 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.

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 35-44 Jahre alt ist. Die Informationen zu Bildung und Haushaltseinkommen müssen im Vergleich zu allgemeinen Statistiken der Bevölkerung bewertet werden, was hier mal entfällt.

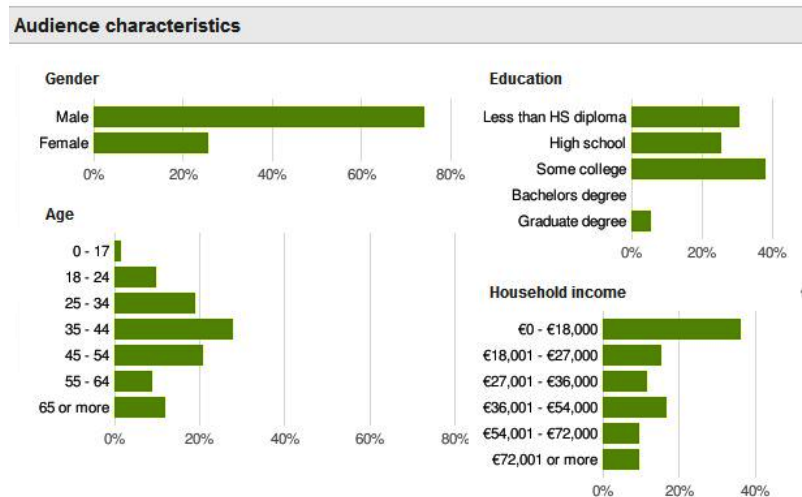


Abbildung 2.2: Ad-Planner Besucherstatistik (Beispiel)

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 ihn 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 bei dem 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... und Google+ (personalisierte Dienste)

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

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. Ein Pseudonym wird auch 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... Die Standortdaten werden ständig an Google übertragen, um sogenannte Mehrwertdienste bereit zu stellen (genau wie das iPhone die Standortdaten an Apple sendet). Smartphones sind als Lifestyle-Gadget getarnte Tracking Devices.

Wir wissen, wo u 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 datensammelnden 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 exklusive, 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 sec bis 1/100 sec schneller als andere unzensierte DNS-Server.

Natürlich werden alle Anfragen gespeichert und ausgewertet. Ziel ist, 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.¹

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 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 Dementis² und stellte klar, dass die Internetfirmen zwar den intern verwendeten 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 sicher³, dann kann man es als PR-Gag

¹<https://epic.org/2010/09/epic-files-suit-for-documents.html>

²<http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google-yahoo-co-nsa-anwalt-internetfirmen-wussten-von-ausspaehaktionen-12855553.html>

³<https://www.heise.de/-2138499>

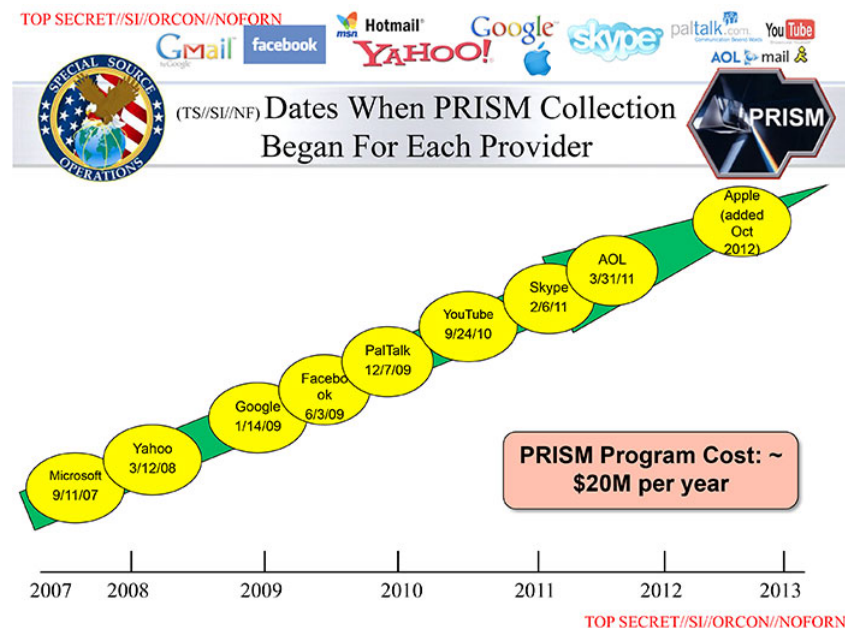


Abbildung 2.3: NSA-Folie zu den PRISM-Partnern

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 Projektes 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 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 Bild 2.4 der EFF.org zeigt.

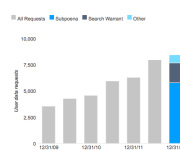


Abbildung 2.4: Steigerung der Auskünfte von Google an Behörden

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 zwei 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, Onlineshops...) verkaufen Informationen über Nutzer an Datenhändler (z. B. Acxiom, KaiBlue, RapLeaf...), welche die Daten anreichern, zusammenfassen und umfassende Profile den eigentlichen Endnutzern wie Kreditkartenfirmen, Personalabteilungen großer Unternehmen und Marketingabteilungen von Microsoft bis Blockbuster verkaufen.

Acxiom konnte bereits 2001, noch bevor Facebook als Datenquelle zur Verfügung stand, auf umfangreiche Datenbestände verweisen. Als das FBI die Namen der angeblichen 9/11 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 situierte Midlife-Single* oder *Goldener Ruhestand & aktiv....* Diese Hauptgruppen werden in bis zu 214 Untergruppen unterteilt nach Lifestyle-Aktivitäten (z. B. *Garten*, *Haustiere*, *Sport*, *Mode*, *Diät...*), Konsumverhalten, Milieuzuordnung (z. B. *intellektuell*, *statusorientiert-bürgerlich*, *traditionelles Arbeitermilieu*, *hedonistisch*, *konsummaterialistisch ...*) usw.

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 ein 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 Internettraffics beobachten, inklusive der Besucher bekannter Porno-Webseiten. Daten von offline Einkäufen werden von Firmen gekauft, die als Payment Processoren 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 Datenschutzpolicies der Portale kann man nachlesen, dass die sensiblen Persönlichkeitsdaten der Nutzer innerhalb der Match Group zwischen Portalen ausgetauscht werden.

Ein Beispiel: laut Tinder Datenschutz Policy⁴ werden folgende Daten gesammelt:

- Informationen, die Nutzer selbst angibt über Name, Ort, Alter, Geschlecht, sexuelle Vorlieben, Fotos, Videos...
- 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...
- 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 Gyroskop)
- 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.

⁴<https://www.gotinder.com/privacy>

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...10.

Towerd@ta 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 Preisliste⁵ 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

⁵<https://www.towerdata.com/email-intelligence/pricing>

ansprechen. Das und vieles mehr ist heute schon möglich.

Es geht aber längst nicht nur um die Einblendung von Werbung. Sarah Downey warnt⁶ 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 platzieren⁸. 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 immernoch 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.
- WebTrekkt 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 eingesetzt, die eine Verknüpfung der gesammelten Daten über mehrere Webseiten hinweg ermöglichen. WebTrekkt nutzt dafür Browser Fingerprinting.

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 und B. Cheng sowie P. Francis vom Max-Planck-Institut für Software Systeme haben ein Paper veröffentlicht, wie man homosexuelle Männer anhand der Klicks auf Werbung erkennen kann⁹. 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 vorhersagen¹⁰.

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

¹⁰<https://www.heise.de/-1820638>

Immer häufiger nutzen Kriminelle die großen Werbenetzwerke, um mit ihrer Schadsoftware möglichst viele Rechner anzugreifen. Kriminelle 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 2016.¹¹

EverCookies nutzen moderne HTML5 Techniken wie DomStorage, ETags aus dem Cache u.a. als Ersatz für Cookies, um den Surfer zu markieren und später anhand dieser Markierungen wiederzuerkennen. Der polnische Informatiker Samy Kamkar hat eine Webseite zur Demonstration von EverCookie Techniken¹² erarbeitet. 38% der populären Webseiten nutzen bereits verschiedene EverCookie Techniken (Stand: Okt. 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 Panopticlick¹³ 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 und 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 dem wiss. Paper *Perfect Pixel: Fingerprinting Fingerprinting Canvas in HTML5*¹⁴ 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 Grafikkarte und Besonderheiten im Soundsystem).

Die Studien *Dusting the Web for Fingerprinters*¹⁵ (2013) und *The web never forgets*¹⁶ (2014) der KU Leuven (Belgien) und OpenWPM (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 Browserfingerprinting als Trackingtechnik bei fast einem Viertel der Top 10.000 Webseiten eingesetzt wird, insbesondere bei News und Shopping Webseiten.¹⁷

¹¹<http://www.cyphort.com/about/news-and-events/press-releases/cyphort-labs-issues-special-report-on-the-rise-in-malvertising-cyber-attacks>

¹²<https://samyp.l/evercookie>

¹³<https://panopticlick.eff.org/browser-uniqueness.pdf> (PDF)

¹⁴<http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf>

¹⁵<http://www.cosic.esat.kuleuven.be/publications/article-2334.pdf>

¹⁶https://securehomes.esat.kuleuven.be/gacar/persistent/the_web_never_forgets.pdf

¹⁷<https://www.golem.de/news/browser-fingerprinting-neue-methoden-gegen-cookie-loses-tracking-2008-150518.html>

- *Bluecava* nutzt ausschließlich Browser Fingerprinting und protzt mit 30% besseren Ergebnissen als Cookie-basierte Techniken.¹⁸
- *Zanox.com* nutzt den Fingerprint des Browsers, wenn Cookies gelöscht oder per Browser-Einstellung blockiert werden.¹⁹
- *WebTrek* berechnet einen Fingerprint auf Grundlage von Geolocation anhand der IP-Adresse, Bildschirmgröße und Farbtiefe des Monitors, innere Größe des Browserfensters, bevorzugte Sprache, User-Agent des Browsers, Version des Betriebssystems sowie Einstellungen für Java, JavaScript und Cookies.²⁰
- *Multicounter* nutzt den Fingerprint zusätzlich zu Cookies oder EverCookies zur Verbesserung der Erkennungsraten.²¹
- *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 Trackindiensten *doubleverify.com*, *li-jit.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 sehr 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 hochgenauen Timern können Webapplikationen das Schreibverhalten der Surfer in Webformularen analysieren und als biometrischen Login verwenden (z. B. von der Firma KeyTrac angeboten) oder als Trackingfeature.

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.

Wischen, Tippen, Zoomen sind die üblichen Gesten für die Bedienung der Touchscreens auf Smartphones. Ein australisches Forschungsteam präsentiert auf der PETS 2018 das Paper *Quantifying the Uniqueness of Touch Gestures for Tracking*²², in dem gezeigt wird, dass diese Touchgesten individuell unterschiedlich sind und 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-Profilen tracken, birgt touch-based tracking das Potenzial, die eigentliche (physische) Person am Gerät zu tracken und zu identifizieren.

¹⁸<http://www.bluecava.com/visitor-insight-campaign-measurement>

¹⁹<http://blog.zanox.com/de/zanox/2013/09/11/zanox-stellt-tpv-fingerprint-tracking-vor/>

²⁰<http://www.webtrekk.com/de/index/datenschutzerklaerung.html>

²¹<http://www.multicounter.de/features.html>

²²<https://petsymposium.org/2018/files/papers/issue2/popets-2018-0016.pdf>

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. Es wird 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 Test²³ 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:

```
<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 beispielweise 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: ²⁴

We not only let you know when your document or PDF was opened, but we will also endeavor to let you know:

²³<https://emailprivacytester.com/>

²⁴<https://ssl1.readnotify.com/readnotify/pmdoctrack.asp>

- *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 weiter ausgebaut. Dabei wird es sowohl technisch durch die großen Datensammler immer weiter ausgebaut und durch politische Entscheidungen werden Datensammlungen 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 |

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 fall-kad.net*, *FeedBurner*, *Springs*, *Adscape*, *AdMob*, *Teracent*, *Invite Media*, *Admeld*, *Adelphic*, *Wildfire Interactive* u.a.m. aufgekauft. Nach dem OpenWPM Report von 2016 gehören die TOP5 Tracking Dienste alle zur Google Familie und von den TOP20 Tracking Diensten 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 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*, *aquanti-ve.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 hat Facebook eine Kooperation mit den Datenhändlern *Axiom* und *Datalogix* bekannt gegeben. 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 Bezahlssystem 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.²⁵
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

²⁵<http://www.latimes.com/business/technology/la-fi-tn-google-ads-tracking-20170523-story.html>

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.²⁶

- 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 Umverteilung von Geld) gilt jetzt auch das Sammeln und Auswerten von privaten Daten als eine Art Wertschöpfung, die neue Produkte ermöglicht, über die die Kunden mehrheitlich erfreut sein sollen.

Auf dem Wirtschaftstag 2015 hat Bundeskanzlerin Merkel sich gegen den Datenschutz und für diese neue Art der Wertschöpfung positioniert. Ihrer Meinung nach sind Daten der bedeutenste Rohstoff dieses Jahrhunderts und die Ausbeutung dieses Rohstoffes sollte nicht durch strenge Datenschutzrichtlinien beeinträchtigt werden.²⁷

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 schizophr 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 hat Bundeskanzlerin Merkel diese Linie der Bundesregierung nochmal bekräftigt und sich vom Grundprinzip der Datensparsamkeit als Leitlinie verabschiedet. 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.

²⁶<https://www.eff.org/deeplinks/2013/12/nsa-turns-cookies-and-more-surveillance-beacons>

²⁷<https://netzpolitik.org/2015/merkel-stellt-sich-gegen-datenschutz-und-netzneutralitaet/>

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 06. Okt. 2015 hat der Europäische Gerichtshof (EuGH) das Safe Harbour Abkommen für ungültig erklärt²⁸, dass 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 haben daraufhin erklärt, dass sie auch ohne Safe Harbour Abkommen so weitermachen wie bisher und die Daten europäischer Nutzer in die USA transferieren und dort verarbeiten werden²⁹. Sie sehen die EU-Standardvertragsklauseln nach Artikel 26, Absatz 2 der EU-Datenschutzrichtlinie von 1995 (EC95/46) als ausreichende Grundlage an. In dieser Ansicht werden sie von der EU-Kommision unterstützt.³⁰

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 Harbour*) 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 hat der britische Premierminister Cameron den **crypto war 3.0** mit der Forderung eröffnet, dass **jede Kommunikation für Geheimdienste einsehbar sein muss**. Weitere Politiker wie Obama, der damalige Bundesinnenminister de Maizièrre oder der australische Justizminister Keenan assistierten. Als hinreichender Grund wird der allgegenwärtige TERRORISMUS kolportiert, der unsere demokratischen Werte bedroht.

Ein generelles Verbot starker Kryptografie wird nicht ernsthaft diskutiert. Es wäre nicht durchsetzbar und eine kommerzielle Nutzung des Internets wäre praktisch tot.

²⁸<https://www.heise.de/tp/artikel/46/46186/1.html>

²⁹<https://www.golem.de/news/safe-harbor-urteil-google-und-microsoft-suchen-neue-wege-des-datentransfers-1510-116945.html>

³⁰http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm

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 Angriffs-Muster 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.
- 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 6 Monate und die Metadaten für 3 Jahre gespeichert werden. Der Versuch der Durchsetzung dieses Gesetzes gegenüber dem Messenger Telegram endete in einem Fiasco³¹. 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 Generalsschlüssels bei den Strafverfolgungsbehörden verpflichtet, um verschlüsselte Kommunikation entschlüsseln zu können. Anbieter von Messaging Diensten wie die 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. Nach seinen Vorstellungen 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 Nov. 2020 wurde der deutsche Vorschlag für eine Entschließung des EU-Rates verabschiedet, die 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 die entschlüsselten Inhalte den Behörden auf Wunsch zur Verfügung zu stellen. Konkrete Gesetze sollen folgen.
Die Datenschutzkonferenz von Bund und Ländern hat die Pläne zurück gewiesen. Die *Aushöhlung der Verschlüsselung*, wie vom EU-Rat gefordert, ist 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

³¹<https://www.golem.de/news/zensur-russland-zensiert-15-millionen-ips-fuer-telegram-sperre-1804-133895.html>

Teilnehmerin 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 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 das Benutzer eine Warnmeldung bekommt, und mit diesem Gerät alles mitlesen. (Vereinzelte waren Polizeibehörden mit der Methode bereits erfolgreich, weil Kriminelle mögliche Schutzfunktionen dagegen nicht aktivierten oder Warnungen ignorierten.)

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

Frontdoor Diskussion: Auf dem Grünen Polizeikongress im Nov. 2019 haben Constanze 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.³²

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 verschlüsselten 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, dass einzelnen US-Bundesstaaten den Erlass einer entsprechenden Verordnung ermöglicht aber auf US-Bundesebene nicht erzwingt.

Im August 2020 hat der für digitale Dienste zuständige EU-Binnenmarktkommissar T. Breton hat bestätigt, 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 300.00 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

³²<https://heise.de/-4595181>

den von Facebook oder Microsoft erkannten Videos handelt sich in der Regel nur um Lockangebote. Die echt harte Ware wird nicht auf Social Media Plattformen angeboten sondern auf Marktplätzen im Darknet.

Der Verlust der Haftungsprivilegierung würde für die 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 unkakulierbarem Risiko werden, wie der Betrieb eines Tor Exit Nodes.

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 Nov. 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.³³

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 die Online-Durchsuchung und Quellen-TKÜ verfügbar, die eine brauchbare Einsatzreife erlangt haben soll. Neben dem BKA möchte auch der Verfassungsschutz dieses Spielzeug einsetzen, beispielsweise 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 Dez. 2016 das staatliche Hacken von Tor- und VPN-Nutzern für das FBI massiv erleichtern, unabhängig davon, in welchem Land die Tor-Nutzer sich befinden.³⁴

Dass das FBI den TorBrowser knacken und installieren kann, haben sie 2013 und 2015 bewiesen. Der 2015 verwendete Exploit scheint 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, dass 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 Baron von Münchhausen

³³<https://netzpolitik.org/2016/bundesregierung-will-entschluesselungsbehoerde-schaffen>

³⁴<https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government>

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 Nov. 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* eingerichtet wie Correctiv oder die ARD/ZDF Faktenchecker, 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 deutschsprachigen Raum vom Recherekollektiv 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 NetzDG³⁵. 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).

3. Um die Deutungshoheit westlicher Mainstream Medien zu sichern und die Reichweite von Alternativen einzuschränken, überarbeitet Google seinen Suchalgorithmus:
 - Ende April 2017 hat Google eine Änderung seines Suchalgorithmus bekannt gegeben, 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 alternative Meinungen sucht.
 - Im Nov. 2017 hat Google CEO Erich Schmidt bekannt gegeben, dass die russische Nachrichtenseite RT.com und das Portal Sputnik News im Google News Service benachteiligt werden sollen, um die Reichweite zu reduzieren.³⁸

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.

(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.)

³⁵<https://netzpolitik.org/2017/un-sonderberichterstatter-netzwerkdurchsetzungsgesetz-verstoess-gegen-menschenrechte/>

³⁶<https://www.wsws.org/de/articles/2017/07/28/goog-j28.html>

³⁷<https://www.wsws.org/de/articles/2017/08/05/goog-a05.html>

³⁸<https://www.rt.com/news/410444-google-alphabet-derank-rt/>

2.5.2 Fake News Beispiele

Mir fallen spontan folgende Fake News aus den letzten 20 Jahren ein, die teilweise schwerwiegendere Folgen hatten als ein Wahlergebnis in Deutschland:

- FAKE: *Im Januar 1999 haben serbische Soldaten beim Massaker von Racak Zivilisten aus dem Kosovo massakriert.*

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 hat Fotos der OSZE-KVM und KDOM nach einem Kampf zwischen UCK und serbischer Armee ein bisschen zweckentfremdet verwendet. 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 hat sich an diesem völkerrechtswidrigen Angriff beteiligt.

- 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 des kuwaitischen Botschafters in den USA.

- FAKE: *Der Irak hat Massenvernichtungswaffen! Insbesondere verfügt Dikator Saddam Hussein über mobile Biowaffen Labore, die auf Tiefladern montiert sind und hochbeweglich.* (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.³⁹

- 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 unprofessional gearbeitet hat und unfähig war, Snowden festzusetzen. Russland hat ihm in auswegloser 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.

- 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%).⁴⁰

³⁹<http://www.faz.net/aktuell/politik/ausland/irak-krieg-keine-massenvernichtungswaffen-1175499.html>

⁴⁰<https://www.zeit.de/politik/deutschland/2016-11/afd-waehler-geringverdiener-spd-die-linke-forsa-umfrage>

- FAKE: *Steckt Russland hinter der Attacke auf Telekom-Router? Bundeskanzlerin Merkel und BND Präsident Kahl warnen angesichts des Telekom Hack 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.⁴¹

Der für den schrecklichen Angriff auf die Telekom Router verantwortliche Hacker wurde vom LG Köln zu eine Bewährungsstrafe(!) von 20 Monaten verurteilt.⁴²

- FAKE: *Russische Hacker wollen die Wahlen in Deutschland manipulieren und haben auch aktive in die Wahlen in Frankreich und den USA eingegriffen.* (Dieses Mantra wird ständig wiederholt, nicht nur in den Medien sondern auch im Verfassungsschutzbericht oder im Wikipedia Artikel über die Wahl in Frankreich.)

WAHR (nach Ländern sortiert):

- Eine kurze, klare Begründung, warum russische Hacker wahrscheinlich nicht in den deutschen Wahlkampf eingreifen werden, hat der Postillion in seiner typisch treffenden Art begründet.⁴³

Der russische Hacker Anatoli Fadejew ist verzweifelt: Schon bald ist Bundestagswahl und der 27-Jährige aus Sankt Petersburg hat sich immer noch nicht entschieden, ob er Angela Merkel (CDU) oder Martin Schulz (SPD) attackieren soll, um den jeweils anderen zu begünstigen. Offenbar findet der von Putin beauftragte Hacker beide diesjährigen Kanzlerkandidaten nicht überzeugend.

- Bezüglich der Präsidentschaftswahlen in Frankreich teilte der Chef der französischen Nationalen Agentur für Sicherheit der Informationssysteme (ANSSI), Guillaume Poupard, laut der Agentur AP mit, dass es keine Spur von russischen Hackerangriffen bei den Wahlen gab.⁴⁴
- Auch bei den US-Wahlen hatten sich keine russischen Hacker eingemischt. Laut Aussage von Assange wurden die Hillary-E-Mails von dem DNC-Mitarbeiter Seth Rich⁴⁵ an Wikileaks geliefert, der im Nov. 2016 beim Joggen erschossen wurde. Wikileaks versprach \$20.000 Belohnung für sachdienliche 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 haben in einem Memorandum an den US-Präsidenten die folgenden Schlussfolgerungen aus der Analyse veröffentlicht: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.)

⁴¹<https://www.heise.de/-3520212>

⁴²<https://www.golem.de/news/deutsche-telekom-router-hacker-bekommt-bewaehrungsstrafe-1707-129183.html>

⁴³<https://www.der-postillon.com/2017/07/hacker.html>

⁴⁴<http://www.washingtontimes.com/news/2017/jun/2/macron-hack-shows-no-sign-russian-involvement-desp/>

⁴⁵<https://de.sputniknews.com/politik/20170517315781593-usa-russland-leaks-hillary-mord>

⁴⁶<https://twitter.com/wikileaks/status/763041804652539904>

⁴⁷<https://consortiumnews.com/2017/07/24/intel-vets-challenge-russia-hack-evidence/>

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

In den Snowden Dokumenten und den Vault7 Leaks kann man nachlesen, wer weltweit in fremde Computersysteme eindringt. Davon kann das ständige Gerede von den bösen russischen Hackern nicht ablenken.

- Die Corona Krise 2020 ist 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)...

FAKE: Mein persönliches Fake News Highlight ist diese Meldung aus dem Bundesgesundheitsministerium vom 14. März (Twitter⁵⁰, Facebook⁵¹, ZDF⁵²):

! 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, die ab 23. März in Deutschland in Kraft traten: Kontaktverbot, Schließung der Geschäfte außer Baumärkte und Lebensmittelversorgung, Schließung der Restaurants, Bars, Spielplätze und des gesamten öffentlichen Lebens, Verbot von Reisen und Demonstrationen...

- 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 Sexangeboten in kompromittierende Situationen zu locken, Falschinformationen unter ihrem Namen im Netz zu publizieren oder Mails an Freunde und Kollegen unter ihrer Identität 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, das 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 orchestrierte.⁵³

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...) Durch eine Leak von internen Dokumenten der Integrity Initiative wurden weitere Kampagnen in Großbritannien, Italien und Norwegen bekannt:

⁴⁸<https://consortiumnews.com/2018/07/03/former-us-envoy-to-moscow-calls-intelligence-report-on-alleged-russian-interference-politically-motivated>

⁴⁹<https://www.cnet.com/news/over-40-of-republicans-think-bill-gates-will-use-covid-19-vaccines-to-implant-microchips/>

⁵⁰https://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.nachdenkseiten.de/?p=47955>

- 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 abgestempelt und als Gefahr für die Demokratie. Eine Analyse von ConsortiumNews⁵⁴ 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.
- Norwegen ist traditionell skeptischer gegenüber der US-Politik und zu wenig anti-russisch eingestellt. Norwegische Journalisten tendieren dazu, Informationen von russischer Seite die gleich Gewichtung zuzusprechen, wie Informationen aus westlichen NATO Ländern oder den USA. Seit 2016 ist die Integrity Initiative in Norwegen aktiv, um durch geeignete Maßnahmen etwas gegen diese gefährliche Starrköpfigkeit zu unternehmen.

Für russische Medien ist es *the biggest story of 2018*, in deutschen Medien habe ich mit Ausnahme von Telepolis^{55 56 57 58} fast nichts über die Integrity Initiative gelesen. Am gleichen Tag, als Anonymous die Dokumente über den deutschen Cluster der Integrity Initiative veröffentlichte, hat der Spiegel ein Fake News Fall im eigenen Haus publik gemacht und alle deutschen Medien waren mit Claas Relotius⁵⁹ beschäftigt. Als am 03. Jan. neue Dokumente zur Integrity Initiative veröffentlicht wurden, war in Deutschland der Promi-Leak⁶⁰ 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 seinem Youtube und Facebook Account veröffentlicht er emotional, menschlich 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 Berichterstatte.

In einem Interview mit BuzzFeed wurde er mit einigen seiner eigenen Aussagen konfrontiert und nach den Quellen gefragt. Seine Reaktion:⁶¹

...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 sich 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.

Auch auf der linken Seite gibt es Spinner, die mit der massenweise Abschachtung von Untermenschen eine neue Nazidiktatur verhindern wollen. Denken verboten?⁶²

⁵⁴<https://consortiumnews.com/2019/01/14/the-twitter-smearing-of-corbyn-and-assange/>

⁵⁵<https://www.heise.de/tp/features/Integrity-Initiative-Britische-Beeinflussungskampagne-gegen-Russland-4232365.html>

⁵⁶<https://www.heise.de/tp/features/Infowar-oder-Absurdistan-Britisches-Aussenministerium-im-Strudel-der-Desinformation-4253994.html>

⁵⁷<https://www.heise.de/tp/features/Neues-von-der-britischen-Beeinflussungskampagne-des-omioesen-Institute-of-Statecraft-4266174.html>

⁵⁸<https://www.heise.de/tp/features/Integrity-Initiative-taucht-ab-4286004.html>

⁵⁹<http://www.spiegel.de/kultur/gesellschaft/fall-claas-relotius-spiegel-legt-betrug-im-eigenen-haus-offen-a-1244579.html>

⁶⁰<https://www.heise.de/-4265180>

⁶¹<https://twitter.com/BuzzFeedNewsDE/status/1064538241880203264>

⁶²https://www.privacy-handbuch.de/diskussion.htm#08_01_19

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. 2.5 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.⁶³



Abbildung 2.5: 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 auszustiegen und von der Blindheit geheilt zu werden. Man muss es nur selbst wollen.

2.5.3 Medienkompetenztraining

Der beste Schutz gegen Fake News und Propagandalügen ist Medienkompetenz. Übereilte gesetzliche Regelungen oder Privatisierung der Wahrheitsfindung durch Unternehmen wie Facebook sind im Spannungsfeld von freier Meinungsäußerung keine Lösung.

Ein bisschen Medienkompetenztraining an Fake News Beispielen:

Quellen prüfen: Im Dez. 2016 kursierte das Gerücht, dass die syrische Armee bei der Befreiung Aleppo mehrere hochrangige NATO-Offiziere gefangen genommen haben soll, die dort die Rebellen bzw. Terroristen unterstützt haben sollen.

Als Quelle für diese Fake News wurde immer wieder der Nachrichtenkanal Russia-Today genannt und auf das Video *Syrischer UN-Botschafter nennt die Namen der gefangenen NATO-Offiziere im UN-Sicherheitsrat* verwiesen, das angeblich vom russischen Nachrichtensender RT.com stammen soll.⁶⁴

ABER: Man findet dieses Video nicht im Youtube Channel von RT.com, das RT-Logo ist amateurhaft in das Video hinein montiert und hat durch die Kompression die grafische Struktur verloren, der Hintergrund ist echt unprofessionell ausgeleuchtet. ... Zum Vergleich kann man sich ein echtes Video aus dem Youtube Channel von RT.com anschauen, Die Unterschiede zur professioneller Technik sind offensichtlich.

Die Story wurde von Voltaire.Net in Umlauf gebracht und ist frei erfunden.

⁶³<http://www.spiegel.de/politik/ausland/martin-schulz-ueber-afd-diese-typen-muss-man-bekaempfe-a-1078912.html>

⁶⁴<https://www.youtube.com/watch?v=VwrYluAvMPE>

Assoziation falscher Zusammenhänge: PI-News berichtet im September 2017 über die bayrische Kriminalstatistik:⁶⁵

Die Zahl der Vergewaltigungen ist im ersten Halbjahr 2017 im Vergleich zum Vorjahreszeitraum in Bayern um 47,9 Prozent angestiegen. [...] Gerade die Zahl der durch Zuwanderer begangenen Vergewaltigungsdelikte ist mit +90,9 Prozent ein Offenbarungseid gescheiterter Grenzsicherung.

Klartext: Ohne die massenhaften illegalen Grenzübertritte hätte es auch nicht den explosionsartigen Anstieg an Vergewaltigungen gegeben, nicht nur in Bayern.

Ursache für den Anstieg der Sexualstraftaten in der Polizeistatistik ist aber in erster Linie eine Verschärfung der Gesetze (neuer § 177 StGB). Jetzt gehören auch sexuelle Nötigungen und sexuelle Übergriffe zu den Vergewaltigungsdelikten. Ein nennenswerter Anstieg von Vergewaltigungen ist nicht vorhanden und damit auch keine explosionsartige Vergewaltigungswelle durch Zuwanderer.

Eine genauere Analyse⁶⁶ der Zahlen zeigt, dass die Zahl der Vergewaltigungen im Vergleich zum Vorjahr nur gering gestiegen ist, um 5% von 68 auf 71 und damit innerhalb der normalen Schwankungen. Die Zahl der tatverdächtigen Deutschen ist etwas gesunken und die Zahl der tatverdächtigen Zuwanderer ist von 8 auf 17 gestiegen. Ein explosionsartiger Anstieg durch 1,5 Mio Zuwanderer sieht anders aus.

2.5.4 Fake News oder Propaganda - was ist der Unterschied?

Fake News wird zu einem Modewort für alles, was irgendwie nach Propaganda riecht. Carter Page, Ex-Wirtschaftsberater des gewählten US-Präsident D. Trump, springt auch auf den Hype auf und bezeichnet beispw. die westliche Berichterstattung über die Ukraine-Krise und Krim als größte Fake News der letzten Zeit:⁶⁷

The recent history of Ukraine in general and Crimea in particular over the past several years may be among the most egregious examples of fake news in recent memory.

Nein, das war eine Propaganda Kampagne, die u. a. auch Fake News als Elemente verwendete. Ich erinnere mich z. B. an eine Meldung, dass die Aufständischen in der Ostukraine OSZE Beobachter gefangen genommen hätten. Das war nur eine Falschmeldung. (Die OSZE dementierte kurze Zeit später und es stellte sich heraus, dass die gefangen genommenen deutschen Offiziere in Spionagemission unterwegs waren.)

Es wurden neben Fake News auch alle anderen propagandistischen Methoden verwendet. Die Berichterstattung des ÖRR wurde vom Programmbeirat der ARD als fragmentarisch, tendenziös, mangelhaft und einseitig gerügt⁶⁸. Und das nennt man **Propaganda**.

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 24-30 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.

⁶⁵<https://www.heise.de/tp/features/Vergewaltigungen-in-Bayern-Herrmann-muss-Schockzahlen-zurechtruecken-3837889.html>

⁶⁶<https://www.heise.de/tp/features/Vergewaltigungen-in-Bayern-Herrmann-muss-Schockzahlen-zurechtruecken-3837889.html>

⁶⁷<https://www.rt.com/news/369828-russia-america-relations-trump-advisor/>

⁶⁸<https://www.heise.de/tp/features/Ukraine-Konflikt-ARD-Programmbeirat-bestaetigt-Publikumskritik-3367400.html>

- Die Analyse des Soziales 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 geographic coincidences*⁶⁹ zeigt, ermögliche 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.
- Mit den Geofencing Datensammlungen ist eine einfache **Überwachung** und **Einschüchterung** möglich. In der Ukraine wurden diese Daten bereits im Jan. 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.

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 Bild 2.6 zum Monitoring von politischen Demonstrationen nutzen kann.

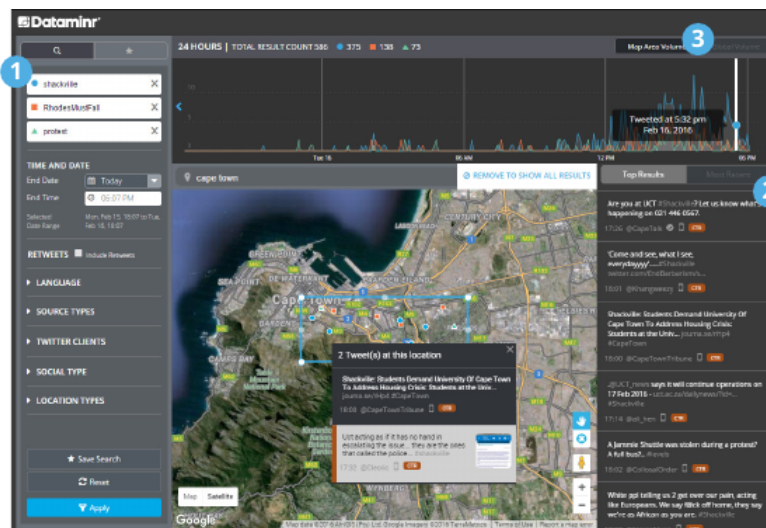


Abbildung 2.6: Auswertung der Twitter Postings eines Studentenprotestes in Südafrika aufgrund der Geolocation der Postings

- Die **Bewegungsanalyse** ermöglicht Aussagen über sehr private Details. Man kann z. B. durch die Analyse der Handybewegungen erkennen, ob jemand als Geschäftsreisender häufig 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*⁷⁰.

Das Magazin Wired berichtete im Danger Room (Oktober 2011), dass das FBI Smartphones bereits seit Jahren mit der Zielstellung der "Durchleuchtung der Gesellschaft"

⁶⁹<http://www.pnas.org/content/107/52/22436.short>

⁷⁰<https://www.heise.de/tr/artikel/Immer-im-Visier-276659.html>

trackt. Muslimische Communities 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*⁷¹.

Im September 2012 hat in den USA der Sixth Circuit Court of Appeals entschieden, dass bezügliche 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 beispielsweise 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 (iPhone, Laptops, PC...) 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.⁷²

Für die Datensammlungen rund um das iPhone wurde Apple mit dem BigBrother Award 2011 geehrt. Auszug aus der Laudation 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 Sicherheit⁷³, 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...). 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.

⁷¹<https://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims>

⁷²<https://www.apple.com/chde/legal/privacy/>

⁷³<https://www.heise.de/-2257924>



Abbildung 2.7: Lokalisierung eines Smartphones durch Facebook

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!

- Lokalisierungsdienste wie *Gowalla* oder *Foursquare* bieten öffentlich einsehbare Standortdaten und versuchen, durch spielartigen 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 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 krank geschrieben. Seine Ärzte rieten ihm zu einem Urlaub. Facebook-Fotos mit Surfbrett am Strand kosteten ihn erst das Krankengeld - und dann den Job.⁷⁴

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. mit systematisch 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.

⁷⁴<https://www.apotheke-adhoc.de/nachrichten/detail/pta-live/urlaub-trotz-krankengeld/>

Zivile Kommunikations-Analyse

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 bietet ein umfangreichen Datenpool oder die Kommentare in Blogs und Foren. 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 oder ...VZ werden analysieren kann, um omosexuelle 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...

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 (Bild 2.8). Dabei wird nicht nur die Anzahl der Kommunikationsprozesse ausgewertet, es wird auch die zeitliche Korrelation einbezogen.

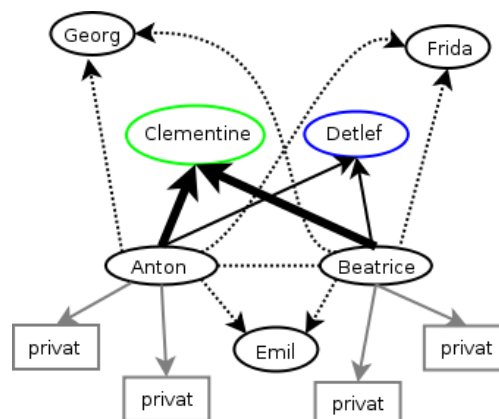


Abbildung 2.8: Soziales Netz von Anton und Beatrice

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 (Bild 2.9). Bei *Emil* handelt es sich evtl. um einen zufällig gemeinsamen Bekannten von *Anton* und *Beatrice*, der nicht in die "mg" eingebunden ist.

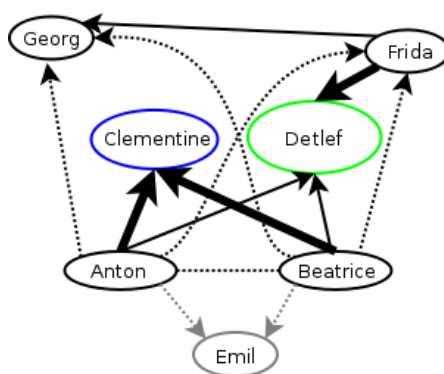


Abbildung 2.9: Präzisierte Struktur der "mg"

Reale Datenmengen

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 Bild 2.10 mit den Rohdaten erstellt.

Etwas besser aufbereitete Daten visualisiert Bild 2.11 mit den Kommunikationsdaten einer Woche von Ton Siedsmas.

Wenn man auch die Standortdaten des Smartphone mit auswerten kann, werden die Informationen deutlich detaillierter. Bild 2.12 zeigt einen Tag von Ton Siedsmas.

Analysertools wie *i2 Analyst's Notebook* von IBM oder *rola rsCASE* können diese Daten hübsch aufbereiten und die Schlapphüte bei der Analyse effektiv unterstützen (Bild 2.13).

2.8 Überwachungen im Internet

Eine umfassendere Übersicht zu verschiedenen Sicherheits-Gesetzen 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.⁷⁵

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

⁷⁵<https://www.daten-speicherung.de/index.php/ueberwachungsgesetze>

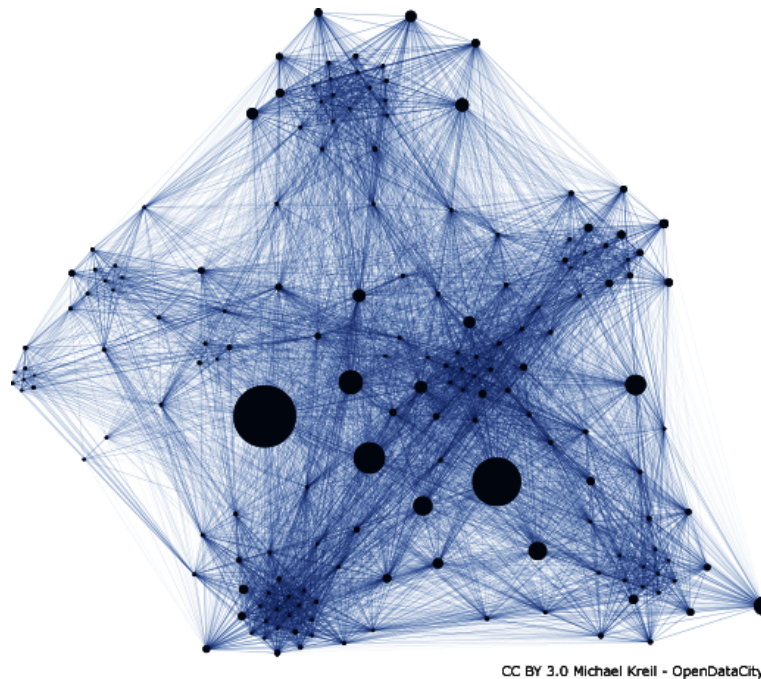


Abbildung 2.10: Kommunikationsnetzwerk von Malte Spitz

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.

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

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.

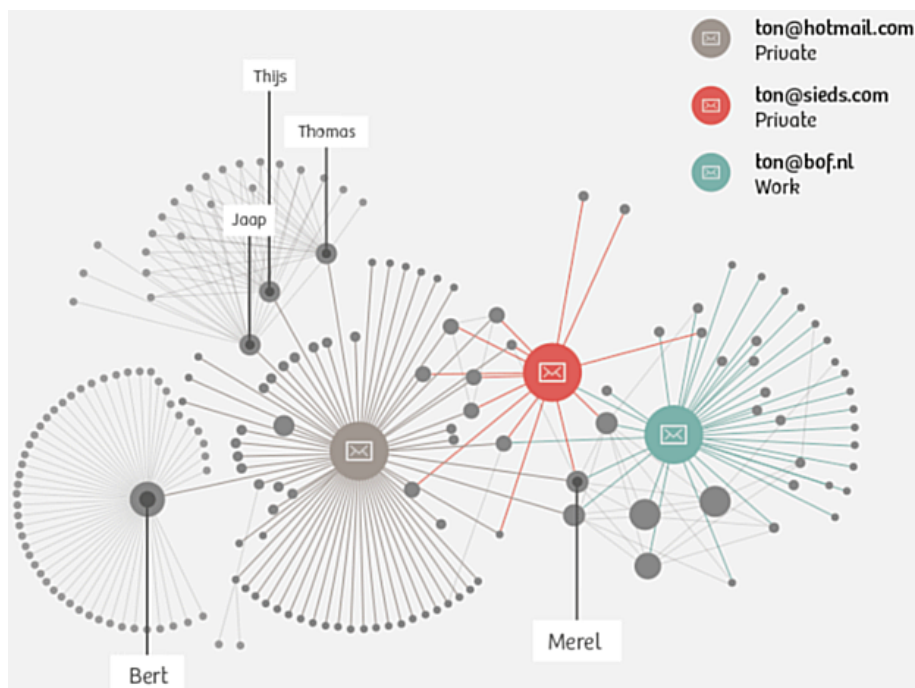


Abbildung 2.11: Aufbereitete Kommunikationsdaten von Ton Siedsmas

- 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 hat das EU-Parlament mit Mehrheit der christ- und sozialdemokratischen Fraktionen die Richtlinie zur 6-monatigen Datenspeicherung der Verbindungs- und Standortdaten (VDS) beschlossen (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 sondern als Maßnahme zur *Regulierung des Binnenmarktes* definiert, was außerdem die EU-Länder zu einer Umsetzung zwingt.
- 2006 hat der Wissenschaftliche Dienst des Bundestages ein Rechtsgutachten mit schweren Bedenken gegen die VDS vorgelegt.
- 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 keine Einfluss auf die Tendenz der Entwicklung hatte. Es gibt mehr Straftaten im Internet bei abnehmender Aufklärungsrate.

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

- 2010 erklärt das Bundesverfassungsgericht in einem Grundsatzurteil das Gesetz zur VDS als nicht vereinbar mit dem Grundgesetz. (Az: 1 BvR 256/08)⁷⁶
- 2012 zeigte das Max-Planck-Instituts (MPI) für ausländisches und internationales Strafrecht in einer umfangreichen wissenschaftlichen Analyse, dass KEINE Schutzlücke ohne Vorratsdatenspeicherung besteht und widerspricht damit der Darstellung von mehreren Bundesinnenministern und BKA-Chef Ziercke, wonach die VDS für die Kriminalitätsbekämpfung unbedingt nötig wäre. Die in

⁷⁶http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html

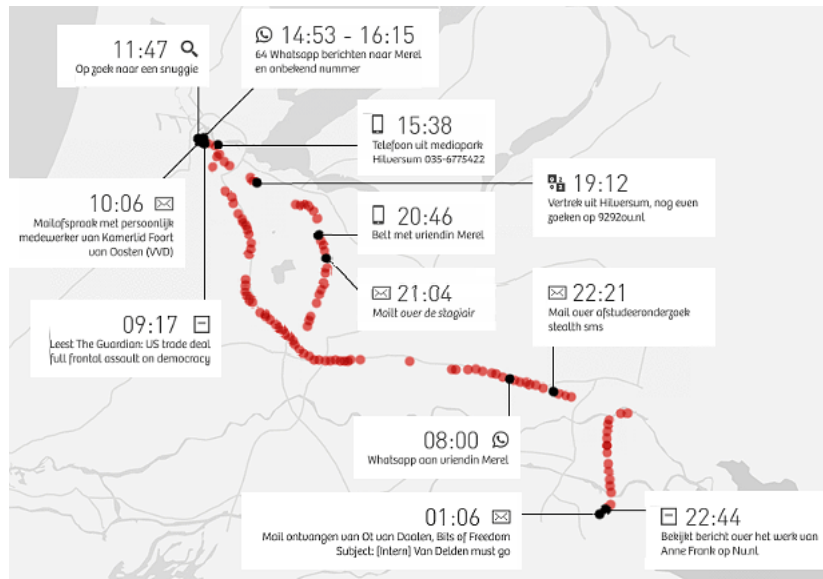


Abbildung 2.12: Standortdaten eines Tages von T. Siedsmas

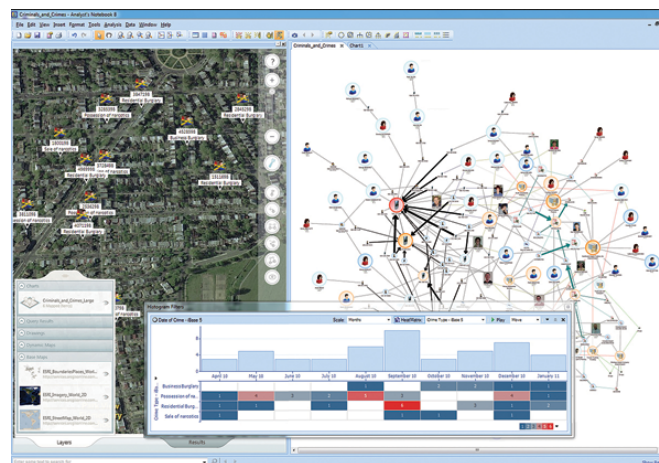


Abbildung 2.13: Screenshot von i2 Analyst's Notebook (IBM)

der Presse immer wieder herangezogenen Einzelbeispiele halten einer wissenschaftlichen Analyse nicht stand.⁷⁷

- 2012 gibt es einen nicht erfolgreichen Anlauf, die VDS international im Rahmen der UNODC als verpflichtende Richtlinie zu etablieren. Der Verfassungsschutz hat diesen Versuch offensiv unterstützt.⁷⁸
- 2014 wird 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 wird im Eilverfahren ein neues Gesetz zur *Speicherungspflicht für Verkehrsdaten* verabschiedet. Bundesjustizminister H. Maas konnte auf der Pressekonferenz zur Verabschiedung des Gesetzentwurfes im Bundeskabinett auf Nachfrage keinen Grund nennen, warum die Vorratsdatenspeicherung notwendig sein soll:

⁷⁷<https://www.ccc.de/de/updates/2012/mythos-schutzluecke>

⁷⁸<https://netzpolitik.org/2012/uno-bericht-der-kampf-gegen-terroristen-beginnt-im-internet-mit-vorratsdatenspeicherung-und-identifizierungspflicht/>

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 hat der Bundestag erneut das neue Gesetz zur Vorratsdatenspeicherung beschlossen. Verfassungsklagen wurden inzwischen eingereicht.
- 2017 legt der Wissenschaftliche Dienst zum wiederholten Mal ein Gutachten zur Vorratsdatenspeicherung vor, dass zu dem Schluss kommt, dass das aktuelle Gesetz nicht mit geltendem EU-Recht vereinbar ist. In mehreren Punkten verstößt das neue Gesetz gegen die Vorgaben des Europäischen Gerichtshofes.⁷⁹

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

Bestandsdatenauskunft Der IT-Sicherheitsforscher Pete Swire hat im April 2012 ein Paper⁸⁰ veröffentlicht, in dem er die aktuellen Tendenzen in der Überwachung aufzeigt. Weil das *Lauschen am Draht* in allen Variationen zunehmend uneffektiv 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 kommt der Gesetzgeber den Wünschen der Geheimdienste weit entgegen. Die Cloud-Provider und Mail-Provider sollen 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 allgm. 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 gäbe einen Millionen Euro schweren Massenmarkt, der durch Sperren von Webseiten empfindlich ausgetrocknet werden kann. Die Aussagen wurden geprüft und für falsch befunden⁸¹.

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.

⁷⁹<https://netzpolitik.org/2017/gutachten-gesetz-zur-vorratsdatenspeicherung-erfuellt-vorgaben-des-eugh-nicht/>

⁸⁰https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038871

⁸¹<http://blog.odem.org/2009/05/quellenanalyse.html>

2. In der zweiten Stufe wurde am 18.06.09 das *Zugangerschwernisgesetz* verabschiedet. Alle Provider mit mehr als 10.000 Kunden sollen diese geheime Liste von Websites zu sperren. Neben den (ungeeigneten) DNS-Sperren sollen auch IP-Sperren und Filterung der Inhalte zum Einsatz kommen.
3. Die CDU/FDP-Regierung ist im Herbst 2009 einen halben Schritt zurück gegangen und hat mit einem Anwendungserlass die Umsetzung des Gesetzes für ein Jahr aufgeschoben. Diese Regierung meint also, über dem Parlament zu stehen und ein beschlossenes Gesetz nicht umsetzen zu müssen.
4. Im Rahmen der Evaluierung des Gesetzes geht das BKA nur halbherzig gegen dokumentierten Missbrauch vor, wie eine Veröffentlichung des AK-Zensur zeigt. Gleichzeitig wird weiter Lobbyarbeit für das Zensurgesetz betrieben ⁸².
5. Die Auswertung des eco Verband zeigt, dass Webseiten mit dokumentiertem Missbrauch effektiv gelöscht werden können. 2010 wurden 99,4% der gemeldeten Webseiten gelöscht ⁸³. Auch 2011 und 2012 konnte das BKA 99% aller gemeldeten KiPo-Webseiten löschen lassen. Warum also die Internet-Stoppsschilder?
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 ⁸⁴. 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 und informellen Mitarbeitern...

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 ⁸⁵.

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

⁸²<http://ak-zensur.de/2010/08/kapitulation.html>

⁸³http://www.eco.de/verband/202_8727.htm

⁸⁴https://netzpolitik.org/wp-upload/bundestag_filter-gutachten.pdf

⁸⁵<http://www.berlinonline.de/berliner-zeitung/print/politik/725127.html>

Laut Gesetz kann die Überwachung auch ohne richterliche Genehmigung begonnen werden. Sie ist jedoch spätestens nach 3 Tagen einzustellen, wenn bis dahin keine richterliche Genehmigung vorliegt.

Präventiv-polizeil. 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 Verdächtigen 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 ⁸⁶
- Razzien im Vorfeld des G8-Gipfels waren rechtswidrig ⁸⁷
- Konstruieren und Schnüffeln mit §129a ⁸⁸
- Durchsuchungen beim LabourNet waren rechtswidrig ⁸⁹

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

Datenbanken: Begleitet werden diese Polizei-Gesetze vom Aufbau umfangreicher staatlicher Datensammlungen. Von der Schwarze 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 Vollerfassung der Bevölkerung voran getrieben. 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 Nov. 2015 eskaliert der Ausbau der Überwachung und wird als die angeblich einzige Alternative zum Schutz der Bevölkerung diskutiert. Die EU erlaubt Frankreich sogar die Verletzung der Euro-Stabilitätskriterien⁹⁰, weil durch den notwendigen(?) Ausbau des Überwachungsapparates nach den Anschlägen außergewöhnliche finanzielle Belastungen entstehen. Die Medien schockieren 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 2.14 auf Basis der Daten der *Global Terrorism Database*⁹¹ zeigt,

⁸⁶<http://de.indymedia.org/2008/10/228421.shtml>

⁸⁷<http://www.ag-friedensforschung.de/themen/Globalisierung/g8-2007/bgh.html>

⁸⁸<http://www.neues-deutschland.de/artikel/175230.konstruieren-und-schnueffeln-mit-s-129a.html>

⁸⁹<http://www.labournet.de/ueberuns/beschlagnahme/index.html>

⁹⁰<http://www.faz.net/aktuell/wirtschaft/haushaltspolitik-schutz-der-buerger-wichtiger-als-defizitziele-13917723.html>

⁹¹<http://www.start.umd.edu/gtd>

dass Europa hinsichtlich Terrorgefahr noch nie so sicher war, wie heute.

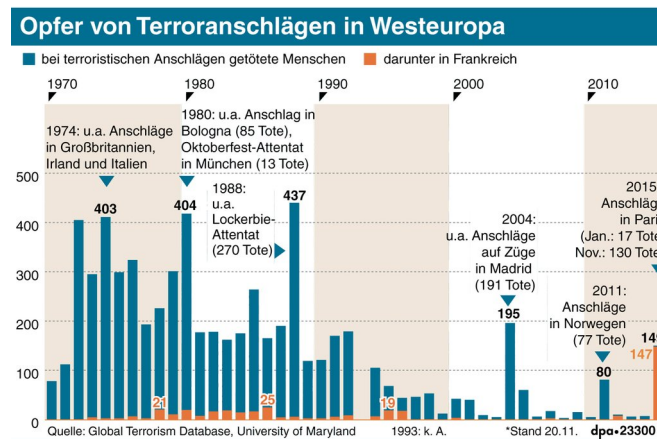


Abbildung 2.14: Opfer von Terroranschlägen in Westeuropa

Die jährlichen *EU Terrorism Reports* von Europol zeigen das gleiche Bild. 2005/2006 gab es fast 500 Terroranschläge pro Jahr in Europa, also mehr als ein Anschlag pro Tag und mehr als 700 Verhaftungen (siehe: TE-SAT Report für 2006⁹²). 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 Anschläge⁹³. Der Europol-Bericht TE-SAT 2014 listet noch 152 Terroranschläge mit 7 Toten auf, der niedrigste Stand.⁹⁴

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 jihadistischen Anschlägen vor allem in Frankreich. Dabei starben 148 Personen, da jihadistische Selbstmordattentäter eine möglichst hohe Zahl von Todesopfern erzielen wollen. 687 potentielle islamistische Attentäter wurden verhaftet, davon wurden 98% verurteilt.⁹⁵

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

In Deutschland gab es einen Anschlag in diesem Kontext, der Terrorist Anis Amri fuhr mit einem LKW im Dez. 2016 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, BKA und Verfassungsschutz waren über die Gefahr informiert, der marokkanische Geheimdienst hatte gewarnt und trotzdem...⁹⁶

Als Konsequenz aus dem Anschlag forderten Bundesinnenminister Thomas de Maizière (CDU) und andere Politiker reflexartig einen Ausbau der Überwachung. Insbesondere die

⁹²<https://www.europol.europa.eu/sites/default/files/publications/tesat2007.pdf>

⁹³<https://www.counterextremism.org/resources/details/id/229>

⁹⁴<https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014>

⁹⁵<https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014>

⁹⁶<https://www.heise.de/tp/features/Amri-TOP-1-der-Terrorabwehr-3914967.html>

Videoüberwachung steht auf der Wunschliste. C. Ströbele, ehem. Mitglied des Bundestages und der PKGr, zieht andere Konsequenzen aus dem Fall Amri:⁹⁷

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

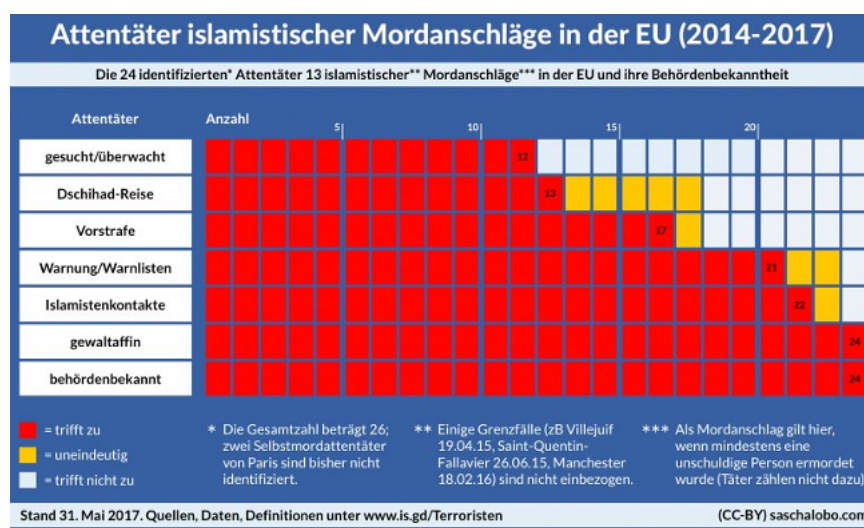


Abbildung 2.15: Alle 24 Terroristen mit islamistischen Hintergrund waren vor den Anschlägen als gewaltbereite Gefährder bekannt

Im Jahr 2019 gab es in Europa insgesamt drei erfolgreiche Terroranschläge mit jihadistischem Hintergrund und ein rechtsextremer Terrorangriff. 10 Personen sind dabei gestorben. Gegenüber den Vorjahren (2018: 7 Anschläge) und 2017 (10 Anschläge) ein Rückgang. Es wurden 1.004 Terroristen in Europa verhaftet. 115 geplante Terrorangriffe waren nicht erfolgreich und wurden verhindert. In Deutschland wurden 3 Anschläge verhindert und 35 potentielle Terroristen verhaftet, davon 32 mit jihadistischem 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. Österreichische Sicherheitsbehörden haben nichts unternommen - bis der Terrorist im Nov. 2020 ballend durch Wien lief und mehrere Menschen tötete. Ein WEGA-Team (Wiener Sondereinheit) konnten den Attentäter nach 9min 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. Warum wird dieses erfolgreiche Konzept jetzt nicht mehr diskutiert? Das Frankreich und Belgien auf diesem Gebiet der Integration massive Defizite haben, ist seit Jahren bekannt. Der vom franz. 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 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 der *Terror* gab es in der Vergangenheit weitere Beispiele von Panikattacken wie

⁹⁷<https://deutsch.rt.com/inland/61697-neue-vorwurfe-im-fall-amri-us-interessen/>

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 einigen Tagen 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 für ihre Interessen immer besser 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 sMittel, 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 2.16 zeigt die Länder, die seit 2010 Geld zur Finanzierung von Terrorismus bereitgestellt haben.

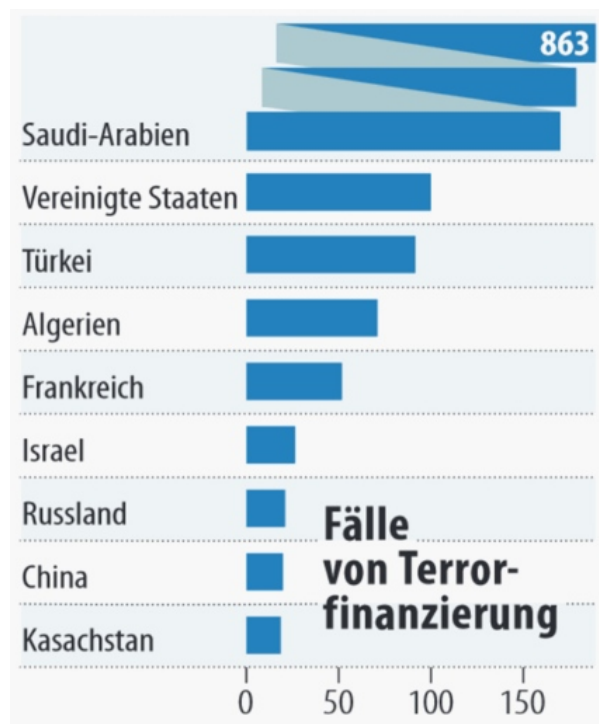


Abbildung 2.16: Staaten, die Terroristen finanzieren

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. Statt dessen werden die wirtschaftlichen Sanktionen gegen Syrien, Russland und den Iran aufrecht erhalten.

Auch Frankreich ist seit Jahrzehnten als Förderer von staatlichem Terrorismus bekannt und hat in afrikanischen Ländern mehrere blutige Putsche organisiert, weil die gewählten Regierungen nicht den neo-kolonialen Wirtschaftsinteressen von Frankreich folgten.⁹⁸

2.10 Ich habe doch nichts zu verbergen

Dies 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 willkürlich gesammelte Daten unser Leben gravierend beeinflussen können:

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 Datenanalyse (kommerzielle Datensammler, Anbieter von Software zur Mitarbeiterüberwachung, Geheimdienste) 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 Einkäufen 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, dass sie im Rahmen der Mitarbeiterüberwachung den Wunsch nach beruflicher Veränderung schneller erkennen können, als der betroffene Mitarbeiter sich selbst darüber im Klaren ist. 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 hat im Rahmen eines Selbstversuches mehrere E-Mails von seinem Gmail Account versendet mit kritischen Bemerkungen zu seinem Arbeitsverhältnis. Unmittelbar darauf konnte er Veränderungen in der personalisierten Werbung registrieren, die plötzlich auf Headhunter und kommerzielle Jobbörsen hinwies.

⁹⁸<https://www.heise.de/tp/artikel/46/46592/1.html>

Kein Studienplatz?

In Großbritannien werden Studienbewerber für bestimmte Fachrichtung geheimdienstlich überprüft. 739 Bewerber 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 Gesinnungs-Prüfungen sollen zukünftig ausgeweitet werden.⁹⁹

Einzelbeispiele

- Emma L. hatte sich auf dem Dating-Portal OkCupid zu einem Treffen verabredet. Das Date war ein Reinflall (kommt manchmal vor). Wenig später wurde ihr der Dating-Partner von Facebook als Freund empfohlen, in der *People You May Know* Section. Maria L. wurden ihre Tinder-Dates von Facebook als Freunde empfohlen. Es gibt auf Twitter noch viele weitere Beispiele für diese seltsamen Facebook Empfehlungen.¹⁰⁰

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.¹⁰¹

- Target ist einer der größte Discounter in den USA. Eines Tages stürmte ein wütender Vater in eine Filiale und beschwert sich, dass seine minderjährige Tochter Rabattmarken für Babysachen erhalten hat. Später musste der Vater kleinlaut zugegeben, dass seine Tochter wirklich schwanger war, er selbst aber nichts davon wusste. Target hatte die Schwangerschaft der minderjährigen Tochter an den kleinen Änderungen im Kaufverhalten erkannt.¹⁰²
- Im Rahmen der Zulässigkeitsprüfung für Piloten wurde Herr J. Schreiber mit den vom Verfassungsschutz gesammelten Fakten konfrontiert¹⁰³:
 1. Er wurde 1994 auf einer Demonstration kontrolliert. Er wurde nicht angezeigt, angeklagt oder einer Straftat verdächtigt, sondern nur als Teilnehmer registriert.
 2. Offensichtlich wurde daraufhin sein Bekanntenkreis durchleuchtet.
 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 besitzt. Bei dem sogenannten *Bauwagen* handelt es sich um einen Allrad-LKW, den Herr S. für Reisen nutzt (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 ging mit ihm zur Drogenberatung. In den folgenden Jahren gab es keine Drogenprobleme. Von der Bundeswehr erhält er eine Ablehnung, da er ja mit

⁹⁹<https://www.heise.de/tp/artikel/44/44538/1.html>

¹⁰⁰<https://twitter.com/search?q=facebook%20suggest%20tinder>

¹⁰¹<https://netzpolitik.org/2016/facebook-nutzt-standort-fuer-freundesvorschlaege/>

¹⁰²<http://www.tagebau.com/?p=197>

¹⁰³<http://www.pilotundflugzeug.de/artikel/2006-02-10/Spitzelstaat>

sechs Jahren eine Psychotherapie durchführen musste und Drogenprobleme gehabt hätte.¹⁰⁴

- Kollateralschäden: Ein großer deutscher Provider liefert falsche Kommunikationsdaten ans BKA. Der zu Unrecht Beschuldigte erlebt das volle Programm: Hausdurchsuchung, Beschlagnahme der Rechner, Verhöre und sicher nicht sehr lustige Gespräche im Familienkreis. Die persönlichen und wirtschaftlichen Folgen sind schwer zu beziffern¹⁰⁵.

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 Betroffenen zu unrecht verurteilt wurden, weil sie Opfer von Kreditkarten Betrug waren. 39 Menschen hatten Selbstmord begangen, da ihnen alles genommen wurde.¹⁰⁶

- “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 übernimmt 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 uns zu benachrichtigen. Wir bezeichnen die (repressiven) Folgen dann als Schicksal.

Politische Aktivisten

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

1. Erich Schmidt-Eenboom veröffentlichte 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*”¹⁰⁷ 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

¹⁰⁴<https://blog.kairaven.de/archives/998-Datenstigmaanekdoten.html>

¹⁰⁵<https://www.lawblog.de/index.php/archives/2008/03/11/>

¹⁰⁶https://en.wikipedia.org/wiki/Operation_Ore

¹⁰⁷<http://www.spiegel.de/politik/deutschland/0,1518,384374,00.html>

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. Es werden Bekannte und Freunde aus dem persönlichen Umfeld einbezogen. Sie werden in der AntiTerrorDatei gespeichert, auch ihre Kommunikation kann überwacht werden, es ist sogar möglich, Wanzen in den Wohnungen der Freunde zu installieren.

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 geeigneter 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 der 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 sWhistleblower 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 Wegwerfadressen 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 Einkaufen mit Lieferung, als IT-Nerd, als Wissenschaftler, als Fotograf oder als Blogger. ... 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 (beispw. als Blogger, Autor oder Händler), die nicht mit einer realen Person verknüpft werden kann, dann hat man einen Dan Level erreicht.

(Das ist 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...).

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...
- 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 und so können den Surf-Profilen die 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 anonymen E-Mail Postfach mit dem Real-Name Postfach und dem Surf-Profil verknüpft werden.

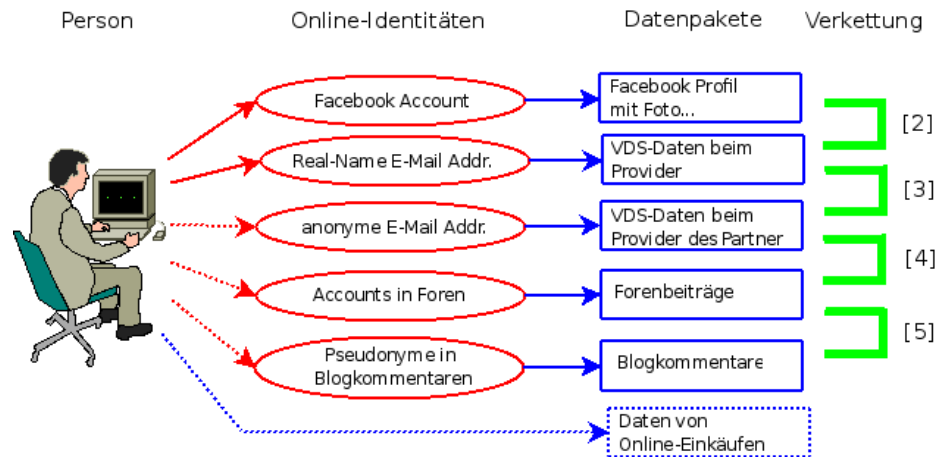


Abbildung 3.1: Datenverknüpfung

- 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.

Verknüpfung der Informationen und Datenpäckchen

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

1. Online Communities 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-Communities zu identifizieren ¹.
 - MIT-Studenten erkennen homosexuelle Neigungen ihrer Kommilitonen anhand der Informationen über Freundschaften in den Facebook-Profilen ².
 - Der Grünen-Vorsitzende Özdemir pflegte eine Freundschaft mit dem Intensivstraftäter Muhlis Ari, 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 de-anonymisiert 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.

¹<https://www.heise.de/tp/r4/artikel/31/31691/1.html>

²<https://www.heise.de/tp/r4/artikel/31/31181/1.html>

³<https://www.heise.de/tp/r4/artikel/32/32138/1.html>

5. Durch Vergleiche von Aussagen und Wortwahl lassen sich Korrelationen zwischen verschiedenen Nicknamen 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 ⁴)
- Die Libris Shops (Zugang zu Bestellungen von 1000 Buchshops ⁵)
- Sparkassen-Shops (350.000 Rechnung online einsehbar ⁶)
- Acht Mio. Adressen von Quelle-Kunden sollen verkauft werden ⁷

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 de-anonymisiert 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 ...*

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 gesucht oder Anhaltspunkte für Essen in einem nicht-koscheren Restaurant. Auch aktiv wird dabei gehandelt und Fake-Einladungen zu einer Party während des Sabbats verschickt.
- Firmen verschaffen sich unrechtmäßig Zugang zu Verbindungs- und Bankdaten, um ihre Mitarbeiter auszuforschen (z. B. Telekom- und Bahn-Skandal).

⁴<https://www.netzpolitik.org/2009/exklusiv-die-buecher-der-anderen>

⁵<https://www.netzpolitik.org/2009/exklusiv-die-libri-shops-der-anderen>

⁶<https://www.netzpolitik.org/2009/zugriff-auf-350-000-rechnungen-im-sparkasse-shop>

⁷<https://www.zeit.de/digital/datenschutz/2009-11/quelle-kundendaten-verkauf>

- 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 Dienstleistungen überschüttet, die man nie in Anspruch genommen hat ⁸.
- 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. ⁹

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 nach Informationen dieser fiktiven Person selbst 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 wenige Treffer, im Moment sind es 3 Treffer. Gleich wieder aufgeben?

Die moderne Studentin ist sozial vernetzt. Naheliegender 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:

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 nicht genommen sondern ins Klo geworfen.
- Sie hat Probleme im Studium und will sich krankschreiben lassen, um an Prüfungen nicht 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 abgefueckt.de.

⁸<http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung>

⁹<https://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung>

- 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....

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 belauscht 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 einzelner Individuen kann sich zu einem Shitstorm zusammenfinden. Der Schwarm kann kurzzeitig viel Lärm produzieren ohne gesellschaftlichen

Diskurs 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 muss 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 genug haben von der Demokratiesimulation 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 techn. 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 anderer 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. 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 Signal App, Matrix/Riot oder Threema bieten die Möglichkeit, die Schlüssel des Gegenüber 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 Surfens** 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:

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

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 o.a. staatliche Vorgaben nicht respektieren möchte, muss Repressionen durch den Macht- bzw. Staatsapparat befürchten... usw.

Anonymität erreicht man beim Surfen im Netz, indem man in einer ausreichend großen Anonymitätsgruppe mit identischen Merkmalen untertaucht, so dass einzelne Individuen nicht mehr anhand von Merkmalen wie IP-Adresse, Browsertyp und -eigenschaften usw. unterscheidbar sind. Populärste Applikation für anonymes Surfen ist der TorBrowser.

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

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

- Wichtigste Punkt 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 ist auch das eigene Verhalten im Netz wesentlich, 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 nicht-anonymisierte Dokumente versendet, die auf einen kleinen Personenkreis zurück geführt werden können, riskiert seine Anonymität.¹
- Wer sich aus dubiosen Quellen irgendwelche Software Bundles wahllos 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 Projektes² für Windows, MacOS und Linux zum Download bereit.

Die *Extended Support Releases*³ (ESR-Versionen) von Firefox werden im Gegensatz zu den 4-wöchigen Updates des Firefox für ca. ein Jahr gepflegt. Es werden keine neuen Features eingebaut, 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, so dass Mozilla die Telemetriedaten eindeutig einem Download zuordnen kann. Wenn man die Telemetriefunktionen deaktiviert, ist das wenig kritisch, aber man kann auch als alternativen Download das FTP Verzeichnis von Mozilla nutzen. Die dort heruntergeladenen Firefox Browser für Windows und MacOS sind nicht individuell markiert.⁴

Linux-Distributionen enthalten den Browser in der Regel. Man kann den Browser mit der Paketverwaltung installieren:

Debian GNU/Linux, RedHat enthalten den Firefox-ESR. Der Browser wird aus den Repositories mit folgenden Kommandos installiert:

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

Fedora, Ubuntu und Derivate bringen den aktuellen Firefox mit, den man mit folgenden Kommandos installiert, wenn er nicht bei der Installation des OS installiert wurde:

```
Ubuntu: > sudo apt install firefox firefox-locale-de
Fedora: > sudo dnf install firefox
```

Für Ubuntu LTS stellt das Mozilla Team einen Firefox ESR in folgendem PPA bereit:⁵

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>

⁴<https://ftp.mozilla.org/pub/firefox/releases/>

⁵<https://launchpad.net/mozillateam/+archive/ubuntu/ppa>

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

apparmor ist ein Sicherheitsframework für Linux. Als Mandatory Access Control System kontrolliert es einzelne Anwendungen und kann mit Profilen die Rechte von Anwendungen fein granular 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.

Einige Distributionen wie Ubuntu und davon abgeleitete Derivate bringen ein Apparmor Profil für Firefox mit. Das Paket *apparmor-profiles* muss installiert und die Regeln für Firefox sind zu enforcen:

```
> sudo apt install apparmor-profiles apparmor-utils
> 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.

Freunde von *BSD finden Firefox und Firefox ESR in pkgsrc und können die jeweils aktuelle Version mit dem üblichen Dreisatz selbst compilieren.

Schnellkonfiguration für einen privacy-freundlichen Firefox

Wer sich nicht mit den Details beschäftigen möchte, kann diese Anleitung zur Schnellkonfiguration nutzen, um Firefox privacy-freundlich zu konfigurieren. Das Kapitel *Spurenarm Surfen* mit denn ausführlichen Erläuterungen könnte man überspringen und im nächsten Kapitel weiterlesen.

Empfehlung für **Firefox 78+**:

- Das Add-on **uBlock Origin** ist ein effizienter und einfach installierbarer Werbe- und Trackingblocker. Nach der Installation kann man die Konfiguration anpassen und weitere Filterlisten aktivieren für URL-Parameter oder lokale URLs und außerdem iFrames blockieren.
- Das Add-on **CanvasBlocker** kann Zugriffe auf Canvas-API, Screen-API und Audio-API faken (geringfügig modifizieren) um ein Fingerprinting des Browsers zu verhindern. Als Einstellungen sind die vorbereiteten *Stealth Settings* empfehlenswert.
- Das Add-on **Skip Redirect** entfernt Umleitungen in der URL. Diese Umleitungen werden häufig genutzt, um die Klicks auf Links zu externen Domains zu tracken. Hinweis: Für WiFi Hotspot Logins muss man das Add-on deaktivieren.
- Außerdem sind weiteren Einstellungen in der Konfiguration privacy-freundlich zu setzen. Um die Werte nicht alle einzeln setzen zu müssen, kann man die *minimale user.js*, die *moderate user.js* oder *strenge user.js* Konfiguration für Firefox oder Firefox ESR von der Webseite herunterladen und im Browserprofil speichern. Beim Start überschreiben die Werte der *user.js* die Präferenzen.⁶
- Das Add-on **NoScript** ist für höhere Sicherheitsanforderungen in Kombination mit der *strenge user.js* empfehlenswert. Das Add-on kann Freigaben für Javascript und anderen Content detailliert verwalten. Außerdem enthält es eine XSS-Protection.
- **Optional:** Außerdem gibt es noch Add-ons, die für die Privatsphäre nicht relevant aber trotzdem sinnvoll sein könnten und die gefahrlos installiert werden können:

⁶https://www.privacy-handbuch.de/handbuch_21u.htm

Das Add-on **Binnen-I be gone** ersetzt ideologisch motivierte Sprachverhunzungen in Texten durch das generische Maskulin. Wer beim Lesen von Konstrukten wie *InfluencerInnen* oder *Verbrecher:innen* oder *Politiker*innen* immer genervt ins Stolpern kommt und sich fragt, wie man das jetzt aussprechen müsste, wird es mögen.

(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 privacy-freundlichen **Suchmaschinen** zu vereinfachen, sind einige Such-Plugins vorbereitet. Wenn man auf die Webseite https://www.privacy-handbuch.de/handbuch_21browser.htm aufruft, kann man mit einem Klick auf die drei Punkte in der URL Zeile klicken und in dem ausklappenden Menü die gewünschten Suchmaschinen hinzufügen. Das funktioniert auch auf den Webseiten der Suchmaschinen.

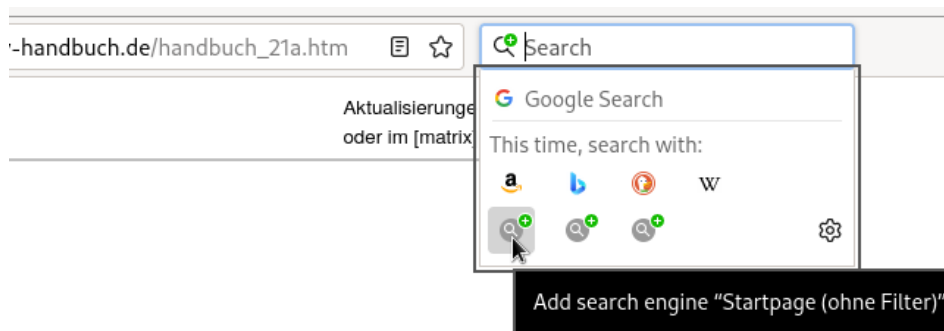


Abbildung 4.1: Suchmaschinen hinzufügen

4.2 Datensparsame Suchmaschinen

Suchmaschinen werden am häufigsten genutzt, um sich im Web zu orientieren. Neben den bekannten Datensammlern wie Google, Bing oder Yahoo! gibt es 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.

Suchmaschinen mit eigenem Index

Es ist nicht einfach, eine Suchmaschine aufzubauen, die die Privatsphäre der Nutzer respektiert, einen umfangreichen Index zur Verfügung stellt und gute Ergebnisse liefert. Zwei Alternativen zur Google Suche:

Qwant (<https://www.qwant.com>)

Qwant definiert sich selbst nicht als Suchmaschine sondern als Entdeckungsmaschine. Es gibt eine JavaScript-freie Lite Version, aber die Suchergebnisse sind mit Freigabe von JavaScript und Cookies deutlich besser. Neben den News und der Suche in Socila Medie gefällt mir die Bildersuche von Qwant.

Bei den Suchergebnissen setzt Qwant die Zensurwünsche der EU (bzw. EU Verordnungen zur Zensur) um. Im Krieg zwischen Russland und Ukraine wurden beispw. russische Nachrichtenmedien gemäß Anordnung aus Büssel aus dem Index entfernt.

DuckDuckGo.com (<https://duckduckgo.com>)

DuckDuckGo ist eine privacyfreundliche 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 genutzt werden oder zum Umrechnen von Einheiten, Fragen nach dem Wetter können beantwortet werden (in englisch: *weather*)...

In den DuckDuckGo Settings kann man die Sucheinstellungen konfigurieren. Die Einstellungen werden in Cookies oder als URL Parameter gespeichert.⁷

DuckDuckGo manipuliert seit 11. März 2022 die Suchergebnisse in der gleichen Weise wie Google und reduziert die Relevanz von Webseiten, die im Westen der russische Desinformation verdächtigt werden, ohne sie komplett aus dem Index zu werfen. (Leider werden westliche Desinformationstrolche nicht in gleicher Weise behandelt.)

Mojeek (<https://www.mojeek.com>)

Mojeek.com ist eine kleine (aber aufstrebenden), privacy-freundliche 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 (und damit auch bei Startpage), die offizielle, westeuropäische Nachrichtenseiten vergleichsweise deutlich bevorzugt. Die russischen Feindsender wurden bei mojeek.com nicht aus dem Index geworfen.

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

Persönliche Einstellungen werden ausschließlich als Cookies gespeichert. Wenn man die Einstellungen anpassen will (z.B. 20 oder 50 Ergebnisse pro Seite) darf die Cookies für die Domain mojeek.com beim Beenden des Browsers nicht löschen.

Metasuchmaschinen

Meta-Suchmaschinen 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 die Identität der Nutzer gegenüber den angefragten Suchmaschinen verbergen, da sie als Proxy agieren.

Startpage (<https://startpage.com>)

bietet privacy-freundlichen 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:

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.

⁷<https://duckduckgo.com/settings>

In den Startpage Settings kann man den *Family-Filter* deaktivieren und weitere Einstellungen vornehmen. Sie werden in Cookies oder als URL Parameter gespeichert.⁸

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 verwendet standardmäßig für die Websuche folgende Suchmaschinen als Quelle: Bing, Scopia, Infotieger und OneNewspage.

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 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 werden wenn man den Metager Proxy verwenden will. Der Proxy entfernt Javascript und viele Bilder:

Corona-Proteste: Mehr als 100.000 Menschen auf der Straße

berliner-zeitung.de/news/corona-proteste-mehr-als...

Berlin - Mehr als 100.000 Menschen haben am Montagabend bundesweit gegen die Corona-Maßnahmen demonstriert .

ÖFFNEN IN NEUEM TAB ÖFFNEN ANONYM ÖFFNEN

SearX und SearXNG (<https://searx.space>)

sind Open Source Metasuchmaschinen, die man selbst betreiben könnte, wenn man sich in das Thema einarbeitet. Es gibt bereits 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 SearX(NG) nicht mit Werbung finanziert wird, werden im Gegensatz zur Startpage und Metager keine Daten an Dritte weitergegeben.

Die Einstellungen für die Suche (welche Suchmaschine 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 Anfrage, bei Änderung der Suchanfrage werden wieder die Default-Einstellungen genutzt. Um die Einstellungen längerfristig zu speichern, muss man die Speicherung der Cookies im Browser dauerhaft zulassen.

Hinsichtlich Zensur sind die SearX(NG) Instanzen von den Suchmaschinen abhängig, die die Ergebnisse liefern. Man kann ein breites Spektrum an Suchmaschinen aktivieren, um mehrere Ansichten einzubeziehen.

Meta-Suchmaschinen schützen die Privatsphäre oft nur ein bisschen. Sie entfernen eindeutig identifizierende Informationen aus dem Datenstrom, leiten aber trotzdem einige Daten an Datensammler weiter. Diese Daten könnten unter Umständen ausreichen, um den Surfer wiederzuerkennen. Außerdem sind Google & Co. generell an der Auswertung von allen Suchanfragen interessiert, um ihre Macht auszubauen, auch wenn sie keinem Nutzer zugeordnet werden können.

Hinsichtlich politischer Zensur sind die Metasuchmaschinen von den Ergebnissen abhängig, die die großen Suchmaschinen liefern und werden somit zumindest indirekt beeinflusst. Dieser Effekt ist bei Startpage stark ausgeprägt (da nur von Google abhängig).

⁸<https://www.startpage.com/do/settings>

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 DeepL⁹ nutzen. Der Translator kennen neben Englisch und Deutsch weitere Sprachen.

Peer-2-Peer Suchmaschine

Yacy¹⁰ ist eine zensurresistente Peer-2-Peer Suchmaschine. Jeder kann sich am Aufbau des Index beteiligen und die Software auf seinem Rechner installieren. Der Crawler ist in Java geschrieben, benötigt also eine Java-Runtime (JRE), die es für WINDOWS bei Oracle¹¹ zum kostenlosen Download gibt. Linuxer können das Paket *default-jre* mit der Softwareverwaltung installieren. Danach holt man sich die Yacy-Software von der Website des Projektes und startet den Installer - fertig. Für Debian, Ubuntu und Linux Mint bietet das Projekt ein Repository¹² mit fertigen Paketen.

Nach dem Start von Yacy kann man im Browser die Basiskonfiguration anpassen und los gehts. Die Suchseite ist im Browser unter <http://localhost:8090> erreichbar.

Die Beantwortung der Suchanfragen dauert mit 5-10sec ungewohnt lange. Außerdem muss JavaScript für <http://localhost> freigegeben werden, damit die Ergebnisseite sauber dargestellt wird. Mit den Topwords unter den Ergebnissen bietet Yacy ein Konzept, um die Suchanfrage zu präzisieren.

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.

⁹<https://www.deepl.com/translator>

¹⁰<http://yacy.net>

¹¹<https://java.com/de>

¹²<https://wiki.yacy.net/index.php/De:DebianInstall>

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 privacyfreundliche Suchmaschine zu nutzen statt Google.

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* in 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 ein sehr individuelle Parameter, der von Betriebssystem und 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 Fingerprint des Browsers gut geeignet. Anhand des Browser-Fingerprint 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. Andere Suchmaschinen bieten eine andere Sicht auf das Netz - auch nicht schlecht, erfordern aber etwas Umgewöhnung.

4.2.1 Suchmaschinen in Firefox hinzufügen

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

1. Auf den Startseiten der Suchmaschinen findet man in der Regel einen Button zur Installation eines Such-Add-ons. Mit der Installation des Add-on kann die neue Suchmaschine auch gleich als Default eingestellt werden.

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 Startpage¹³ oder DuckDuckGo¹⁴ Settings kann man die Suche konfigurieren.
 - Man kann die Filter abschalten, um mal nach schmutzigen Dingen zu suchen.
 - Man kann die Suchanfragen von HTTP GET auch HTTP POST umstellen, damit die Suchbegriffe nicht in der URL auftauchen und in der History werden.
 - Man kann das Laden der 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 einstellen und das Farbschema.
 - ...

¹³<https://www.startpage.com/do/settings>

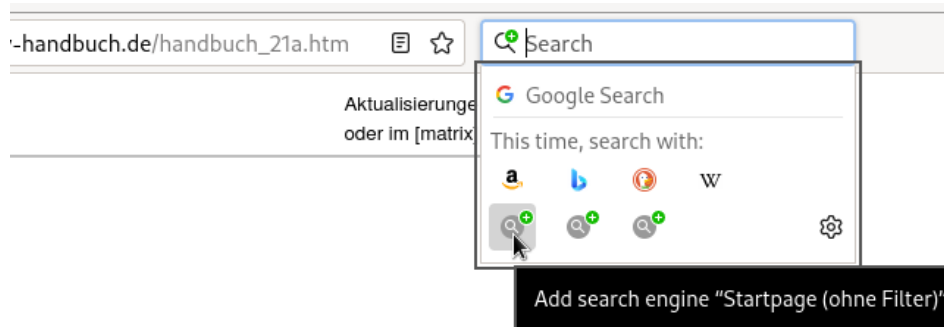
¹⁴<https://duckduckgo.com/settings>

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 Parameter 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. Man kann in den Firefox Einstellungen die Suchleiste in der Symbolleiste aktivieren.



Diese Suchleiste bietet die Möglichkeit, mit einem Klick weitere Suchmaschinen Plug-ins zu installieren, die auf einer Webseite bereitgestellt werden.



- Wenn man auf der Webseite vom Privacy-Handbuch ist, kann man angepasste Such-Plug-ins für Startpage (DE, ohne Filter), DuckDuckGo (DE), Qwant oder Metager auf diesen Weg installieren.
- Die Webseite mycroft.mozdev.org bietet hunderte weitere Plug-ins für verschiedene Suchmaschinen, die auf diesem Weg installiert werden können.
- Einige Webseiten wie netzpolitik.org bieten eigene Such-Plug-ins zum durchsuchen der eigenen Seite an, die auf diesem Weg installiert werden können.

Nach der Installation einiger Such-Plug-ins kann man in den Einstellungen von Firefox die Suchmaschinen anpassen, die standardmäßig installierten Suchmaschinen deaktivieren und **eine privacy-freundliche Default-Suche wählen** (Abb: 4.2).

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

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 irgendwie 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:

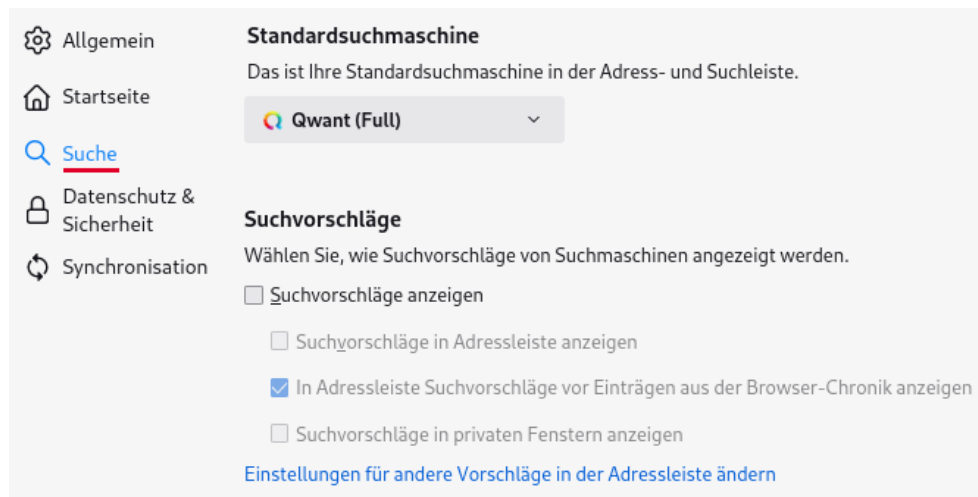


Abbildung 4.2: Default Suchmaschine auswählen

```
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.

4.2.2 Vorschläge bei Eingabe einer URL reduzieren

Um die Anzeige von Vorschlägen bei Eingabe einer URL etwas zu reduzieren, kann man die Suchfunktion bei URL Eingabe 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 eine handverlesenden und gesponsorte Liste von Vorschläge bei Eingabe einer Adresse in der URL Leiste 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, beispielsweise die Vorschläge aus den geöffneten Seiten deaktivieren oder Lesezeichen, da man auf diese Quelle direkt zugreifen kann, wenn man möchte.

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

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

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

4.3 Cookies und EverCookies

Cookies werden für die Identifizierung des Surfers genutzt. Neben der erwünschten Identifizierung um personalisierte Inhalte zu nutzen, beispielsweise einen Web-Mail-Account

oder um Einkäufe abzuwickeln, werden sie für das Tracking von Surfern verwendet.

Der Screenshot Bild 4.3 zeigt die Liste der Cookies, die bei einem einmaligen Aufruf der Seite *www.spiegel.de* gesetzt wurden. Es ist nicht ungewöhnlich, dass populäre Webseiten mehrere Datensammler einbinden. Eine Studie der Universität Berkeley ¹⁵ hat 2011 beim Surfen auf den Alexa TOP100 Webseiten 5.675 Cookies gefunden (ohne Login oder Bestellung). 4.914 Cookies wurden 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 Tracking Dienste mehr als 40% des Surfverhaltens auch dann verfolgen konnten, wenn man Cookies für Drittseiten blockierte und nur First-Party Cookies erlaubt. ¹⁶

Ein Beispiel ist der Trackingdienst WebTrek, der sich auf Webseiten wie *heise.de*, *zeit.de* oder *zalando.de* mit DNS-Aliases als Subdomain der überwachten Webseite First-Party Status erschleicht, um seine Tracking Cookies zu setzen. ¹⁷

- 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. ¹⁸
- Microsofts folgte im Januar 2018 und hat eine Lösung umgesetzt, 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. ¹⁹
- Facebook folgte den Beispiel von Google und Microsoft im Herbst 2018, nachdem Mozilla angekündigt hat, 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. ²⁰

Der Screenshot Abb. 4.4 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. 22 Cookies werden bei *www.spiegel.de* im First Party Context geschrieben. Nur drei Tracking Dienste schreiben ihre Cookies noch als Drittseite.

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.

Tracking Cookies konnten lange Zeit anhand dieser Markierungen wiederhergestellt werden, auch wenn alle Cookies gelöscht wurden. Moderne Browser bieten inzwischen

¹⁵<http://heise.de/-1288914>

¹⁶https://securehomes.esat.kuleuven.be/gacar/persistent/the_web_never_forgets.pdf

¹⁷<https://anonymous-proxy-servers.net/blog/index.php/?archives/377-Tracking-mit-Cookies.html>

¹⁸<https://www.heise.de/-3859526>

¹⁹<https://advertise.bingads.microsoft.com/en-us/blog/post/january-2018/conversation-tracking-update-on-bing-ads>

²⁰<https://marketingland.com/facebook-to-release-first-party-pixel-for-ads-web-analytics-from-browsers-like-safari-249478>

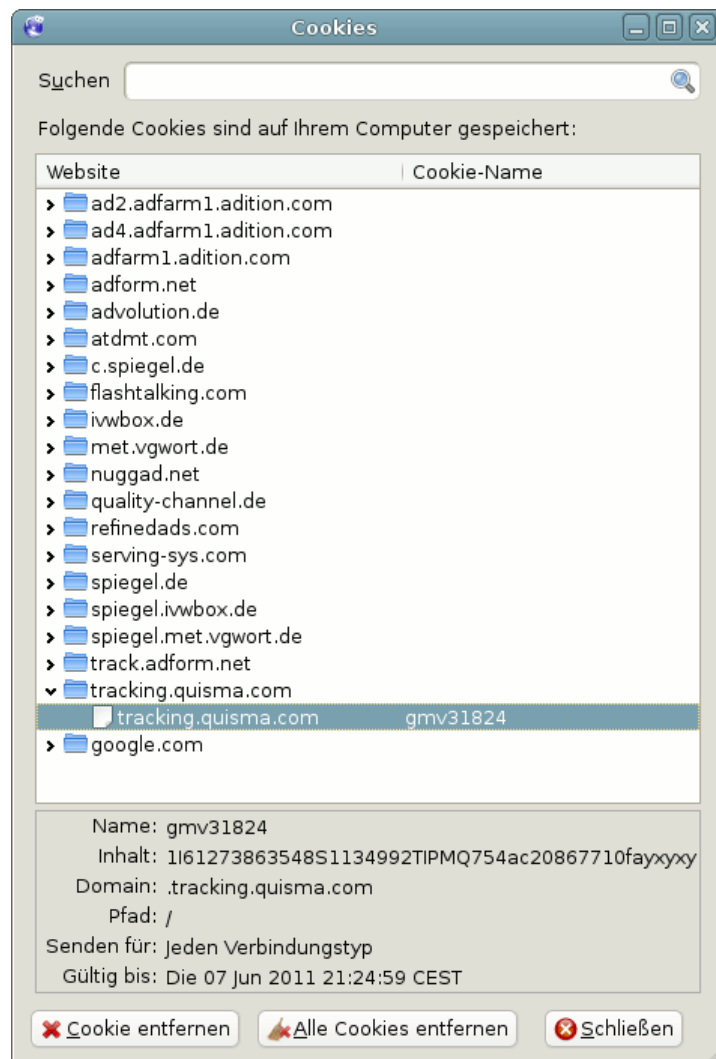


Abbildung 4.3: Liste der Cookies beim Besuch von Spiegel-Online 2011

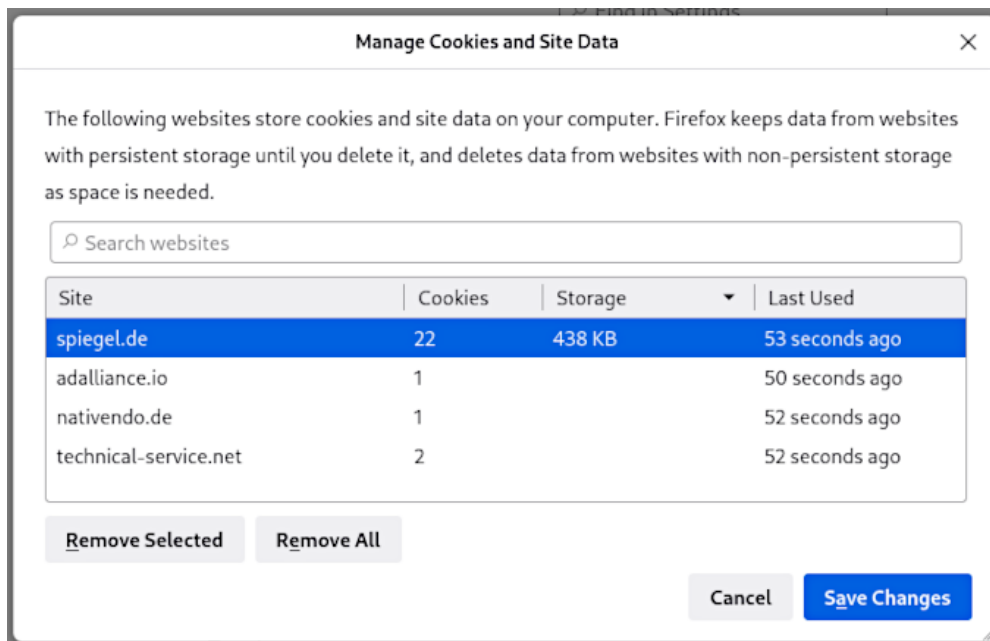


Abbildung 4.4: Liste der Cookies beim Besuch von Spiegel-Online 2022

Schutzmöglichkeiten gegen diese Trackingverfahren.

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

NSA & Co.

Die Tracking-Cookies wurden auch von der NSA und GCHQ im Rahmen der globalen Überwachung genutzt. Die Geheimdienste beobachteten den Datenstrom und identifizierten Surfer anhand langlebiger Tracking-Cookies. Zielpersonen werden 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 Website ergeben sich damit unterschiedliche Tracking-IDs in Cookies, HTML5 Storage, unterschiedliche ETags im Cache und TLS Sessions...

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

1. Die *Netzwerk Partitionierung* isoliert alle Cache Speicher (HTTP, Bilder, Fonts...), SSL Session IDs, HSTS, OCSP, DNS... in getrennten Containern für jede First-Party Domain und ist seit Firefox 85.0 standardmäßig aktiv.

2. *Total Cookie Protection* ist das Konzept zur Isolation von Cookies, Third-Party Cookies, DOMStorage und IndexedDB in getrennten Containern für jede Domain. Dieses Feature kann man unter *about:config* mit folgender Einstellung aktivieren:

```
network.cookie.cookieBehavior = 5
```

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:

```
network.cookie.lifetimePolicy      = 2
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
```

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

```
privacy.clearOnShutdown.offlineApps = true
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, evtl. möchte man dauerhaft auf einigen Webseiten eingeloggt bleiben o.ä. Dann darf man die *SiteSettings* beim Beenden des Browsers nicht löschen (gilt ab Firefox 99+):

```
privacy.clearOnShutdown.siteSettings = false
```

In den Firefox Einstellungen kann man in der Sektion *Datenschutz und Sicherheit* Ausnahmen für Webseiten definieren, deren Cookies nicht beim Beenden gelöscht werden sollen.

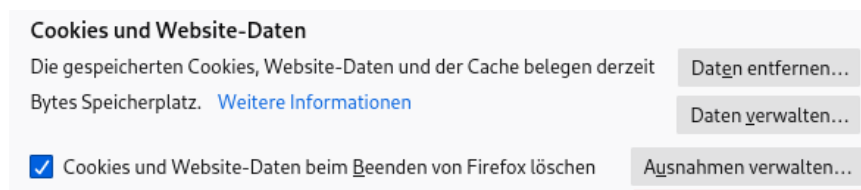


Abbildung 4.5: Webseiten definieren, die dauerhaft Cookies speichern dürfen

3: Schutz gegen Redirect Tracking

Beim Redirect Tracking wird der Surfer bei Klick auf einen Link nicht direkt von der Webseite A zur Webseite geleitet (A -> B) sondern von der Webseite A zur Zwischenstation T geschickt, die den Besucher mit Trackingelementen 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 WiFi Hotspot Logins muss man das Add-on deaktivieren.)

Firefox 79+ kann Redirect Tracking erkennen und die Trackingmarkierungen entfernen kann. Das Feature ist seit Firefox 83+ standardmäßig aktiviert. Firefox löscht 1x in 24 Stunden 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 automatisch, die nicht mehr gebraucht werden oder nach vorgegeben Regeln (und machen um jedes gelöschten Cookies viel Getöse).

Das einfache Löschen von Cookies schützt nur wenig gegen Tracking. Trackingdienste verwenden EverCookies, um gelöschte Tracking Cookies wiederherzustellen. Diese Add-ons erfüllen ihre Aufgabe, bieten aber hinsichtlich Trackingschutz kaum Verbesserungen.

4.4 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. anderen Surf-Container ist nicht möglich. Somit werden in den verschiedenen Contexten unterschiedliche Tracking Markierungen gesetzt. Man kann sich auch in verschiedenen Surf-Containern (user-Context) gleichzeitig mit unterschiedlichen Identitäten bei einer Website anmelden.

Aber: Surf-Container schützen nicht gegen Tracking anhand des Browser Fingerprint!

- Da das gleiche Browser Profil mit identischer Konfiguration und 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 wurde mit Firefox 58+ von Mozilla implementiert.
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... 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. Dieses Feature kann man mit folgender Einstellung aktivieren:

```
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 statt dessen *Total Cookie Protection* zu nutzen.

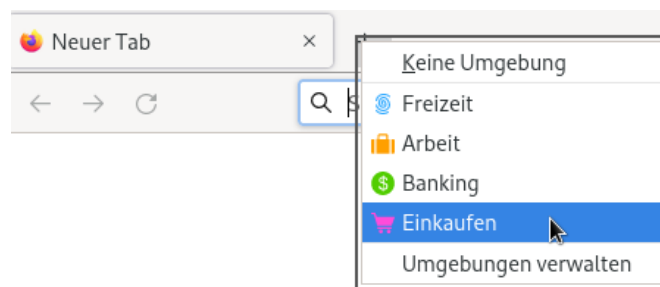
3. **userContext** steht seit Firefox 50+ zur Verfügung. Es werden mehrere Surf-Container bereitgestellt, die man selbst aktiv auswählen muss. Um das Feature zu aktivieren, muss man zuerst unter der Adresse *about:config* folgende Werte setzen:

```
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.

4.5 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 Bayerischen 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

²¹<https://www.sueddeutsche.de/digital/blutspende-brk-facebook-patientendaten-1.4576563>

- 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 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 wurde auch Antworten auf sensible, gesundheitliche Fragen zur Ferndiagnose an die Werbenetzwerke übertragen.²²

Immer häufiger nutzen Kriminelle die große Werbenetzwerke, um mit ihre Schadsoftware möglichst vielen Rechnern anzugreifen. Nach Beobachtung von Trend Micro²³ kaufen Kriminelle zur Zielgruppe passende Werbeplätze, 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 erwarteten eine Fortsetzung des Trends für 2016. Beispiele für derartige Angriffe:

- Im Januar 2013 lieferten die Server des Werbenetzwerkes OpenX bösartige Scripte aus, die den Rechner über Sicherheitslücken im Java Plug-in und im Internet Explorer kompromittierten.²⁴
- Zum Jahreswechsel 2014 wurden innerhalb von 4 Tagen 27.000 Surfer durch Werbung von Yahoo mit Malware infiziert.²⁵
- Eine erfolgreiche, mehrwöchige Malvertising Kampagne konnte im Aug. 2015 mit Hilfe von Doubleclick einige Millionen Surfer infizieren.²⁶
- Im Nov. 2015 wurden die Server des Werbenetzwerkes Pagefair gehackt, um bösartigen JavaScript Code in der Werbung auszuliefern.²⁷

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 websiteübergreifend zu verfolgen.

Die **Like Buttons** werden von Facebook und anderen Soziale 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 deutschen Datenschutzrecht vereinbar. Deutsche Webseitenbetreiber sind aufgefordert, die Facebook Buttons von ihren Seiten zu entfernen²⁸.

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 vorhersagen²⁹. Man verrät mit einem Klick auf einen Like Button möglicherweise Informationen, die man nicht im Netz veröffentlichen möchte.

²²<https://heise.de/-4513282>

²³<http://heise.de/-2429990>

²⁴<http://heise.de/-1787511>

²⁵<http://www.zdnet.de/88180242/werbung-auf-yahoo-com-verteilte-malware-an-nutzer-in-europa>

²⁶<https://blog.malwarebytes.org/malvertising-2/2015/09/large-malvertising-campaign-goes-almost-undetected/>

²⁷<http://www.golem.de/news/anti-adblocker-dienst-500-websites-ueber-pagefair-gehackt-1511-117262.html>

²⁸<https://www.datenschutzzentrum.de/facebook>

²⁹<http://heise.de/-1820638>

4.5.1 Tracking-Filter für Firefox

Es gibt mehrere Add-ons für Firefox, die Werbung und Trackingelemente blockieren. Das Center for Internet and Society der Stanford Law School hat in einer Analyse vom September 2011 einige Lösungen verglichen³⁰. Die Ergebnisse in Bild 4.6 zeigen: keine Lösung ist perfekt.

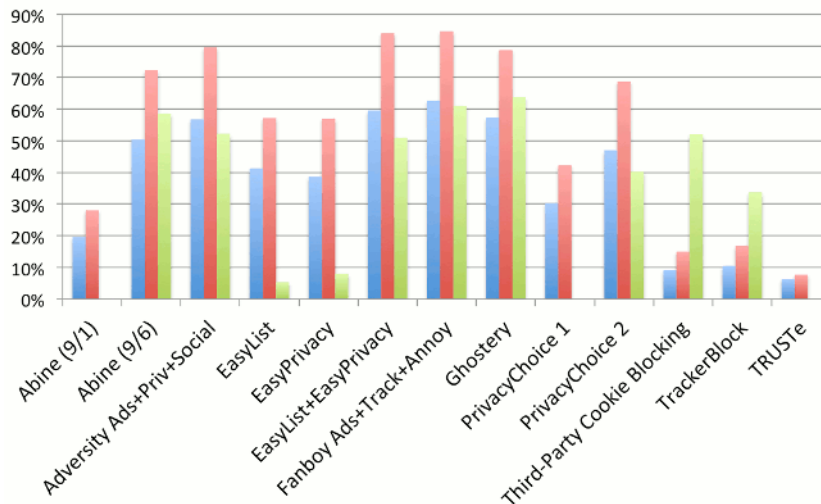


Abbildung 4.6: Effektivität verschiedener Tracking-Filter

Aufgrund der Flexibilität bei der Einbindung verschiedener Filterlisten und der langfristigen Stabilität in der Entwicklung sind textitublock Origin und textitublock Plus empfehlenswert. Mit den Easylist Filterlisten erreichen die Add-ons die besten Ergebnisse. Die Listen werden ständig weiterentwickelt. Zusätzlich zur den Blocklisten gegen Werbung und Tracking gibt es auch Listen, die die Social Media Buttons blockieren. *FanBoy* arbeitet seit 2010 mit EasyList zusammen, daher die gleichfalls guten Ergebnisse.

Ghostery schneidet im Test auch gut ab und wird oft empfohlen. Insbesondere in der Diskussion um Acceptable Ads in AdBlock Plus wird *Ghostery* immer wieder als angeblich saubere Alternative genannt. Dabei wird übersehen, dass *Ghostery* bei den Trackingdiensten Drawbridge³¹ und Tapad³² als Partner gelistet ist. Die Spezialität dieser Trackingdienste ist die Identifikation der unterschiedlichen Geräte (Smartphones, Computer auf der Arbeit und zuhause, Laptops, Tablets), die von einem User benutzt werden. Die Kooperation mit den Trackingdiensten ist auf der *Ghostery* Webseite³³ nicht klar beschrieben und nicht offengelegt. Möglicherweise handelt es sich dabei um die via *Ghostrank* von dem Browser Add-on gesammelten Daten? Da diese Zusammenarbeit mit der Werbeindustrie und die resultierenden Folgen wie *Ghostery Verified Domains* undurchsichtig sind, wird *Ghostery* hier NICHT empfohlen.

4.5.2 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

³⁰<https://cyberlaw.stanford.edu/node/6730>

³¹<http://drawbrid.ge>

³²<http://www.tapad.com>

³³<https://www.ghostery.com>

Trackingdienste und damit als Nebeneffekt Werbebanner, die für Tracking genutzt werden. Folgende Schutzlevel stehen dabei zur Auswahl:

Standard: In Firefox 69.0 ist der Schutz gegen Trackingscripte 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: Außerdem gibt es die benutzerdefinierte Konfiguration, in der man selbst entscheiden kann, welche Schutzmechanismen aktiviert werden sollen. An dieser Stelle könnte man auch die allgm. Richtlinien zur Behandlung von Cookies konfigurieren.

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 und 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 WebTrek werden nicht blockiert. Das ist evtl. nicht verwunderlich, da sich WebTrek 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 Datenschutz-policy von EASYmedia findet man folgenden Satz zum Austausch von Daten mit Dritten:

- 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. . .)

- 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 Web-Trekk, Dynamic Yield, TealiumIQ, Adserve.io usw. könnte man eindeutig als Tracking einsortieren.

Das sind nur Beispiele und ist keine wiss. Analyse. Es zeigt aber, dass der Trackingschutz von Firefox oft nur oberflächlich arbeitet und 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 abschalten und statt dessen einen anderen AdBlocker 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
```

4.5.3 uBlock Origin für Firefox

uBlock Origin³⁴ ist ein effizienter und einfach installierbarer Werbeblocker für Firefox. Zur Installation muss man nur auf den Downloadbutton auf der Webseite klicken.

Nach der Installation findet man oben rechts in der Toolbar des Browsers das uBlock Symbol. Mit einem Klick auf des 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, steht auf der Webseite eine Konfiguration für uBlock Origin als Vorschlag vom PrHdb Team zum Download bereit, den man auf dem Reiter *Einstellungen* importieren kann.³⁵

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.

Belästigungen (Cookie Banner u.ä.)

uBlock Origin schützt nicht nur gegen Tracking und Werbung sondern mit den passenden Filterlisten auch gegen lästige Cookie Banner u.ä. auf vielen Webseiten. Standardmäßig sind die Adguard- und uBlock-Annoyances Filterlisten für diesen Zweck enthalten und filtern recht gut.

Die Web Annoyances Ultra List³⁶ arbeitet noch ein bisschen gründlicher (aber 100% Perfektion ist nicht erreichbar). Mit einem Klick auf diesen Web Annoyances Ultra List Install Link kann man die Filterliste einfach zu uBlock Origin hinzufügen oder man importiert sie von folgender Adresse:

³⁴<https://addons.mozilla.org/de/firefox/addon/ublock-origin>

³⁵https://www.privacy-handbuch.de/handbuch_21d2.htm

³⁶<https://github.com/yourduskquibbles/webannoyances>

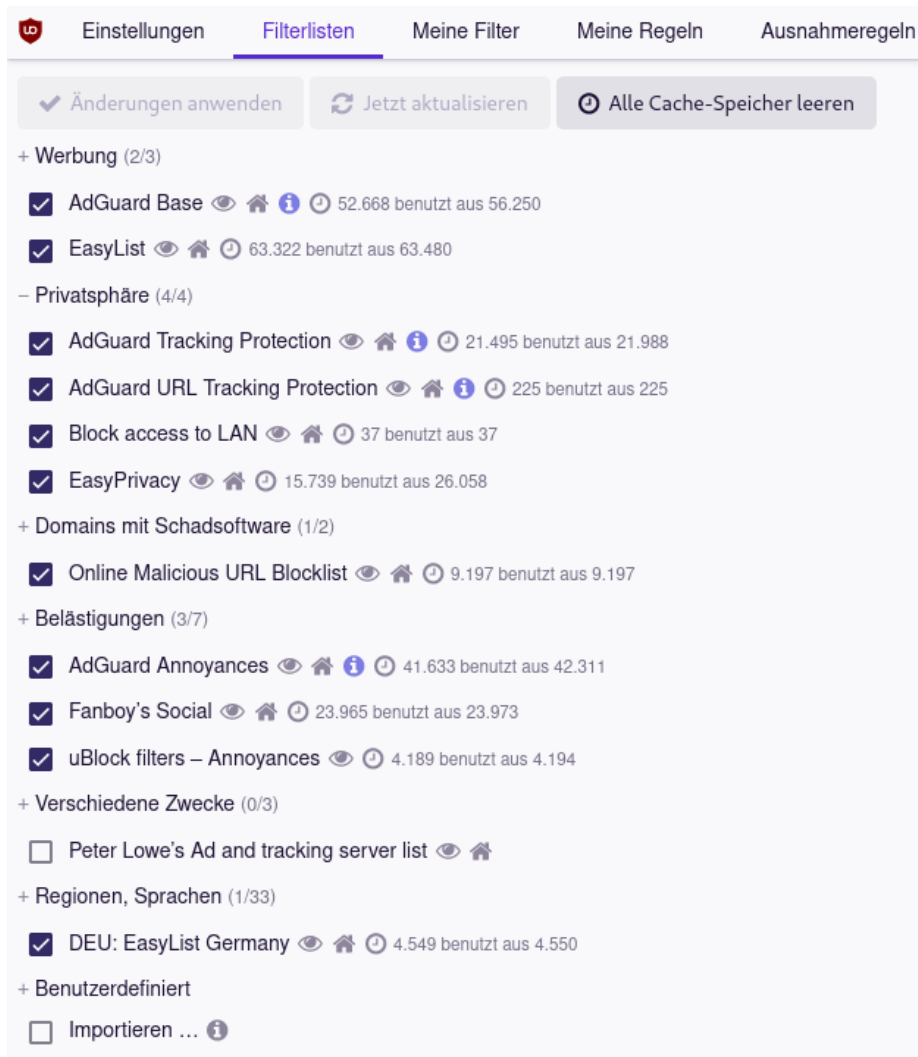


Abbildung 4.7: uBlock Origin: zus. Filterlisten aktivieren

<https://raw.githubusercontent.com/yourduskquibbles/webannoyances/master/ultralist.txt>

Da die Liste restriktiv ist, kann es vereinzelt zu falschen Darstellungen kommen.

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 werde damit auch die via Fonts dargestellten Navigationssymbole blockiert, so dass viele Webseiten unbenutzbar werden.

Statt dessen wird der Google CSS Font Server *fonts.googleapis.com* mit einem eigenen uBlock Filter blockiert:

```
||fonts.googleapis.com$important,third-party
```

Um Schutz gegen Tracking via Schriftarten zu gewährleisten, ist folgende Einstellungen unter *about:config* besser geeignet:

```
browser.display.use_document_fonts = 0
layout.css.font-loading-api.enabled = false
gfx.downloadable_fonts.enabled     = false
```

uBlock Origin zusammen mit NoScript verwenden

Wenn man uBlock Origin zusammen mit NoScript benutzt und aus Privacygründen das Senden von CSP-Reports blockiert, dann muss man auf dem Reiter *Meine Regeln* eine Regel hinzufügen, damit NoScript arbeitsfähig bleibt:

```
no-csp-reports: * true
no-csp-reports: noscript-csp.invalid false
```

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 werden.

4.6 JavaScript

JavaScript ist eine der Kerntechniken des modernen Internet. Der große Funktionsumfang wird aber auch für das Tracking missbraucht und einige Sicherheitsrisiken.

4.6.1 Browserfingerprinting 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.

Bildschirm: Informationen über die Größe des Monitors und des Browserfensters werden am häufigsten für das Hardwarefingerprinting 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*³⁷ beschrieben und 2016 auf 14.371 Webseiten als Trackingverfahren nachgewiesen. Der Canvastest auf Browserleaks.com³⁸ 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 ein Text mit unterschiedlichen Schriftarten benötigen würde, wenn er geschrieben werden würde. Browserleaks.com demonstriert das Verfahren.³⁹

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.

³⁷<https://www.privacy-handbuch.de/download/canvas.pdf>

³⁸<https://www.browserleaks.com/canvas>

³⁹<https://www.browserleaks.com/rects>

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 Grafikhart- 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 Audio-buffer 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.⁴⁰

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 Browserfingerprint generieren würde.

Timing-APIs können von Webanwendungen zur Analyse des Ladens von Ressourcen oder des Nutzerverhaltens missbraucht werden (*Timing Attacks on Web Privacy*).⁴¹

Die Leistungscharakteristik moderner Grafikkarten sind sehr individuell, so dass sie sich für das Fingerprinting der Hardware eignet. Man kann z. B. die komplexe GPU Operationen ausführen und die Zeit messen, wie beim *DrawnApart* Angriff.⁴²

Dieses Fingerprinting erfordert hochgenaue 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.

Ein Deaktivieren der Gamepad-API wäre durch Trackingdienste ebenfalls erkennbar und würde ein besonderes Merkmal für den Browserfingerprint erzeugen, daher nicht empfehlenswert. Falls ein Gamepad angeschlossen sein sollte, verhindert das Add-on *JShelter* den Zugriff.

Media Device Enumeration: liefert Daten über Kamera und Mikrofon, die man für das Hardware Fingerprinting zu verwenden kann. Der Surfer muss dabei nicht um Zustimmung für den Zugriff auf Kamera oder Mikrofon gebeten werden.

Das Add-on *JShelter* verhindert einen Zugriff auf die Multimedia Geräte ohne das die API abgeschaltet werden muss. Das ist unauffälliger als das häufig empfohlen Deaktivieren der API bei anderen Projekte.

HTML Beacons: kann ein Browser beim Verlassen/Schließen einer Webseite Daten zur Analyse an den Webserver senden, die via Javascript gesammelte wurden. Statt die Beacon API zu deaktivieren, ist es unauffälliger, das Senden nur zu simulieren.

Wenn man HTML5 Beacons nicht verschickt, kann es vorkommen, dass eine Webseite nach einem Klick nicht aktualisiert wird. eBay.com ist ein Beispiel dafür. Man muss oft den Reload Button klicken, um eine wirklich aktuelle Seite zu sehen.

Schutz gegen Javascript Fingerprinting

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. Damit wird eine Wiedererkennung des Surfers über

⁴⁰<https://audiofingerprint.openwpm.com>

⁴¹<http://sip.cs.princeton.edu/pub/webtiming.pdf>

⁴²<https://arxiv.org/pdf/2201.09956.pdf>

mehrere Webseiten anhand des Browser Fingerprint unmöglich.

Es gibt mehrere Add-ons, die Javascript APIs faken können. An dieser Stelle wird eine Kombination von CanvasBlocker und JShelter empfohlen. Der Funktionsumfang beider Add-ons überschneidet sich in den Standardeinstellungen, so dass man die Konfiguration anpassen und darauf achten muss, welche Funktion welches Add-on übernimmt.

Die folgende Tabelle ist eine Empfehlung für die Kombination der beiden Add-ons CanvasBlocker und JShelter, die man übernehmen oder variieren kann:

| Funktion | CanvasBlocker | JShelter |
|------------------------|---------------------------------|--------------------------------------|
| Bildschirm API | minimale Größe vortäuschen | |
| Canvas API | aktiviert (ohne WebGL) | Locally generated Images unprotected |
| DOMrect API | aktiviert | |
| TextMetrix API | aktiviert | |
| SVG API | aktiviert | |
| WebGL | deaktiviert | aktiviert (Little lies) |
| Timer API | | 1/10 sec mit zus. Rauschen |
| Audio API | | Amplitude variieren (Little lies) |
| Multimedia Devices | | keine Geräte anzeigen |
| Schutz der Webworker | | deaktiviert (zuviel Probleme) |
| Gamepad-API | | keine Geräte anzeigen |
| VR-Displays | | keine Geräte anzeigen |
| Sensors-API | | Schutz aktiviert |
| History API | max. 2 Einträge | |
| Geolocation API | | Long Distance Obfuscation |
| Hardware Informationen | | zufällige Werte |
| Beacon API | | nichts senden aber ok liefern |
| window.name | löschen (aber nicht in iFrames) | |

Firefox Add-on JShelter

Das Add-on **JShelter**⁴³ kann Zugriffe auf Javascript-APIs faken (geringfügig modifizieren), um ein Fingerprinting des Browser für Trackingzwecke zu verhindern.

Nach der Installation findet man in der Symbolleiste ein neues Icon. Mit einem Klick auf das Icon kann man den Sicherheitslevel für die aktuelle Webseite auswählen oder die Einstellungen von JShelter anpassen und einen neuen Level anlegen.

Das Add-on bietet drei vorbereitete Level. Wenn man JShelter in Kombination mit dem Add-on CanvasBlocker einsetzt, sollte man einen eigenen Level definieren, der auf die Kombination mit CanvasBlocker abgestimmt ist, so dass sich jeweils ein Add-on um eine Javascript API kümmert. Es muss beispielsweise definiert werden, welches der beiden Add-on sich um Canvas Elemente oder WebGL kümmert, was beiden beiden Add-ons standardmäßig aktiviert ist.

Einen Vorschlag für die Einstellungen von JShelter in Kombination mit CanvasBlocker zeigt die Tabelle oben. Um diesen Vorschlag umzusetzen, muss man einen neuen Level definieren. Nachdem man den neuen Level erstellt hat, muss man ihn noch zum Default Level machen (orange markiert). Dafür klickt man in der Übersicht den gewünschten Level an.

⁴³<https://addons.mozilla.org/de/firefox/addon/javascript-restrictor/>

Die komplette Konfiguration kann man von der Webseite des Privacy-Handbuch (online: https://www.privacy-handbuch.de/handbuch_21t2.htm) kopieren und im JShelter importieren.

JavaScript Restrictor

Configured levels and default level:

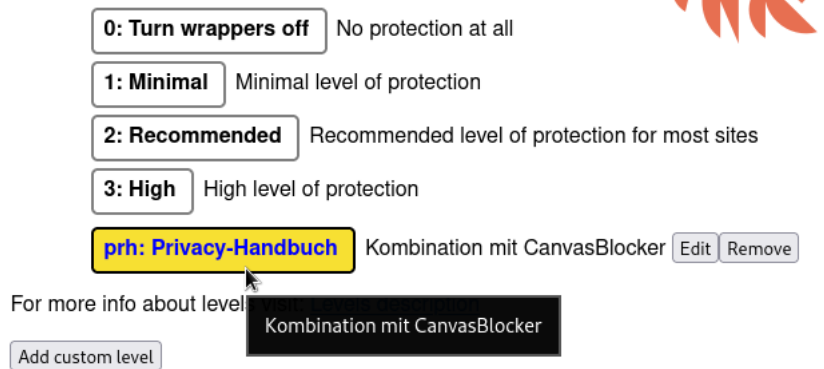


Abbildung 4.8: JShelter: Default Level setzen

Firefox Add-on CanvasBlocker

Das Add-on **CanvasBlocker**⁴⁴ kann Zugriffe auf Canvas-API faken (geringfügig modifizieren) oder faken. Daneben werden noch weitere Javascript-APIs modifiziert wie die Audio-API oder die Screen-API zum Auslesen der Fenster- und Bildschirmgröße, die als Informationen für Browserfingerprinting genutzt werden.

Der Name des Add-ons CanvasBlocker kommt daher, dass die Entwicklung mit dem Faken bzw. Blockieren der Canvas-API begann, um Tracking mit der Canvas-API zu stören. Inzwischen hat sich das Add-on zu einem umfangreicheren Tool entwickelt.

CanvasBlocker bietet viele Einstellungsmöglichkeiten. Um die Konfiguration zu vereinfachen, bietet es drei Presets von Einstellungen, die bei der Installation angeboten werden:

1. *Convenient Settings* (nur leichte Modifikationen der APIs)
2. *Stealth Settings* (meiner Meinung nach die besten Einstellungen, da sie einen umfangreichen Schutz bieten aber schwer als Fakes erkennbar sind)

Wenn man den *Expert Mode* aktiviert, kann man zusätzlich die persistente Speicherung von Daten abschalten oder nach X Tagen löschen lassen, damit man langfristig nicht anhand der immer gleichen Fakes auf einer Domain identifiziert wird.

3. *Maximum Protection* (maximaler Schutz aber mit kleinen Störungen auf einigen Websites, außerdem sind die Fakes teilweise durch Trackingscripte erkennbar)

Bei der Installation muss man einen der genannten Parametersätze auswählen. Um nachträglich die Presets zu ändern, klickt man in den Einstellungen von CanvasBlocker auf dem Reiter *General* in der Sektion *Settings* auf den Button *Open* für die Presets (Abb: 4.9). Es öffnet sich ein neuer Tab, wo man einen der vorbereiteten Parametersätze auswählt.

Die Canvas-API, WebGL oder SVG Bilder werden nicht nur für das Tracking verwendet. Viele Javascript-lastige Webseiten verwenden es auch, um die optimale die

⁴⁴<https://addons.mozilla.org/de/firefox/addon/canvasblocker/>

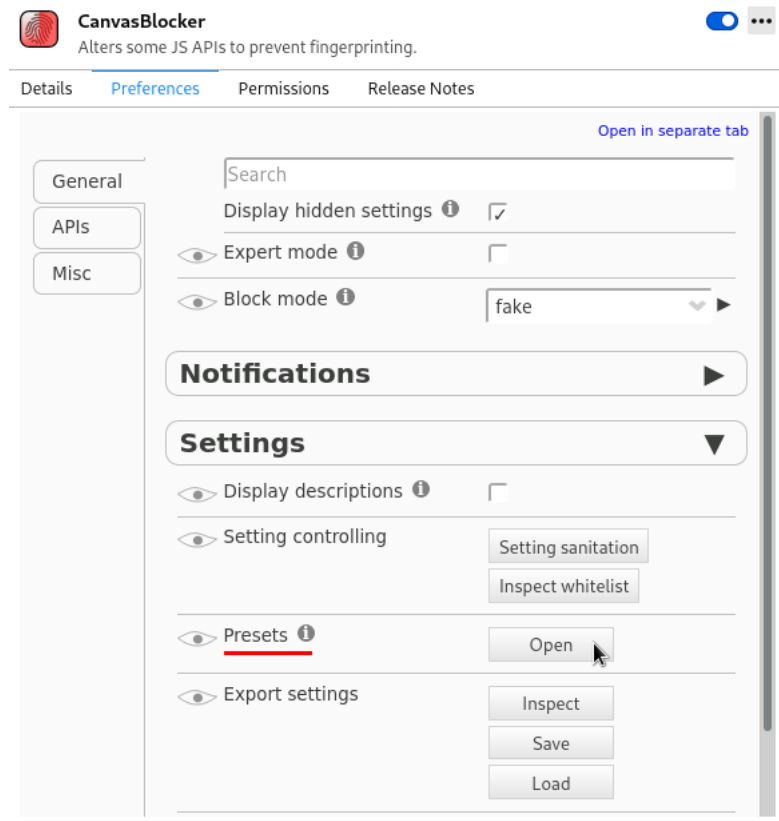
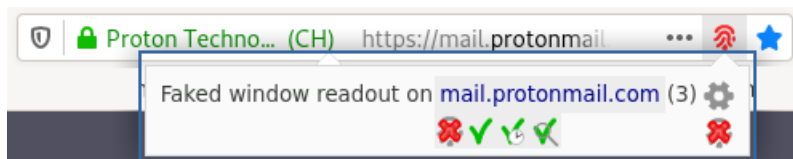


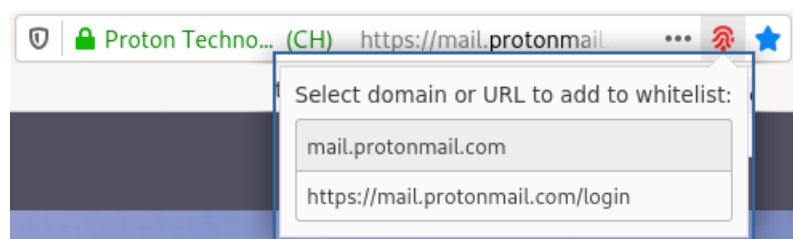
Abbildung 4.9: CanvasBlocker: Presets für die Konfigurationsparameter auswählen

Darstellung der Webseiten zu berechnen. Vertrauenswürdige Webseiten kann man deshalb in eine Whitelist aufnehmen.

Wenn der Zugriff auf eine geschützte Javascript API festgestellt wird, erscheint in der URL-Leiste ein kleiner Fingerabdruck als Symbol. Wenn man auf den Fingerabdruck klickt, erscheint ein Fenster mit den Informationen, auf welche APIs die Webseite zugreift.



Mit einem Klick auf das grüne Häkchen kann man einen dauerhaften Eintrag für die Whitelist erstellen oder mit einem Klick auf das grüne Häkchen mit der Uhr einen temporären Eintrag, der bis zum Schließen des Browsers gültig ist. Im zweiten Schritt legt man fest, ob der Eintrag für die gesamte Domain gültig sein soll oder nur für die aktuelle Seite.



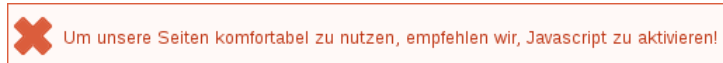
4.6.2 Sicherheitsbedenken bei Javascript

Bösartiger JavaScript Code kann aktiv Sicherheitslücken im Browser ausnutzen und den Rechner kompromittieren. Im Januar 2013 lieferten die Server des Werbenetzwerkes OpenX bösartige Scripts aus, die den Rechner über Sicherheitslücken im Internet Explorer kompromittierten. Auch die bisher bekannten Exploits von NSA/FBI gegen den TorBrowser nutzten bösartiges JavaScript.

Bösartiger JavaScript Code kann sich auch gegen Dritte richten, ohne dass der Nutzer es bemerkt. Chinas Great Cannon⁴⁵ injiziert JavaScript Code beim Aufruf chinesischer Webseiten, um die PCs der Nutzer als Botnet für DDoS-Attacken zu nutzen.

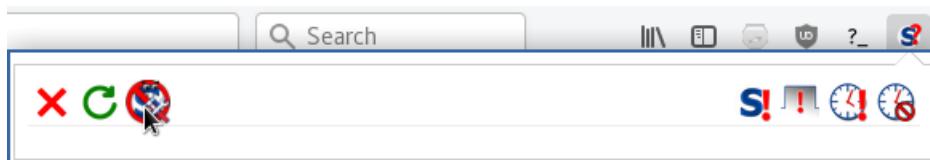
Prinzip Whitelisting mit NoScript

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.



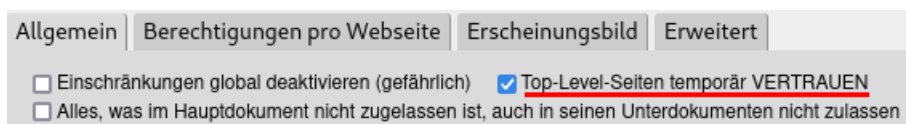
Mit dem Add-on NoScript kann man nicht nur Einstellungen für Javascript verwalten sondern auch für Frames, Fonts, WebGL u.a. Bei der Verwendung von NoScript kann es zu frustrierenden Einschränkungen des Surferlebnisses kommen. Daher wird dieses Add-on vor allem dann empfohlen, wenn man besondere Anforderungen 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 in dem Menü.



Für eine Erstkonfiguration steht ein Vorschlag vom PrHdb Team zum Download zur Verfügung, die man in den Einstellungen von NoScript importieren kann.

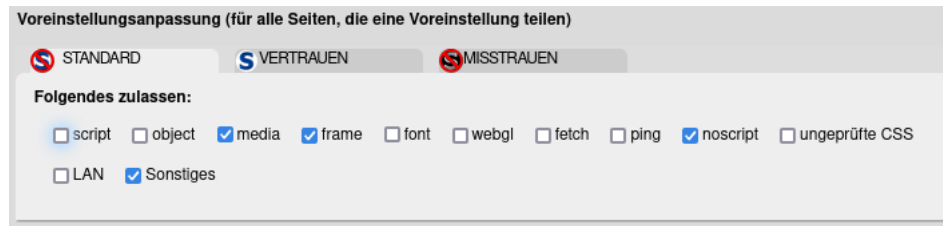
Da das moderne Web ohne Javascript kaum benutzbar ist, kann man in den globalen Einstellungen die aktuelle Top-Level Seite immer als temporär als vertrauenswürdig definieren. (Diese temporären Freigaben werden allerdings nicht mit dem Verlassen der Webseite gelöscht sondern bleiben bis zum Löschen aller temporären Freigaben oder Neustart des Browser 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 JSshelter mit Network Boundary Shield verwendet.

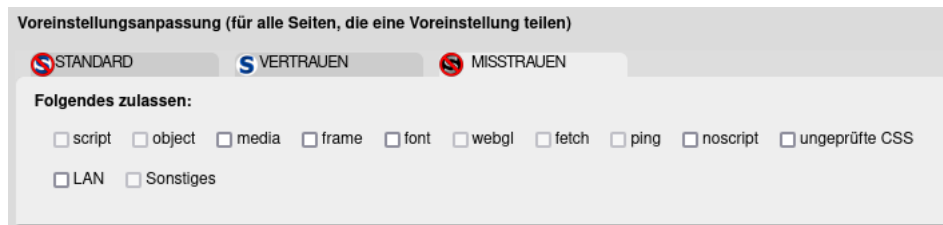
⁴⁵<https://citizenlab.org/2015/04/chinas-great-cannon/>



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 garnichts.



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.

Skripte von Drittteilen

Es kann vorkommen, dass man für zusätzliche Domains Freigaben konfigurieren muss, damit eine Webseite korrekt funktioniert. Insbesondere bei Videoportalen tritt es häufig auf, dass Drittteile zusätzliche Freigaben verlangen. Wenn man auf das NoScript Symbol klickt, sieht man, welche Freigaben nötig sein könnten.

Bei der Entscheidung, welche Domian wirklich nötig sind und welche Domain nur Trackingscripte laden, muss man raten. Skripte von *googletagmanager*, *ioam* oder *trafficjunky* 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 diese Freigaben nur auf dieser Webseiten gelten sollen. Abb 4.10 zeigt ein Beispiel für die Freigaben, die für das Videoportal Netflix.com nötig sind und die nur für diese Webseite gelten sollen.

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 freigegeben.

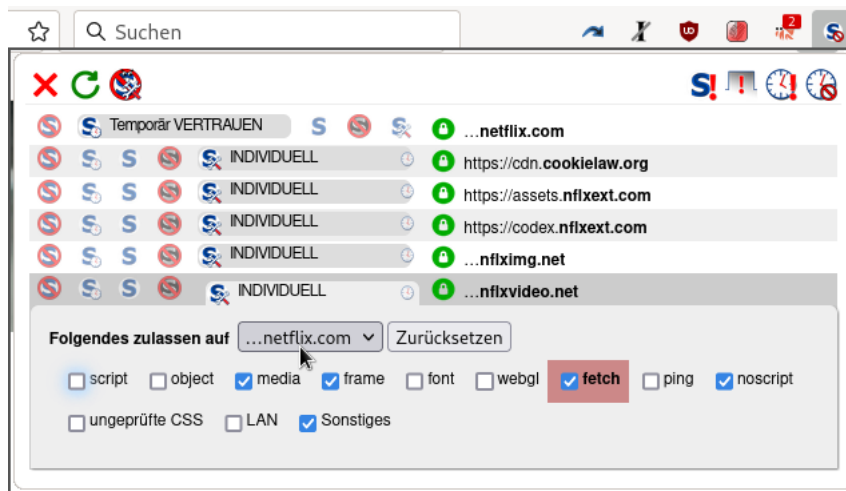


Abbildung 4.10: Individuelle Freigaben in NoScript für Netflix.com konfigurieren

- 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 Dritseiten 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*, *yting.com* und *googlevideo.com* freigeben. Da viele Webseiten Youtube Videos einbinden, kann man diese Freigaben dauerhaft speichern.
- Um Vimeo-Videos von 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 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, beispw. Bug #1607443 in Firefox 72.⁴⁶

iSEC Partners empfiehlt deshalb in einem Sicherheitsaudit für den TorBrowser, die JIT-Compiler für hohe Sicherheitsanforderungen (strenge Einstellungen) zu deaktivieren:

```
javascript.options.ion           = false
javascript.options.baselinejit  = false
```

Diese Einstellungen können die Performance einiger Webseiten deutlich verringern.

⁴⁶<https://www.heise.de/security/meldung/Jetzt-patchen-Angreifer-attackieren-Firefox-4630850.html>

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 Invite Media aufgekauft hatte. Auch dieses Tracking nutzt einen unsichtbaren iFrame, um Tracking Wanzen 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 privacy-freundlichere Youtube Variante. Man kann das Add-on *Privacy Enhanced Mode for Embedded Youtube*⁴⁷ installieren. Es schreibt die Adressen für embedded Youtube Videos auf die No-Cookie Adresse um.

4.7.1 iFrames allgemein blockieren

Mit dem Add-on uBlock Origin kann man alle iFrames von Drittseiten blockieren, indem man auf dem Reiter *Meine Regeln* eine Filterregeln einfügt (Abb: 4.11).

```
* * 3p-frame block
```

Die Regeln könne auf der rechten Seite zum temporären Ausprobieren editiert werden und werden dann mit dem Button *Dauerhaft speichern* zur linken Seite übernommen.

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 Zustimmungseite für Cookies

⁴⁷<https://addons.mozilla.org/de/firefox/addon/youtube-nocookie/>

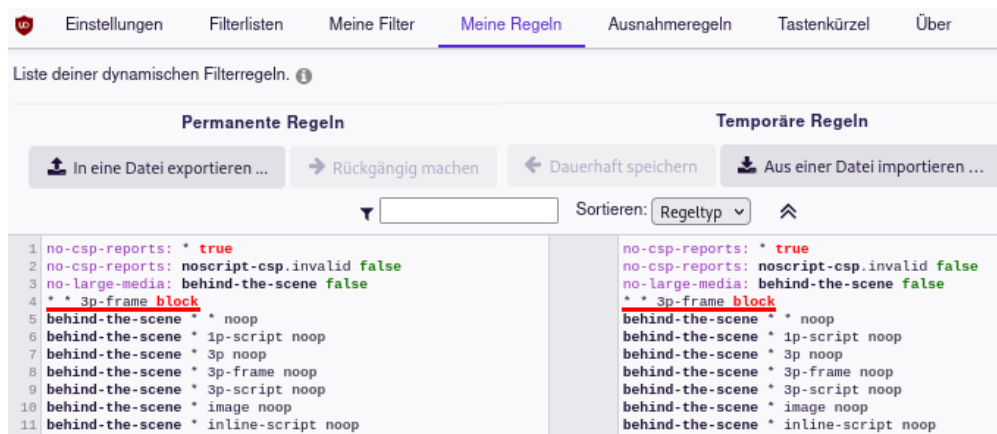


Abbildung 4.11: Blockieren der Frames von Drittseiten mit uBlock Origin

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 komplett blockiert.

```
||privacy-mgmt.com$important
```

4.7.2 Integrierte Videos mit Click-2-Play laden

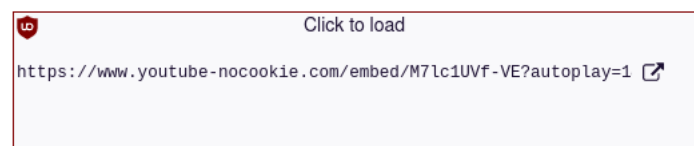
Mit der oben genannten Regel verschwinden auch die eingebetteten Videos von den Webseiten. Um die Videos mit Click-2-Play zu laden, kann man folgende Regeln unter *Meine Filter* einfügen:

```
||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
```

Die Filterliste kann auch 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:



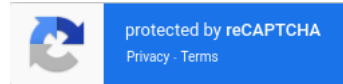
4.7.3 Googles reCAPTCHA und hCaptcha von Cloudflare

Einige Webseiten verwenden reCAPTCHA oder hCaptcha als Schutz gegen Robots. Captcha werden als iFrame geladen und können mit Click2Load Regeln sichtbar werden:

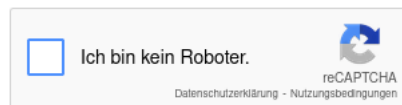
```
||www.google.com/recaptcha/api*/anchor?$3p,frame,important,redirect=click2load.html
||www.recaptcha.net/recaptcha/api*/anchor?$3p,frame,important,redirect=click2load.html
||newassets.hcaptcha.com/captcha/$3p,frame,important,redirect=click2load.html
```

Mit einem Klick muss man es aktivieren und sieht dann, welche Variante genutzt wird.

1. Das kleine reCAPTCHA sieht so aus und mit dem Klick ist schon alles erledigt:



2. Wenn man bei dem Captcha ein Häkchen setzen muss, um zu beweisen, dass man kein Robot ist, muss man iFrames in uBlock für diese Webseite freigeben, damit es funktioniert:



Das kann man mit einem Klick auf das dunkelgrau markierte Feld erledigen (Abb ??).

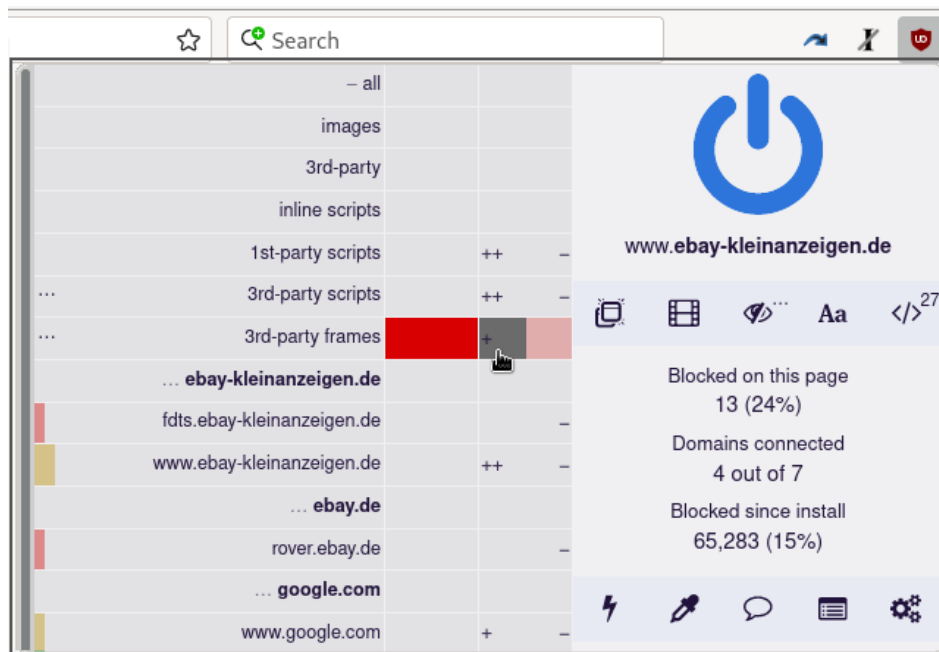


Abbildung 4.12: iFrames von Drittseiten für die aktuelle Webseite freigeben

Danach muss man die Webseite neu laden und 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 URL-Parameter

URL-Parameter werden häufig für mit folgenden Intentionen für das Tracking verwendet:

1. Beim Tracking des Erfolgs von Werbe-Kampagnen 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.

Diese Technik wurde von der Urchin Software Corporation entwickelt, die 2005 von Google übernommen und in das eigene Portfolio integriert wurde. Deshalb beginnen die Tracking Parameter bei Google noch heute mit *utm_* (Urchin Tracking Module).

2. Mit dem URL-Campagnen-Mapper von WebTrek 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 Webseiten-übergreifendes Tracking ermöglichen.

Facebook hängt beispielsweise 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 webseiten-übergreifend (und App-übergreifend) ohne Cookies/EverCookies zu tracken.

Ein Beispiel von der Webseite heise.de (Mobilversion) zeigt beide Anwendungen für das Tracking mit URL-Parametern durch WebTrek 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 beispw. einen Kanal im Messenger Telegram und posten Links zu aktuellen Artikeln. Diese Links sind mit Tracking Parametern verseucht.

Trackingparameter aus URLs löschen

Auch mit dem Add-on **uBlock Origin** kann man Parameter aus URLs entfernen. Dafür muss man eine Liste von Filterregeln erstellen, beispielsweise für das Facebook Tracking:

```
$removeparam=fb_action_ids
$removeparam=fb_action_types
$removeparam=fb_comment_id
$removeparam=fb_ref
$removeparam=fb_source
$removeparam=fbclid
```

...oder Tracking Parameter auf einer bestimmten Webseite (beispw. eBay):

```
||www.ebay.$removeparam=_trkparms
||www.ebay.$removeparam=_trksid
||www.ebay.$removeparam=amdata
||www.ebay.$removeparam=mkrid
||www.ebay.$removeparam=campid
```

Das AdGuard Team stellt eine Filterliste für Tracking Parameter bereit, die in uBlock Origin in dem Abschnitt *Privatsphäre* enthalten ist und die man einfach aktivieren kann.

4.9 Zugriff auf lokale URLs blockieren

Neugierige oder bössartige 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 oder auf andere Dienste im lokalen Netzwerk (LAN) zugreifen:

- Auf der [TAILS-Dev] Mailingliste wurde darauf hingewiesen, dass ein Angreifer oder Trackingdienst JavaScript Code in eine Webseite einbetten könnte, der das interne LAN nach Servern scannt oder versucht lokale Dienste wie den Druckerservice CUPS unter der Adresse *http://localhost:631* zu kontaktieren und diese Informationen zum Fingerprinting nutzt, um den Surfer später wiederzuerkennen.⁴⁸

⁴⁸<https://mailman.boum.org/pipermail/tails-dev/2015-April/008607.html>

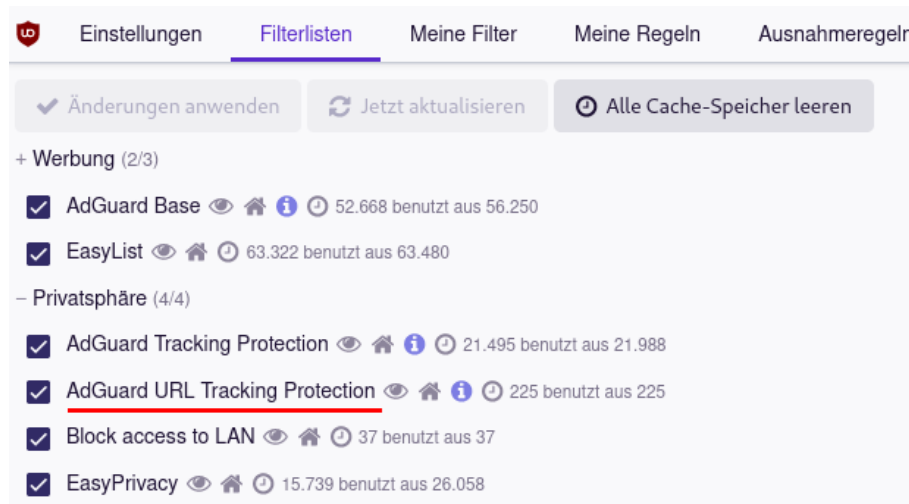


Abbildung 4.13: uBlock Origin: Filterliste für Tracking Parameter in URLs aktivieren

- Bösartiger JavaScript Code könnte lokale Dienste wie CUPS oder andere Rechner im LAN angreifen. Im Mai 2015 wurde ein Exploit-Kit entdeckt, der als böses JavaScript auf Webseiten platziert wird und bei Aufruf der Webseite den Router angreift, um DNS Einstellungen zu ändern und den Internetzugriff beliebig zu manipulieren.⁴⁹
- 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 sich um ein Sicherheitsfeature und keinen Angriff oder Tracking, aber trotzdem...

JS-Restrictor: Network Boundary Shield (bevorzugt)

Das Network Boundary Shield (HTTP Shield) vom Add-on JS-Restrictor ist nach der Installation standardmäßig aktiv. Es blockiert alle Zugriff von Webseiten aus dem Internet 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 vom lokalen Netz 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 (Abb: 4.14).

Hinweis: das eine Webseite irgendwie nicht wie erwartet unktioniert, ist KEIN plausibler Grund für die Deaktivierung. Das zeigt nur, dass ein Angreifer aktiv versucht, etwas zu tun, was verboten wurde. Gerade in dieser Situation wäre die Schutzfunktion wichtig.

Man sollte sich nicht so einfach austricksen lassen und eine Schutzfunktion ohne plausibel Grund deaktivieren, nur weil man neugierig ist und sehen will, wie die Webseite korrekt dargestellt wird.

uBlock Origin Filterliste

Nachdem eBay im Mai 2020 begonnen hatte, die lokalen Ports zu scannen, hat das uBlock Team die *Block Intrusion into LAN* Liste erstellt, die im Abschnitt *Privatsphäre* zu finden

⁴⁹<https://heise.de/-2665387>

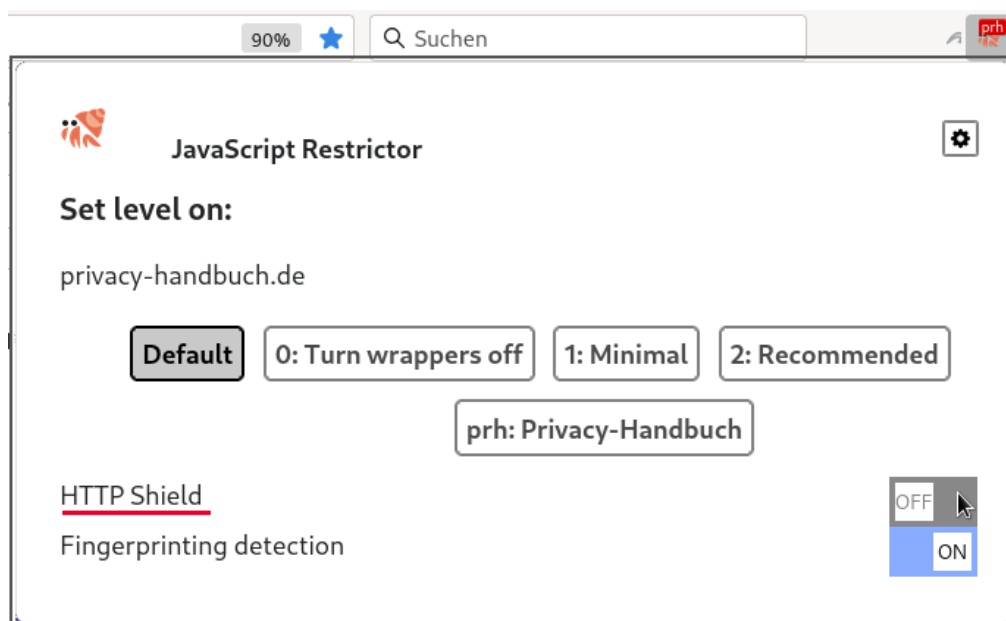
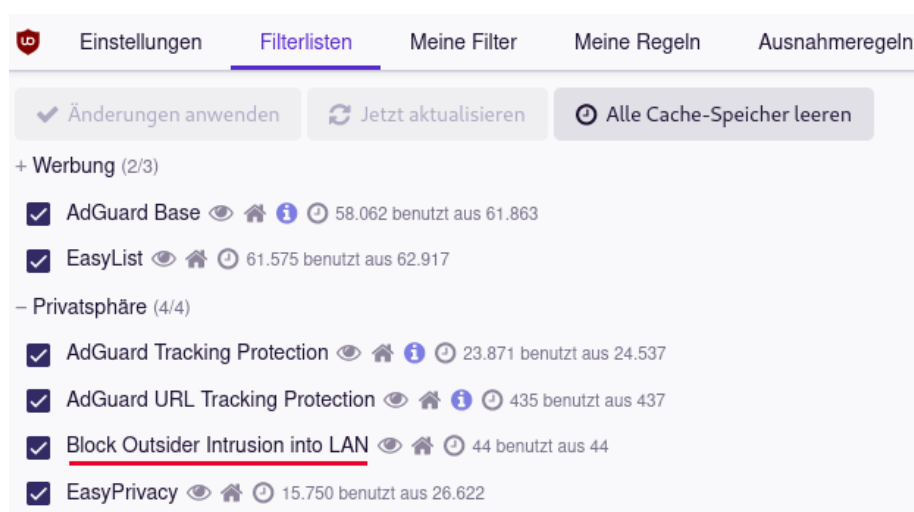


Abbildung 4.14: Network Boundary Shield für eine Webseite deaktivieren

ist (Abb: 4.15). Diese Filterliste kann als Alternative nutzen, wenn man das Add-on JS-Restrictor nicht verwenden möchte oder (wenn man will) zusätzlich zum Network Boundary Shield von JS-Restrictor verwenden.

Abbildung 4.15: 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 Domain 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 externe Webseiten zu sperren. Dafür fügt man auf dem Reiter *Meine Filter* eine Regel nach folgendem Muster hinzu:

```
||<lokale DNS Domain>~$3p,domain=~localhost|~127.0.0.1|~[::1]|~0.0.0.0|~[::]|~local
```

4.10 Firefox activity-stream

Der activity-stream ist auf der NewTab Page und der Startseite aktiv. Unter einem Suchfeld werden häufig besuchte Webseiten angezeigt sowie individuell optimierte Vorschläge für populäre Webseiten, die von Pocket ausgewählt werden. Außerdem verkauft Mozilla Plätze in den Empfehlungen für Werbung, die als *Gesponsert von...* gekennzeichnet wird.

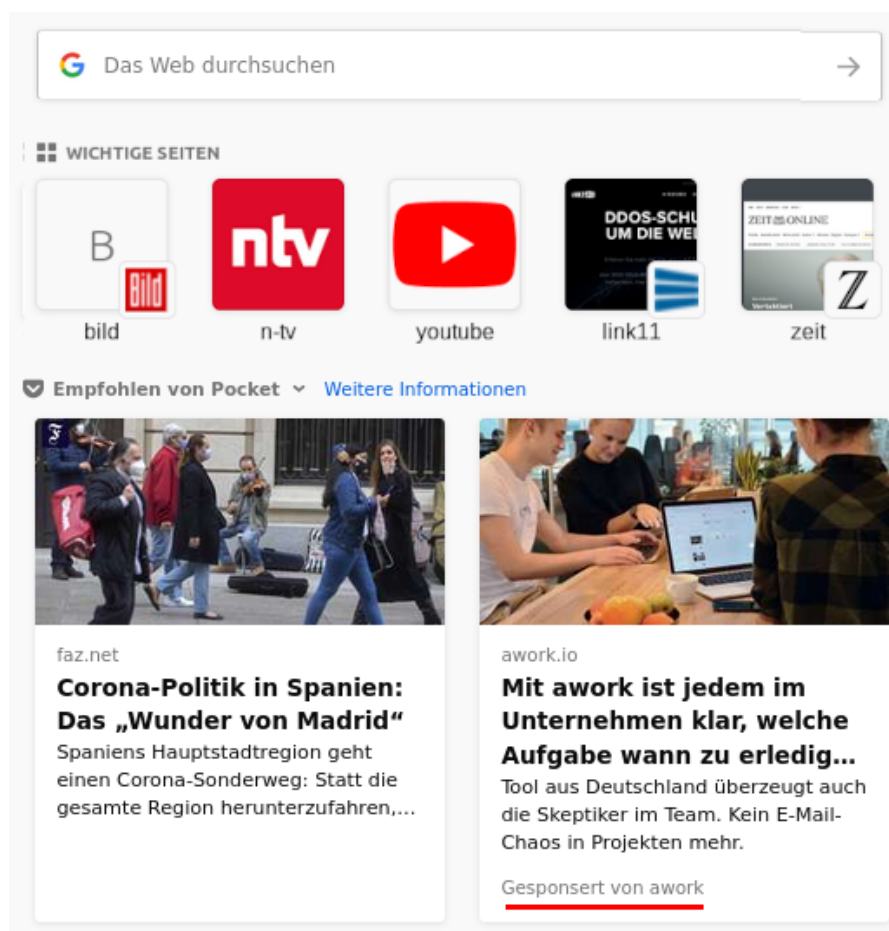


Abbildung 4.16: Gesponserte Empfehlungen auf der NewTab Seite und Startseite

- 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 privacy-relevant.

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, dann signalisiert man damit 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 der activity-stream vom User abgeschaltet wurde.

(Also wieder jemand, der sich für unsere Interessen interessiert, um tolle Vorschläge zu machen, und mit individuellen Vorschlägen ein bisschen Werbung verteilt.)

Beim Test der Funktion wurden Webseiten wie Bild.de, Youtube.com und ähnliches 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. 4.18: *wt3_eid* und *wt3_sid* sind Tracking Cookies von WebTrek), obwohl www.Bild.de nie aufgerufen wurde.

Wie konnte die Webseite Bild.de die Trackingcookies setzen? Um die NewTab Page darzustellen (seit Firefox 61 auch die Startseite), holt Firefox eine JSON Datei von Mozilla, die eine Liste mit den 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, um einige Trackingcookies zu setzen. Das ist bei anderen Empfehlungen auch möglich.

activity-stream deaktivieren

Mit Firefox 57 hat Mozilla den *activity-stream* in der NewTab Page integriert und mit Firefox 61 auch auf der Startseite, die standardmäßig genutzt wird. Außerdem wurde in Firefox 61 eine grafische Konfigurationsmöglichkeit integriert, um es zu deaktivieren. Seit Firefox 78 erscheinen Vorschläge aus dem *activity-stream* zusätzlich bei Eingabe einer URL und seit Firefox 83 werden Plätze in den Empfehlungen als Werbeflächen verkauft.

Unter der Adresse *about:config* kann man Einstellungen ebenfalls 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, dann kann man folgende Parameter unter *about:config* setzen:

```
browser.startup.page      = 1
browser.startup.homepage = <URL>
```

Bezahlte Werbeeinblendungen deaktiviert mit 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 NewTab Page ohne überflüssigen Schnickschnack und wird nicht mit handverlesenen Empfehlungen belästigt. Beim Starten kontaktiert Firefox aber weiterhin die Server mit dem Empfehlungen und holt die aktuellen Dateien. Das kann man Firefox mit folgenden Optionen abgewöhnen:

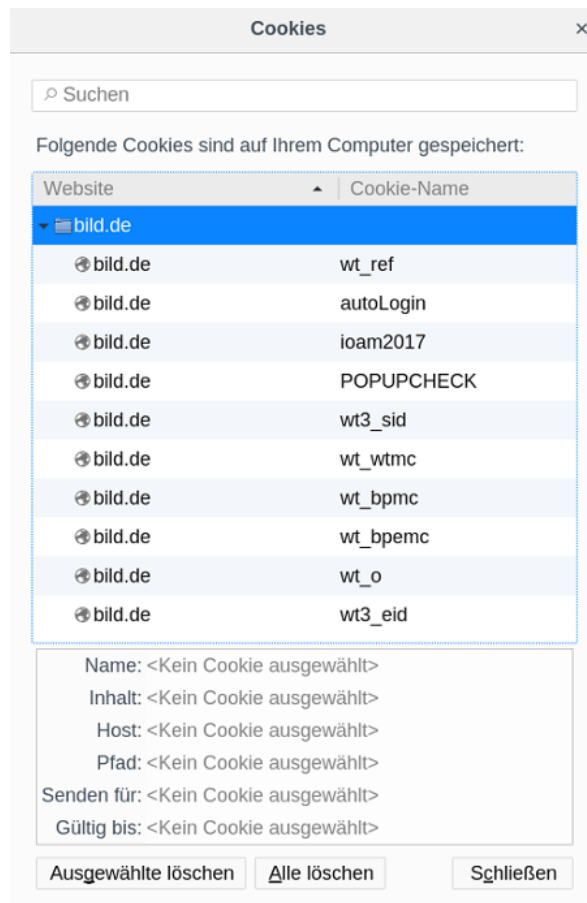


Abbildung 4.17: Cookies von Bild.de nach Aufruf eines neuen Tab

```

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 werden außerdem Telemetrie Pings an den Pocket Server gesendet und Firefox teilt damit dem Pocket Server 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

```

Außerdem ist die Ping-Centre Funktion für Datenversand zu deaktivieren:

```

browser.ping-centre.telemetry = false

```

Firefox speichert Screenshots von jeder besuchten Webseite auf der Festplatte, um sie später als Thumbnails *activity-stream* einzublenden. Diese Speicherung gefällt mir nicht, da ich mein Surfverhalten nicht protokollieren möchte, auch nicht auf dem eigene Rechner. Da man diese Thumbnails nicht mehr benötigt, wenn eine leere Seite statt des *activity-stream* angezeigt wird, kann man eine neue Variable vom Typ Boolean unter `about:config` erstellen um die Erstellung der Thumbnails zu deaktivieren:

```

browser.pagethumbnails.capturing_disabled = true

```

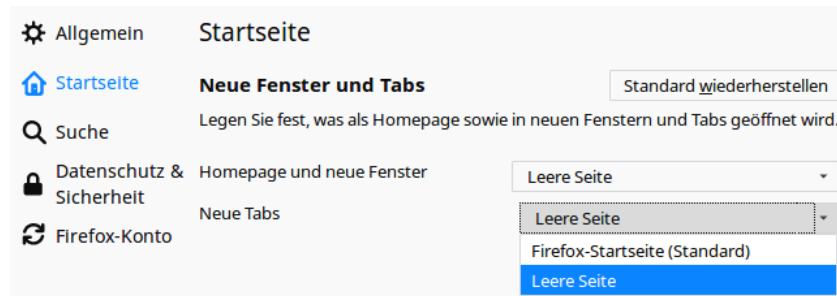


Abbildung 4.18: Leere Seite für Startseite und neue Tabs konfigurieren

4.11 Contextual Feature Recommender (CFR)

Mit Firefox 64.0 hat Mozilla den Contextual Feature Recommender (CFR) eingeführt, was einfach gesagt nur ein Werbesystem für Add-ons und Features ist.

Mir ist unklar, nach welchen Richtlinien Mozilla die Empfehlungen für Add-ons auswählt. Mit der Empfehlung für das Web-Security Add-on hatte Mozilla schon gründlich daneben gegriffen und ein Tracking Add-on als Trackingschutz empfohlen (Bugzilla #1483995). Das Add-on *Web-of-Trust* konnte sich ebenfalls lange als angebliches Security Add-on verkaufen bevor man entdeckte, dass mit diesem Add-on massenweise Daten gesammelt wurden.⁵⁰

Man sollte Add-ons nicht wahllos aufgrund irgendwelcher Empfehlungen installieren, die nicht nachvollziehbar sind. Konzeptloses Zusammenwürfeln von irgendwelchen Privacy Add-on, wie es Mozilla z. B. im Blogartikel *Make your Firefox browser a privacy superpower with these extensions*⁵¹ empfiehlt, ist kein guter, sinnvoller Ansatz. Deshalb kann man den Contextual Feature Recommender abzuschalten, um nicht belästigt zu werden.

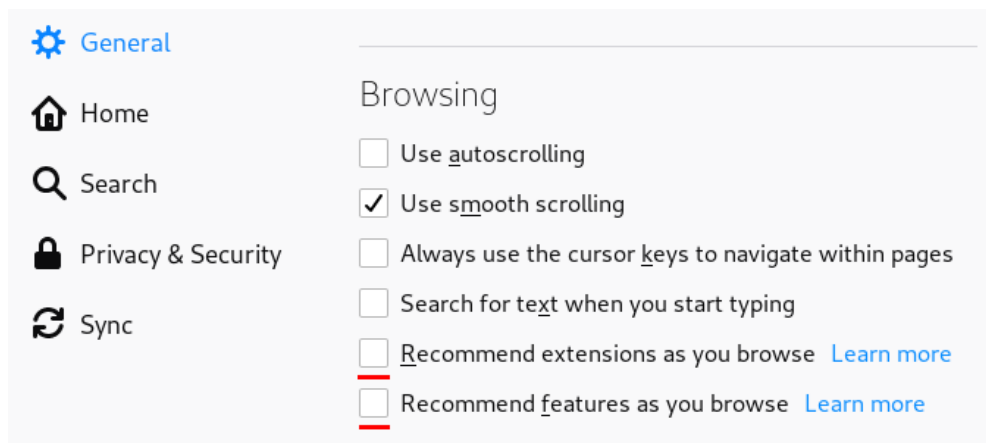


Abbildung 4.19: Contextual Feature Recommender (CFR) deaktivieren

In den Einstellungen findet man die Option im Bereich *Allgemein* unter *Browsing* (Abb. 4.19). Unter *about:config* kann man folgende Variablen setzen:

```
browser.newtabpage.activity-stream.asrouter.userprefs.cfr.addons = false
browser.newtabpage.activity-stream.asrouter.userprefs.cfr.features = false
```

⁵⁰<https://www.tagesschau.de/inland/tracker-online-103.html>

⁵¹<https://blog.mozilla.org/firefox/make-your-firefox-browser-a-privacy-superpower-with-these-extensions/>

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
```

4.12 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 sowie E-Mail Adressen der Surfer konnten ermittelt werden.⁵²

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 verwendete diese Trackingtechnik seit 2011.⁵³

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 in Firefox 85+ standardmäßig aktiviert. In Firefox 78 ESR aktiviert man *FirstParty.Isolation* als Schutz.

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.

Die Einstellungen zum Löschen des Cache und der Chronik beim Schließen des Browsers findet man in den *Einstellungen* in Sektion *Datenschutz und Sicherheit* (Abb. 4.20).

Wenn man auf den Button *Einstellungen* hinter *Die Chronik löschen, wenn Firefox geschlossen wird*, kann man festlegen, welche Daten beim Schließen des Browsers gelöscht werden.

Alternativ kann man unter *about:config* folgende Werte setzen:

⁵²<https://www.heise.de/newsticker/meldung/Plaudertasche-Web-Browser-erleichtert-Deanonymisierung-919076.html>

⁵³<https://heise.de/-1288914>

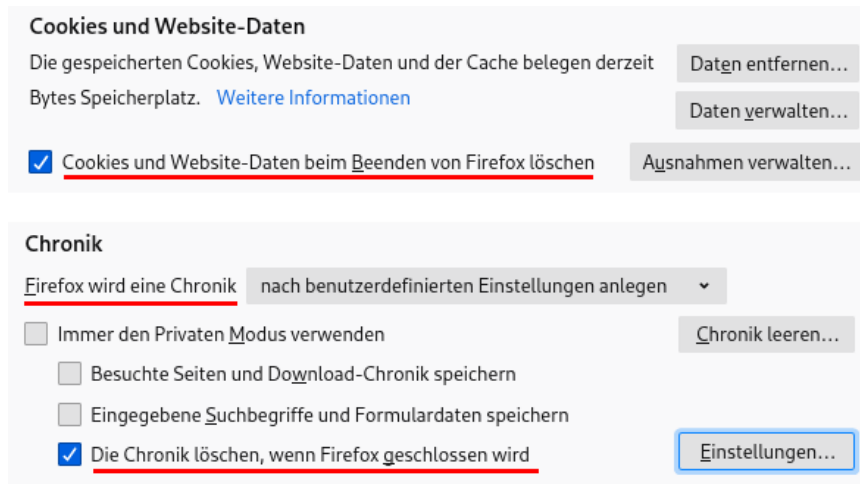


Abbildung 4.20: Deaktivieren der Surf-History und Löschen des Cache

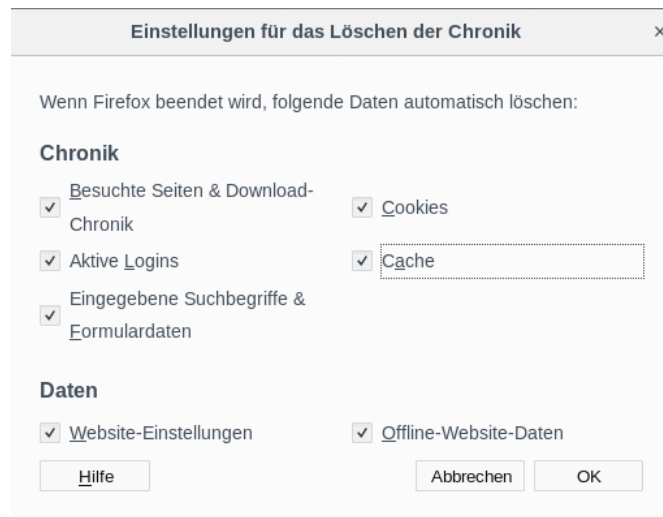


Abbildung 4.21: Konfiguration der zu löschenden Daten beim Beenden

```

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. 4.22).

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 ver-

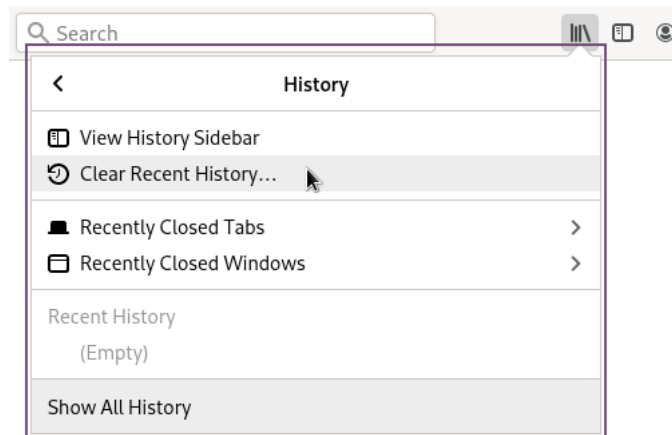


Abbildung 4.22: Chronik während des Surfens löschen

meiden, 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
```

4.13 Referer

Mit jedem Klick auf einen Link sendet Browser einen Referer im HTML Header an die aufgerufenen 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 UserID (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 wurde 120 populäre Webseiten untersucht. 56% der Webseiten sendeten nach dem Login private Informationen wie E-Mail Adresse, Name oder Wohnort an Trackingdienste.

Mit Firefox 87 (März 2021) hat Mozilla auf dieses Risiko für die Privatsphäre reagiert und kürzt den Referer beim Aufruf von Elementen von Drittseiten auf die Domain. Das Beispiel für den Aufruf eines Werbebanners von DoubleClick sieht dann so aus:

```
GET http://ad.doubleclick.net/adj/....
Referer: http://submit.sports.com/
Cookie: id=123456789.....
```

⁵⁴<http://w2spconf.com/2011/papers/privacyVsProtection.pdf>

Firefox bietet auch die Möglichkeit, das Senden des Referers an Drittseiten zu blockieren. Dafür setzt man unter der Adresse *about:config* folgende Option:

```
network.http.referer.XOriginPolicy = 2
```

Mit dieser Einstellung werden Subdomains als Drittseiten behandelt und es wird auch an Subdomains kein Referer gesendet. Das schützt somit auch gegen Trackingdienste, die sich mit DNS-Aliases als Subdomains auf populären Webseiten einschleichen (z. B. Web-Trekk bei Heise.de und Zeit.de). Allerdings bringt es möglicherweise vereinzelt Probleme bei einigen Websites mit sich. Folgende Einstellung minimiert die Probleme:

```
network.http.referer.XOriginPolicy = 1
```

Damit werden Subdomains wie die Hauptdomain behandelt und es wird ein Referer gesendet. Lediglich an echte Drittseiten wird kein Referer übergeben.

Einige Webseiten zum Thema Privacy empfehlen, das Senden des Referers mit folgender Option komplett zu deaktivieren:

```
network.http.sendRefererHeader = 0
```

Diese Einstellung ist nicht empfehlenswert, da es den Schutz gegen Tracking nicht wesentlich verbessert. Innerhalb einer Domain kann der Webmaster einen Surfer immer verfolgen, mit oder ohne Referer. Die Einstellung führt statt dessen zu einem individuellen Fingerprint, da der Request-Header ganz ohne Referer sich von den 99% der anderen Surfer unterscheidet. Außerdem hat man öfters seltsame Probleme, weil Spam-Schutz Module in Diskussionsforen und Blogs oft den Referer als Feature zur Erkennung von Spam-Bots auswerten.

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 PPlugins aktiviert. Um zu verhindern, dass 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:

OpenH264 Videocodec von Cisco wird für WebRTC benötigt. Wenn man WebRTC abschaltet, kann man auch den Videocodec und das Update deaktivieren (bei einige Linux Distributionen wie Fedora ist es standardmäßig so konfiguriert)

```
media.gmp-gmpopenh264.autoupdate = false
media.gmp-gmpopenh264.enabled    = false
```

Außerdem kann das OpenH264 Plugin in der Add-on Verwaltung ausblenden:

```
media.gmp-gmpopenh264.visible = false
```

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 es wirklich nicht verwenden will 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-ins für die Anzeige von PDF-Dokumenten im Browser war über viele Jahre ein erhebliches Sicherheitsrisiko. 2008 gelang es dem *Ghostnet*, mit böartigen PDF Dokumenten die Computernetze westlicher Regierungen, der US-Regierung und des Dalai Lama zu infizieren, dem Trojaner *MiniDuke* gelang es 2012, mit böartigen 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 böartigen 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). Für hohe Sicherheitsanforderungen kann man die Anzeige von PDF-Dokumenten im Browser deaktivieren und damit die Angriffsfläche für Drive-By-Download Angriffe verringern:

```
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.org⁵⁵ Open Source Alternativen vor.

- Für Windows werden *Sumatra PDF* oder *MuPDF* empfohlen.
- Für Linux gibt es *Okular* (KDE) und *Evince* (GNOME, XFCE, Unity).
- Für MacOS wird *Vindaloo* empfohlen.

Die Linux Distribution **QubesOS** bietet für potentielle *Landesverräter* und andere Risikogruppen, die als Target für den Einsatz der neuen Bundestrojaner in Frage 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

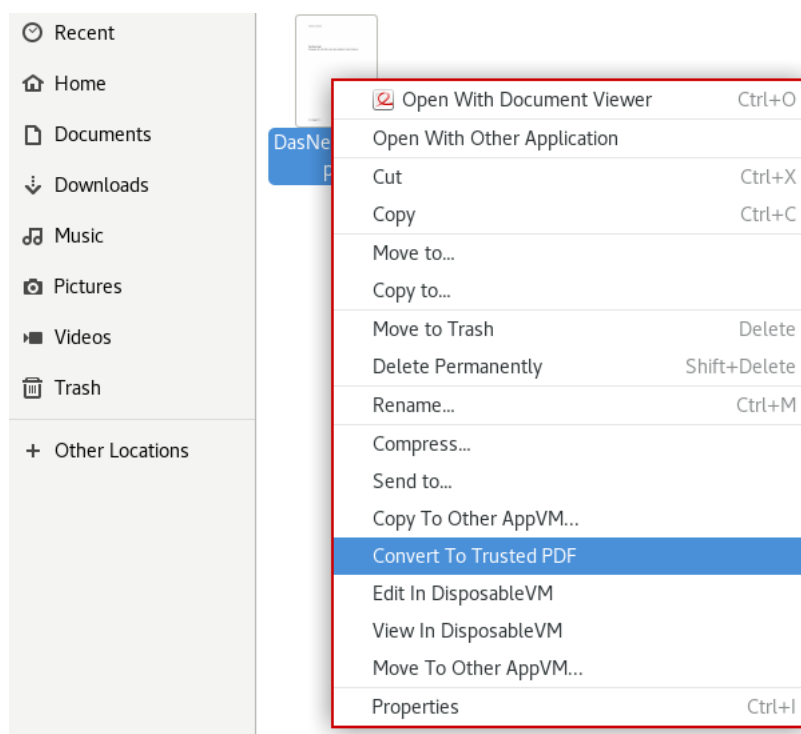


Abbildung 4.23: Konvertierung von PDFs im Dateimanager in QubesOS

Download mit einem Rechtsklick auf ein PDF Dokument im Dateimanager aufrufen.

Für die Umwandlung in Trusted PDFs wird *qubes-app-linux-pdf-converter*⁵⁶ gestartet, das Rendering des (möglicherweise bössartigen) PDF Dokumentes 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!)

4.15 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.

- 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.

Denn HTTPS-First-Mode aktiviert man unter *about:config* mit folgender Einstellung:

⁵⁵<http://www.pdfreaders.org/index.de.html>

⁵⁶<https://github.com/QubesOS/qubes-app-linux-pdf-converter>

```
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: 4.25).

Den HTTPS-Only-Mode kann man in den grafischen Einstellungen in der Sektion *Datenschutz und Sicherheit* aktivieren (Abb: 4.24).

Alternativ kann man unter *about:config* folgenden Wert setzen:

```
dom.security.https_only_mode = true
```

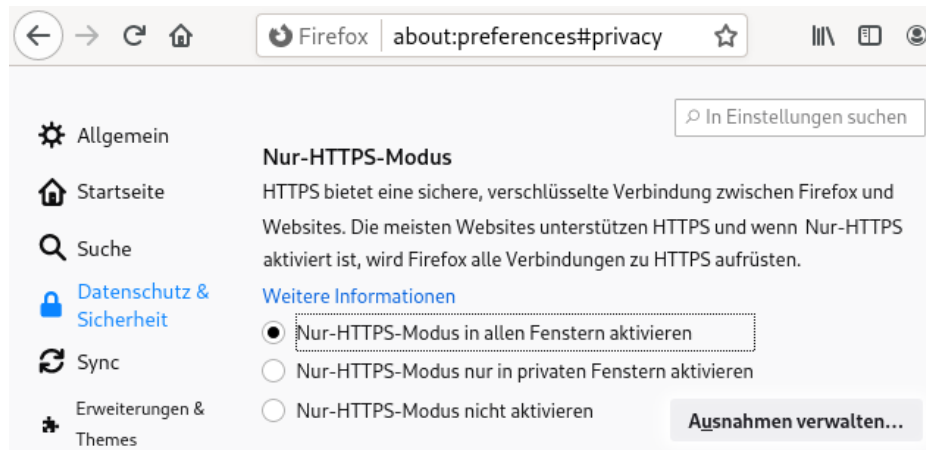


Abbildung 4.24: Nur-HTTPS-Mode in Firefox aktivieren

Außerdem kann man Ausnahmen für Webseiten definieren, für die kein HTTPS erzwungen werden soll. Die Konfiguration des Routers ist somit problemlos möglich.



Abbildung 4.25: Warnung bei Aufruf einer unverschlüsselten HTTP Seite

- 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
```

- über unsichere Verbindungen werden in Firefox 92+ standardmäßig blockiert. In Firefox 91 ESR muss man dafür folgende Option unter `about:config` setzen:

```
dom.block_download_insecure = true
```

(Da seriöse Downloads in der Regel über HTTPS angeboten werden, ist diese Option immer empfehlenswert in allen `user.js` Konfigurationen aktiviert.)

- *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-Protokoll 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
```

- *Certificate Pinning* schützt gegen Man-in-the-Middle Angriffe. Mit folgender Option wird für eine populäre Webseiten wie Google, Youtube, Twitter, TorProject, Dropbox u.a. ein 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 Virens Scanner 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 beispw. oft üblich eigene Root Zertifikate für interne Webseiten und HTTPS Proxy Server zu verteilen. Wenn Virens Scanner als MitM den HTTPS Traffic scannen wollen, nutzen sie auch 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`:

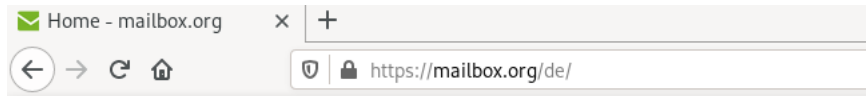
```
security.certerrors.mitm.auto_enable_enterprise_roots = false
```

Bei Bedarf kann man 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.

4.15.1 Anzeige der HTTPS Verschlüsselung

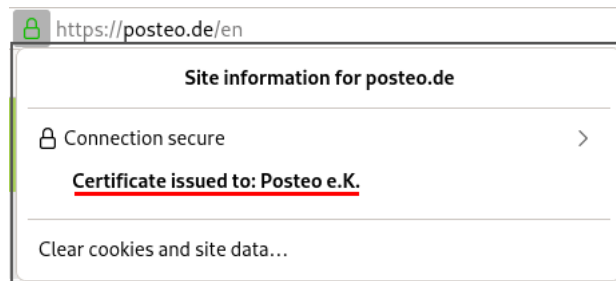
Standardmäßig zeigt Firefox 70+ einen HTTPS-verschlüsselten Transport der Daten nur mit einem kleinen, unscheinbar grauen Icon neben der Adresse an:



Etwas auffälliger war das beruhigende Grün für das Symbol bei älteren Firefox Versionen, welches man mit folgender Option unter *about:config* wieder aktivieren kann:

```
security.secure_connection_icon_color_gray = false
```

Neben einfachen SSL-Zertifikaten gibt *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:



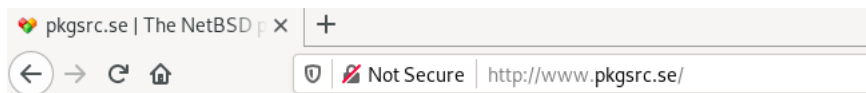
Außerdem kann man sich anzeigen lassen, wenn die Verbindung zum Webserver nicht verschlüsselt ist. Für ein Warn-Icon aktiviert man unter *about:config* folgende Optionen:

```
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:



4.15.2 Vertrauenswürdigkeit von HTTPS

IT-Sicherheitsforscher der EFF kamen bereits 2009 in einer wiss. 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.⁵⁷

⁵⁷<https://eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl>

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 fertige 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 jährlich im März in Dubai 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*⁵⁸ oder *dsniff*⁵⁹ 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-Zertifikate für schwer erkennbare man-in-the-middle Angriffe zu kombinieren:

1. Für einen großflächiger 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.
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 Disaster:

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 um eine staatliche Überwachung, einen Hackerangriff oder einen Konfigurationsfehler(?) handelt, ist unklar.⁶⁰

3. Die Anbieter von Webdiensten können zur Herausgabe der eigenen Zertifikate 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 Zertifikate 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.

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.⁶¹
- 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.
- 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 der genannten E-Mail Adressen ist oft die einzige Prüfung auf Rechtmäßigkeit durch die CAs.

⁵⁸<http://crypto.stanford.edu/ssl-mitm/>

⁵⁹<http://www.monkey.org/~dugsong/dsniff/>

⁶⁰<https://www.heise.de/-2255992>

⁶¹<https://www.heise.de/-2058883>

4.15.3 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*⁶² können das automatisiert ausführen. Die Validierung via OCSP Server bringt kaum Sicherheitsgewinn.⁶³

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/gsignorganizationvalg2 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-Anfrage und Antworten unverschlüsselt übertragen werden, kann auch ein *Lauscher am Draht* diese Informationen abgreifen. Aus Privacy Gründen 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:

```
security.OCSP.enabled = 1
security.OCSP.require = true
```

Da es keine klare Empfehlung für eine Abschaltung oder verschärfte Durchsetzung von OCSP gibt, enthalten 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 aber die Nachteile von beiden Varianten.

OCSP.Stapling ist ein modernes Verfahren, dass die oben genannten 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. Der bekannte Test für Webserver Qualys SSL Labs wird ab Jan. 2017 die Bestnote A+ nur

⁶²<https://moxie.org/software/sslsniff>

⁶³<https://www.thoughtcrime.org/papers/ocsp-attack.pdf>

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
```

4.15.4 Tracking via TLS Session

Beim Aufbau einer verschlüsselten HTTPS-Verbindung zwischen Browser und Webserver wird eine sogenannte Session initialisiert. Diese Session kann für 48h 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 5077⁶⁴).

Die TLS-Session-ID kann von nahezu allen Webserven 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*⁶⁵). Dieses Tracking-Verfahren 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 webseite-übergreifende Tracking beim Surfen.
- Löschen von Cache und Sessions beim Schließen des Browsers verhindert das langfristige Tracking über einen längeren Zeitraum.

4.15.5 Tracking via HTTP Strict Transport Security (HSTS)

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 Bad Tor Exit Nodes aktiv genutzt.

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 kann⁶⁶. 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.⁶⁷

Mit dem Nur-HTTPS-Modus von Firefox ist man gegen dieses exotische Tracking geschützt.

⁶⁴<https://tools.ietf.org/html/rfc5077>

⁶⁵http://www.modified-shop.org/wiki/SESSION_CHECK_SSL_SESSION_ID

⁶⁶<http://heise.de/-2511258>

⁶⁷<https://heise.de/-3998754>

4.15.6 Tracking Risiko durch seltsame Auswahl der SSL/TLS Cipher

Wenn der Browser eine SSL-verschlüsselte Verbindung zu einem Webserver aufbauen will, dann sendet er 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 sendete:

```
<e name='Chrome/57.0.2951.0' protocol='771' greaseExt='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 Webseite 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 Ciphern 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.

4.16 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 fingerprints*⁶⁸ der KU Leuven (2013) kommt zu den 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 5min 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 vom 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 24h im Cache gespeichert.

⁶⁸<https://www.cosic.esat.kuleuven.be/publications/article-2334.pdf>

Für das Laden von Schriftarten vom Google Font Service gelten die Datenschutzbestimmung von Google⁶⁹. Viele Webseiten weisen in den Privacy Statements nicht darauf hin, dass beim Aufruf der Webseite Daten bei Google gespeichert und verarbeitet werden.

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 böartigen 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 böartigen Fonts den Rechner anzugreifen und Code mit Systemrechten auszuführen.⁷⁰

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 Jan. 2021 wurde ein komplexer Angriff auf Windows Rechner und Android Smartphones publiziert, bei dem böartige Schriften auf Webseiten eingebunden wurden 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 verbrannt.

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 Fonts 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.

Konfiguration der Schriftarten in Firefox

Um das Laden von externen 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 = false
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:

⁶⁹<https://www.google.com/intl/de/policies/privacy>

⁷⁰<https://www.heise.de/-4155012>


```
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.

Verfassen

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
```

Verfassen

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, sollten man gut lesbare Standardschriften verwenden. Unter Windows eignet sich *Arial*, unter Linux eignet sich *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.

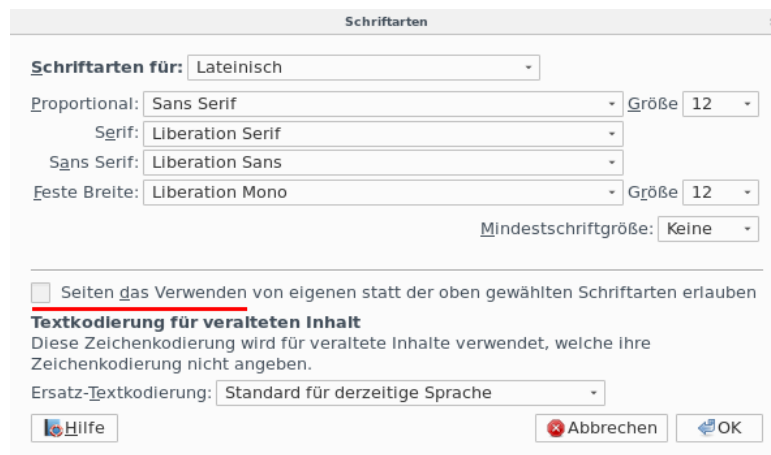


Abbildung 4.26: Schriftarten auswählen

4.17 Hardware Fingerprinting

Über verschiedenen API-Schnittstellen können Trackingscripte Informationen über die Hardware des Rechners sammeln. Durch Messung der Performance aufwendiger Grafik Rendering Operationen oder beim Abspielen von Videos können Trackingscripte ebenfalls Informationen über die Hardware sammeln.

Grafikhardware: Die Hardwarebeschleunigung des Rendering kann man deaktivieren, um ein Fingerprinting der Grafikhardware zu verhindern. Die Einbußen sind kaum erkennbar.


```
gfx.direct2d.disabled           = true
layers.acceleration.disabled    = true
media.hardware-video-decoding.enabled = false
```

Statistiken für Videos: Die Übermittlung von Statistiken beim Abspielen von Videos (Frame-rate usw.) kann unter *about:config* deaktiviert werden:

```
media.video_stats.enabled = false
```

Vibrator-API: kann eine Vibration des Gerätes auslösen. 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. Un auffälliger ist es, die max. 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 Helligkeit der Umgebung abfragen.
2. Proximity Sensor: kann Objekte in der Nähe erfassen.
3. Device Orientation Sensor: liefert Informationen, wie ein Phone gehalten wird.
4. Device Motion Sensor: liefert Informationen über die Bewegung des Gerätes.

Die ersten beiden APIs sind privacy-relevant und können zum Sammeln Daten missbraucht werden, wie der Sicherheitsexperte L. Oljenik für den Proximity und 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 in keine Daten und können daher aktiviert bleiben. Webseiten könnten eine Deaktivierung erkennen und als Merkmal für das Fingerprinting verwenden, wie Browsersleaks demonstriert.⁷¹

Aus den gleichen Gründen wird die Deaktivierung der gesamten Sensor-API nicht empfohlen. Für Smartphones ist das Risiko anders zu bewerten..

4.18 WebRTC mit Firefox

WebRTC wurde von Google und Mozilla initiiert und später vom W3C standardisiert, um der Konkurrenz von Microsoft Skype etwas entgegen zu setzen. Google und Mozilla entschieden sich dafür, die Funktionalität in die Browser zu integrieren, um den Browser als univerelle Anwendung für jegliche Internetkommunikation auszubauen.

Neben der Internettelefonie wird WebRTC auch bei browserbasierten Video-konferenzsystemen wie Jitsi Meet eingesetzt. Bei der direkten 1:1 Kommunikation ist für

⁷¹<https://browserleaks.com/features>

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 Lösung mit durchgehende Ende-zu-Ende Verschlüsselung für Konferenzsysteme sind in der Entwicklung.)

OpenH264 Videocodecs

Um WebRTC mit Firefox zu verwenden, wird das OpenH264 Plugin von Cisco benötigt, das die Videocodecs bereitstellt. Das Plugin ist Closed Source und wird beim ersten Start von Firefox automatisch heruntergeladen und im Profilverzeichnis gespeichert.

Mit folgende Einstellungen unter *about:config* wird das OpenH264 Plugin 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 Plugin standardmäßig deaktiviert. Oft sind Probleme mit browserbasierten Videokonferenzen darauf zurück zu führen, dass das Plugin nicht aktiviert wurde.

Internet Connectivity Establishment (ICE)

Der Datenstrom soll bei WebRTC möglichst direkt zwischen den Teilnehmern ausgetauscht werden. Es wird der ICE Standard (Internet Connectivity Establishment) verwendet, um eine direkte Verbindung zwischen den Clients aufzubauen. 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... 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 Browserleaks⁷² zeigt:

| | |
|-------------------------------|---|
| WebRTC IP Address Detection : | |
| Local IP Address |  172.18.19.18 |
| Public IP Address |  213.220.153.3 |
| IPv6 Address | n/a |

- 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.)
- 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.)
- Externe Adresse des Proxy oder VPN Endpunktes. (Diese Information lässt sich natürlich nicht geheim halten.)

Firefox bietet einige Möglichkeiten, die Privacy Probleme 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 man es abschalten:

⁷²<https://browserleaks.com/webrtc>

```
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 ziehen könnte, 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 der 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-Proxy 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 für das Hardware Fingerprinting zu verwenden. Der Surfer wird dabei nicht um Zustimmung für einem Zugriff auf Kamera oder Mikrofon gebeten. Der WebRTC Test von Browserleaks demonstriert es.

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 oder nicht geeignet wie Cookies und als Schutz gegen Tracking anhand der Device-IDs kann man die Empfehlungen für Cookies umsetzen.

WebRTC Media Devices :

| | |
|---------------------------|---|
| Device Enumeration | ✓ True |
| Has Microphone | ✓ True |
| Has Camera | ✗ False |
| Audio Capture Permissions | ? |
| Video Capture Permissions | ? |
| Media Devices | <pre> kind: audioinput label: n/a deviceId: IYM6u8ZPLpPShf2Sv69aw9sumF17fYUtFUIS1Ve0XNY= groupId: IIWmH+FbBbMr5QRZWUpSm4MPLcrDOKNWDf1WJHmXZ3A= kind: audioinput label: n/a deviceId: XXG8Vx6rRzpMkrrDctvydK5uMnN/tg0w6gssvrDEjUs= </pre> |

Abbildung 4.27: Media Device Enumeration via WebRTC

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 Browserfingerprint 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

```

4.19 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 *DNS und DNSSEC*.

Firefox kann DNS-over-HTTPS nutzen, um die DNS Daten beim Surfen zu verschlüsseln und eine Zensur durch DNS-Server der Provider zu umgehen. Das Feature heißt TRR (Trusted Recursive Resolver). Die Konfiguration ist einfacher, als als einen DNS Daemon mit DNS-over-TLS Support oder DNSCrypt zu installieren. Es schützt allerdings nur den DNS Datenverkehr beim Surfen mit Firefox und 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.

Browserfingerprinting mittels DNS Server

Eine Trackingdienst könnte ermitteln, welcher DNS-Server vom Browser verwendet wird, und diese Information als Parameter für das Fingerprinting des Browser verwenden:

1. Der Webserver sendet im HTML Code ein kleines, überflüssiges Element, dass von einer zufällig generierten Subdomain des Trackingservice geladen werden soll.
2. Der Browser versucht die IP-Adresse für diese Subdomain zu ermitteln. Der konfigurierte Upstream DNS-Server hat die Information nicht im Cache und muss deshalb den autoritativen Server des Trackingdienstes anfragen.
3. Der authoritative DNS-Server des Trackingdienstes registriert die DNS Anfrage und die IP-Adresse des anfragenden DNS-Servers und sendet beides an den Trackingservice, wo die Information mit dem Aufruf der Webseite korreliert werden kann.

Es gibt bisher noch keine Studien, die untersucht haben, ob dieses Verfahren genutzt wird. Aber es ist prinzipiell möglich. Deshalb sollte man kurz nachdenken, ob es Gründe gibt, einen selbst ausgewählten DNS-Server zu nutzen, ob der Vorteil an Sicherheit und Schutz gegen Zensur evtl. unerwünschte Nebeneffekte kompensiert. (Trackingdienste, die via uBlock Origin o.ä. blockiert werden, können auch den DNS Server nicht auswerten.)

Konfiguration in den Netzwerk Einstellungen

In den Einstellungen für die Netzwerkverbindung kann man unter DNS-over-HTTPS aktivieren und die URL für den DNS-Server eintragen, wenn man die Option *Custom* wählt. Eine Liste von Servern findet man unten in der Konfiguration für Experten.

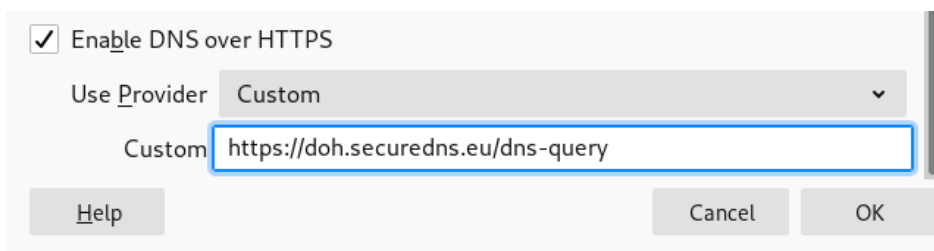


Abbildung 4.28: Konfiguration der DNS-over-HTTPS

Dabei wird der TRR-Mode 2 aktiviert (s.u.). Es wird der TRR Server verwendet und wenn dieser nicht funktioniert, wird automatisch der DNS-Server vom System genutzt. Man würde es nicht bemerken, wenn DNS-over-HTTPS nicht funktioniert. Daher muss man unter *about:networking* bei *DNS* nachschauen, ob es auch funktioniert.

Konfiguration für Experten

Mit folgende 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 (Abgeschaltet aufgrund der Default Einstellung.)
network.trr.mode = 1 (Frage System DNS und TRR und verwendet erstes 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 aufgrund der Entscheidung des Nutzers. FF61+)
```

Firefox für Windows deaktiviert DNS-over-HTTPS unabhängig von den Einstellungen für `network.trr.mode`, wenn ein VPN genutzt wird, wenn ein Proxy in den Windows System Einstellungen 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 Server prüfen und braucht dafür die IP-Adresse des OCSP Servers vom DNS-over-HTTPS Server... Also entweder OCSP komplett deaktivieren:

```
security.OCSP.enabled = 0
```

Oder nicht zwanghaft auf eine OCSP Antwort bestehen:

```
security.OCSP.required = false
```

- Die URL des DNS-over-HTTPS Servers wird mit `network.trr.uri` angegeben:

- DNS-over-HTTPS Server von Freifunk München:

```
network.trr.uri = https://doh.ffmuc.net
```

- DNS-over-HTTPS Server der Digitalen Gesellschaft (CH):

```
network.trr.uri = https://dns.digitale-gesellschaft.ch/dns-query
```

- DNS-over-HTTPS Server von dnsforge.de (mit Ad-Filter):

```
network.trr.uri = https://dnsforge.de/dns-query
```

- DNS-over-HTTPS Server von BlahDNS DE (mit Ad-Filter):

```
network.trr.uri = https://doh-de.blahdns.com/dns-query
```

- DNS-over-HTTPS Server von BlahDNS FI (mit Ad-Filter):

```
network.trr.uri = https://doh-fi.blahdns.com/dns-query
```

- DNS-over-HTTPS Server von Mullvad DNS (mit Ad-Filter)

```
network.trr.uri = https://adblock.doh.mullvad.net/dns-query
```

- DNS-over-HTTPS Server von Mullvad DNS (ohne Ad-Filter)

```
network.trr.uri = https://doh.mullvad.net/dns-query
```

- DNS-over-HTTPS Server von AdGuard (mit Ad-Filter)

```
network.trr.uri = https://dns.adguard.com/dns-query
```

- DNS-over-HTTPS Server von AdGuard (ohne Ad-Filter)

```
network.trr.uri = https://dns-unfiltered.adguard.com/dns-query
```

- Quad9 DNS-over-HTTPS Server:

```
network.trr.uri = https://dns.quad9.net/dns-query
```

- 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 das 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 dieses Angriff 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.ffmpeg.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.com
94.140.14.141 dns-unfiltered.adguard.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 möchte 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 Hotspot 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.)

4.20 Sonstige Maßnahmen

Am Schluss der Konfiguration gibt es noch ein paar kleine Maßnahmen, die überflüssige Features im Browser 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, kann man 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 nur damit deaktivieren, dass man den *Do Not Track* Header aktiviert, was wir nicht empfehlen.

Wenn man einen Screenshot haben möchte, dann gibt es genügend Tools, die Screenshots erstellen können ohne irgendwelche webbasierten Komponenten mit Datensammlung. Die Screenshot Extension von Firefox kann man unter *about:config* abschalten: Wenn ich einen Screenshot haben möchte, dann gibt es dafür genügend Tools, die Screenshots erstellen können und ich entscheide dann, wie ich sie publiziere. Die Screenshot Extension kann man auch unter *about:config* komplett deaktivieren:

```
extensions.screenshots.disabled = true
```

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 Formularedaten. 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 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*⁷³ zeigte. 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 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:

⁷³<https://iehost.net/pdf/w2sp12-final4.pdf>

```
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* and *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 ähnliche 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
```

Kill Switch für Add-ons abschalten

Die Extension blocklist⁷⁴ 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
```

Safebrowsing deaktivieren

Wenn die Safebrowsing Funktion aktiv ist, dann holt Firefox alle 30min 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.

⁷⁴<https://addons.mozilla.org/en-US/firefox/blocked>

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 Virens Scanner und schnell veraltende URL-Listen.

Healthreport und Übertragung von Telemetriedaten deaktivieren

Alle Übertragungen von Telemetriedaten, Healthreport usw. an Mozilla unterbindet man seit Firefox 41 mit folgendem globalen Kill-Switch:

```
datareporting.policy.dataSubmissionEnabled = false
```

Daneben gibt es Parameter für einzelne Reports, die man zusätzlich deaktivieren kann, was aber eigentlich mit dem globalen Kill-Switch erledigt ist.

```
datareporting.healthreport.uploadEnabled = false
```

Zur Deaktivierung des Telemetrie Toolkit setzt man folgenden Wert:

```
toolkit.telemetry.unified = false
```

Einzelne Aktionen zur Telemetrie kann man mit folgenden Optionen deaktivieren:

```
toolkit.telemetry.archive.enabled           = false
toolkit.telemetry.firstShutdownPing.enabled = false
toolkit.telemetry.bhrPing.enabled          = false
toolkit.telemetry.newProfilePing.enabled   = false
toolkit.telemetry.shutdownPingSender.enabled = false
toolkit.telemetry.updatePing.enabled       = false
```

Außerdem kann man das *Ping-Centre* für Datenerhebung und -versand deaktivieren:

```
browser.ping-centre.telemetry = false
```

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:

```
toolkit.coverage.endpoint.base = ""    (leerer String)
toolkit.coverage.opt-out       = true  (laut Mozilla Doku)
toolkit.telemetry.coverage.opt-out = true (im Code verwendet)
```

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
```

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 die 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 diese Webseiten zum Beispiel praktisch keinen Trackingschutz mehr, obwohl die Webseiten teilweise Trackingcode einbinden, den uBlock 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 für Farbe und Hintergrund von HTML Elementen können die Systemfarben der Desktop Umgebung verwenden. Damit sieht die Webseite einer nativen Desktop Anwendung ähnlich. Diese individuellen Farben können via Javascript ausgelesen werden 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*⁷⁵ ist die Verwendung von Systemfarben als *veraltet* markiert.

WiFi Hotspot Portalerkennung deaktivieren

Firefox erkennt die Portalseiten von WiFi Hotspots und öffnet sie in einem neuen Tab. Für diese WiFi Hotspot Portal Erkennung ruft Firefox beim Start und bei einigen weiteren Ereignissen die Adresse `http://detectportal.firefox.com/success.txt` mit einem XMLHttpRequest ab. Wenn dabei ein Redirect gefunden wird statt der erwarteten Antwort, öffnet Firefox den Hinweis zum notwendigen Login auf einer Portal Seite.

- Wenn man einen Computer im eigenen LAN nutzt, ist die WiFi Portal Erkennung überflüssig. Unter `about:config` kann man sie deaktiviert:

```
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 WiFi Portal Erkennung 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 die URL an:

```
network.captive-portal-service.enabled = true
captiveportal.canonicalURL = http://www...../success.txt
```

Hinweis: die Datei muss via HTTP abrufbar sein, also ohne SSL-Verschlüsselung. Anderenfalls ist kein Redirect möglich.

Connectivity Service deaktivieren

Bei jedem Start und bei einem Wechseln der Netzwerkverbindung kontaktiert Firefox den Server `detectportal.firefox.com` außerdem, um die IPv4 und IPv6 Verbindungen zu testen. Diese Verbindungen kann ohne Nachteile zu erwarten mit folgender Einstellung deaktivieren:

```
network.connectivity-service.enabled = false
```

⁷⁵<https://drafts.csswg.org/css-color-3>

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 herunter zu laden. Dabei werden Informationen zum 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
```

Microsoft Family Safety deaktivieren

Microsoft Family Safety ist ein lokaler man-in-the-middle Proxy in Windows 10, der die Zugriffsrechte auf Webseiten steuern kann und damit per Definition ein Zensurtool ist. Ab Firefox 52 ist die Verwendung von Microsoft Family Safety standardmäßig aktiviert. Mit folgender Option kann man unter `about:config` die Nutzung abschalten:

```
security.family_safety.mode = 0
```

4.21 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 eine WiFi Hotspot anmelden können.
- Einige (vertrauenswürdige) Webdienste funktionieren mit Einstellungen von 1. nicht.
- Bei der heimischen Cloud bzw. Router gibt es keine Trackinggefahr und man möchte Probleme durch restriktive Browserkonfiguration 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
```

(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 Profiles, den man unter `about:profiles` findet und die Option `-no-remote` ermöglicht es, das gewählte Profil unabhängig von einer bereits laufenden Firefoxinstanz zu starten.

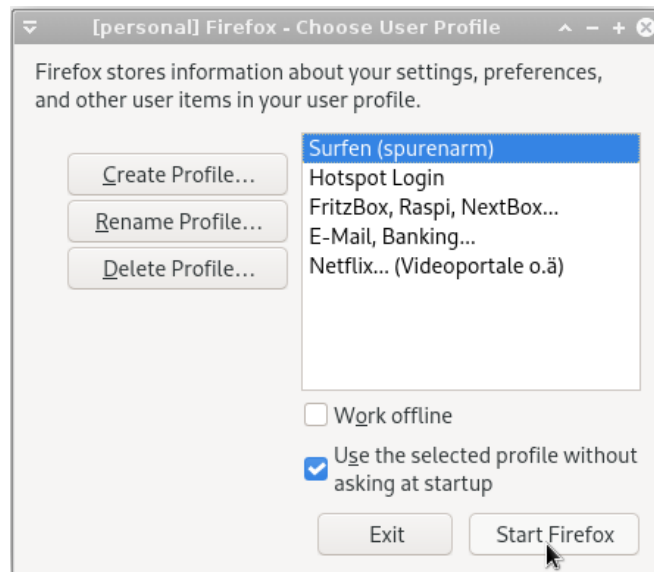


Abbildung 4.29: Firefox Profilmanager

4.22 Zusammenfassung der Einstellungen

Um die Werte nicht alle per Hand anpassen zu müssen, haben wir Beispielkonfigurationen für Firefox 60+ vorbereitet, die man herunter laden 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, dass die Add-ons *uBlock Origin* und *CanvasBlocker* mit den empfohlenen Konfigurationen installiert wurden. Daraus ergeben sich einige Unterschiede zu vergleichbaren Projekten.

Basis Einstellungen: Die *minimale user.js* setzt folgende Einstellungen um:

- 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 sowie Aktivierung der Surfcontainer *FirstParty.Isolate* und *userContext* (Trackingschutz).
- Es wird kein Referrer an Drittseiten und beim Wechsel der Domain gesendet.
- Außerdem werden einige allgm. Sicherheitsfeatures aktiviert (AutoFill für Formulare deaktiviert, Anzeige von unsicheren Verbindungen als Text+Icon...)

Moderate Einstellungen: In der *moderate user.js* werden zusätzlich einige HTML5 Feature deaktiviert, die häufig zum Tracking genutzt werden. Die Funktion normaler Webseiten wird damit in der Regel nur wenig beeinflusst. Auf einigen featurereichen, interaktiven Webseiten kann es allerdings zu Problemen kommen.

- WebGL steht nur mit dem minimalen Featureset zur Verfügung.
- Deaktivierung einiger JavaScript APIs, die für das Fingerprinting des Browsers aber nur selten beim Surfen verwendet werden (Sensors, Gamepad, Media Navigator, WebRTC, Timing APIs...)
- 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.

- Für TLS-Verschlüsselung wird *Unsafe Negotiation* als Fehler gewertet und die Verbindung wird abgebrochen. Auf verschlüsselten HTML-Seiten werden nur Inhalte dargestellt, die über eine verschlüsselte Verbindung geladen wurden. Certificate Pinning wird immer durchgesetzt.

Strenge Einstellungen: Die *strenge user.js* blockiert restriktiv vieles, was für Tracking sowie Sicherheit relevant sein könnte. Neben Trackingschutz sollen auch Möglichkeiten für Angriffe auf den Browser minimiert werden. Diese Einstellungen sind für Risikogruppen geeignet, die für höhere Sicherheit einige Einschränkungen in Kauf nehmen.

- Javascript Just-in-Time-Compiler sind aus Sicherheitsgründen deaktiviert, was die Ausführung von Javascript auf einige Webseiten verlangsamt.
- Anzeige von PDF Dokumenten im Browser und SVG Grafiken sind deaktiviert.
- Auto-Play und Hardware Video Decoding sind deaktiviert.
- Closed Source Video Codecs werden nicht verwendet.
- Favicons werden nicht geladen und nicht gespeichert.
- Es werden keine Login Credentials gespeichert.
- Push Services sind deaktiviert.
- 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 enthält passende Pakete, für Debian/Ubuntu funktioniert:

```
> sudo apt install fonts-font-awesome
```

Hotspot Login: Die *Hotspot user.js* 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, dass 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 die weniger restriktive Variante wählen und die Einstellungen unter *about:config* ergänzen.

4.23 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 privacyfreundliche Add-on. Deshalb gibt es an dieser Stelle ein paar Dinge zusammengestellt, die nicht empfehlenswert sind.

Als Grundsicherung ist die Kombination von *FirstParty.Isolate* + *NoScript* + *uBlock Origin* empfehlenswert. Viele Add-ons bieten Funktionen, die von dieser Kombination bereits abgedeckt werden. Andere sind einfach nur überflüssig.

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, der mit Aktivierung von DNT im Browser zum Ausdruck gebracht wurde, 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, dass 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 preference 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 Jan. 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. Gleichzeitig konnten Lobbyorganisationen erreichen, dass durch Werbung finanzierte journalistische Angebote zukünftig die Daten der Nutzer ohne Zustimmung verarbeiten dürfen. Damit werden die Regelungen der DSGVO ausgehebelt.

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 eine Umsetzung der DNT Spezifikation und Nutzung der Möglichkeiten neue Ansätze für das Fingerprinting des Browsers bieten könnte. Aber *Do-Not-Track* ist bereits 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 folgender Option:

```
privacy.donottrackheader.enabled = false
privacy.trackingprotection.enabled = false
```

Statt der Trackingprotection von Firefox ist uBlock Origin empfehlenswert.

Web of Trust (WOT)

WOT war ein Add-on, das den Surfer über die Reputation der besuchten Webseite informierte und häufig empfohlen wurde. Während des Surfens sammelt WOT Daten über den Besuch jeder Webseite und überträgt 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 zeigten⁷⁶. Die 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.

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.

Die Add-ons *NoScript* zusammen mit einem AdBlocker wie *uBlock Origin* erledigen diese Aufgabe besser.

GoogleSharing

Das Add-on verteilte alle Anfragen an die Google-Suche, Google-Cookies usw. über zentrale Server an zufällig ausgewählte Nutzer von GoogleSharing. Die Ergebnisse werden von den zufällig ausgewählten Nutzern über die zentralen Server zurück an den lokalen Firefox geliefert.

Nach meiner Meinung verbessert man seine Privatsphäre nicht, indem die Daten einem weiteren Dienst zur Verfügung stellt. Dass der eigene Rechner dabei auch unkontrolliert Daten von anderen Nutzern stellvertretend an Google weiterleitet, ist ein unnötiges Risiko. Google speichert diese Informationen und gibt sie bereitwillig an Behörden und als PRISM-Partner auch an Geheimdienste weiter. So kann man unschuldig in Verwicklungen geraten, die man lieber vermeiden möchte.

Statt GoogleSharing sollte man lieber datenschutzfreundliche Alternativen nutzen: die Suchmaschine *Ixquick.com* oder *Startingpage.com*, für E-Mails einen Provider nutzen, der den Inhalt der Nachrichten nicht indexiert, *openstreetmap.org* statt Google-Maps verwenden. . .

Zweite Verteidigungslinie?

Eine Reihe von Add-ons bieten Funktionen, welche durch die oben genannte Kombination bereits abgedeckt werden:

- *FlashBlock* blockiert Flash-Animationen. Das erledigt auch *NoScript*.
- *ForceHTTPS* kann für bestimmte Webseiten die Nutzung von HTTPS erzwingen, auch diese Funktion bietet *NoScript*.
- *Targeted Advertising Cookie Opt-Out* und *Ghostery* blockieren Surftracker. Es werden nur Tracker blockiert, die der oben genannten Kombination auch bekannt sind.
- *No FB Tracking* blockiert die Facebook Like Buttons, das können *uBlock Origin* oder *AdBlock* aber besser. Die *SocialMediaBlock Listen* für diese Werbeblocker blockieren nicht nur Facebook Like Buttons, sondern auch die Wanzen von anderen Social Networks.
-

Wer meint, es nutzen zu müssen - Ok.

⁷⁶<https://www.tagesschau.de/inland/tracker-online-103.html>

4.24 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 Informationen 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 JonDonym⁷⁷ entlarvt viele Fehler:

HTTP Header: Die einzelnen Browser sind durch individuelle Headerzeilen und -reihenfolge 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-Override* (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.

| | |
|------------|--|
| Signatur | 8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox) |
| User-Agent | Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0) |

Das Add-on *Random-Agent-Spoof* (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.

| | |
|------------|--|
| Signatur | 8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox) |
| User-Agent | Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36 |

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 Betriebssystem ermittelt werden:

⁷⁷<http://ip-check.info>

```
User-Agent via HTTP Header: Mozilla/5.0 (Windows NT 10.0; Win64; x64....
Browsertyp via JavaScript: Mozilla/5.0 (X11) 20100101/...
```

Das gleiche gilt auch für TorBrowser unter Linux, wenn man bei einem Firefox für Linux die Option *privacy.resistFingerprinting* aktiviert oder *general.useragent.override* verwendet, um ein anderes Betriebssystem vorzutäuschen. Via Javascript kann man diese Fakes recht einfach entlarven.

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 19px für Linux, 19.5167px für MacOS und 19.2px oder 20px für Windows.

Seltsamkeiten: Der Browser hängt in viele Dingen von Bibliotheken des Betriebssystems ab. Durch Auswertung einige Seltsamkeiten lässt sich das real verwendete Betriebssystem teilweise identifizieren oder zumindest ein User-Agent Fake entlarven. Ein Beispiel OS-spezifische Seltsamkeiten ist das Ergebnis der folgenden Berechnung:

```
Math.tan(-1e300) = -4.987183803371025 (Windows)
Math.tan(-1e300) = -1.4214488238747245 (Linux, iOS)
```

Plug-ins: verraten in der Regel das verwendete Betriebssystem und können dafür keinen Fake konfigurieren.

Schlussfolgerung

Es ist nahezu unmöglich, die User-Agent Kennung von Firefox plausibel in allen Punkten zu faken. Selbst die Entwickler des TorBrowserBundles, die jahrelange Erfahrungen dabei haben und für alle für Nutzer des Anonymisierungsdienstes den einheitlichen Fingerprint eines englischen Firefox ESR für Windows anstreben, können nicht vollständig verhindern, dass Linux oder MacOS Nutzer erkannt werden können.

Ein unvollständiger Fake-Versuch ist aber ein gutes Identifizierungsmerkmal für Trackingdienste, da man sich von der großen Masse der Surfer stärker unterscheidet.

Eine kleine Ausnahme für Linuxer

Viele Linux Distributionen bauen einen Firefox, der in der User-Agent Kennung des Browser den Namen der Linux Distribution mit einfügt.

```
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0
Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0
```

Hier könnte man einen generischen Firefox für Linux vortäuschen, um die überflüssige Information der genutzten Linux Distribution aus der Kennung zu entfernen, indem man unter der Adresse *about:config* die Variable *general.useragent.override* neu anlegt und folgenden Wert einträgt:

```
Mozilla/5.0 (X11; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0
```

Bei jedem Update des Browsers ist die Kennung an die aktuelle Version anzupassen.

Mit dem Add-on CanvasBlocker kann man die Kennung für einen generischen Linux Firefox faken, die sich automatisch an die aktuelle Version anpasst. Dafür ist in den Einstellungen vom Add-on CanvasBlocker auf dem Reiter APIs der Schutz der Navigator-API zu aktivieren und Einstellungen für das Faken der User-Agent Kennung gemäß Abb. 4.30 zu konfigurieren (Linux + Firefox anklicken und den Rest übernehmen).

Betriebssystemvoreinstellungen

Windows Linux Mac OS X

Browservoreinstellungen

Edge Opera Chrome Safari Firefox

Navigatorwerte

| | | |
|-----------------|------------------------|-------------------|
| browserPreset | Firefox | Firefox |
| firefoxVersion | {real Firefox version} | 97.0 |
| osPreset | Linux | Linux |
| platformDetails | X11; Linux x86_64 | X11; Linux x86_64 |
| windowManager | X11 | X11 |

Abbildung 4.30: CanvasBlocker: User-Agent Fake für Linux

Kapitel 5

Spurenarm Surfen mit Librewolf

Librewolf ist ein Firefox Klon mit privacyfreundlichen 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.

Telemetrie, Firefox Sync und weitere Features wurden entfernt. Der Captive Portal Check wurde ebenfalls entfernt, so dass man Librewolf nicht für Logins bei WiFi Hotspots nutzen kann. Für WiFi Hotspot Login benötigt man zus. einen anderen Browser.

Das Librewolf sinnvoll vorkonfiguriert ist, espart man sich bei Nutzung des Librewolf für spurenarmes Surfen die Spielerei und Updates einer user.js Konfiguration oder Anpassungen der einzelnen Werte unter *about:config* per Hand.

5.0.1 Installation

Auf der Librewolf Webseite¹ ist die Installation für für verschiedene System beschrieben:

- Für populäre Linux Distributionen (Debian, Ubuntu, Fedora, Arch, Gentoo) gibt es Repositories, so dass man Librewolf mit dem bevorzugten Paketmanager installieren und regelmäßig aktualisieren kann.
- Für Windows Nutzer gibt es ein Install Paket aber noch keinen offiziellen Updater. Updates werden also nicht automatisch installiert. Man muss bei Updates die neue Version installieren. Um über Updates benachrichtigt zu werden, kann man das Add-on Librewolf Updater² installieren.

Es gibt eine portable Version³ vom Librewolf inklusive Updater⁴ bei Github.

Außerdem kann Librewolf unter Windows mit verschiedenen Paketmanagern installiert werden Chocolatey, Winget, Scoop). Es gibt ein breites Ökosystem rund um Librewolf für Windows.

- MacOS Nutzer könne Librewolf mit *brew* installieren oder als Disc Image.

5.0.2 Anpassungen der Konfiguration

1. **uBlock Origin** ist bereits standardmäßig enthalten. Man kann die vorbereitete Konfiguration vom PrHdb Team herunterladen und importieren.⁵

¹<https://librewolf.net>

²<https://addons.mozilla.org/en-US/firefox/addon/librewolf-updater/>

³<https://github.com/ltGuillaume/LibreWolf-Portable>

⁴<https://github.com/ltGuillaume/LibreWolf-WinUpdater>

⁵https://www.privacy-handbuch.de/handbuch_21d2.htm

2. Zum Schutz gegen Javascript Fingerprinting ist *ResistFingerprinting* standardmäßig aktiviert, das TorProject.org für den TorBrowser entwickelt. Damit wird ein User-Agent Fake als Firefox ESR (Win10) aktiviert, was für den TorBrowser sinnvoll ist:

Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0

Im Librewolf ist dieser Fake leicht erkennbar, wie der Test CreepJS zeigt (Abb: 5.1). Ein Firefox 98 (Linux), der sich als Firefox ESR (Win10) tarnen will, ist aber sehr sehr selten und somit leicht zu verfolgen.



Abbildung 5.1: Von CreepJS ermittelte User-Agent Kennung für Librewolf

Die Aktivierung von *ResistFingerprinting* ist hier kontraproduktiv und sollte deshalb in den Einstellungen auf dem Reiter *Librefox* deaktiviert werden.



Abbildung 5.2: ResistFingerprinting in den Einstellungen vom Librewolf deaktivieren

Statt *ResistFingerprinting* kann man die Add-ons **CanvasBlocker** und **JShelter** installieren und die vorbereiteten Konfigurationen importieren, wie es auch für Firefox als Schutz gegen Javascript ingerprinting empfohlen wird.

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* durch das generische Maskulin. Wer sich einmal an das Add-on gewöhnt hat, möchte es nicht mehr vermissen.
5. Als Suchmaschine ist DuckDuckGo vorinstalliert. Weitere Suchmaschinen kann wie für Firefox beschrieben nachinstallieren und als Standardsuche setzen.

Kapitel 6

Passwörter und 2-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. 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 Loginversuch wird anhand von Merkmalen ein Risikolevel berechnet, ob möglicherweise ein missbräuchlicher Login erfolgt. Übersteigt der Risikolevel einen Grenzwert, wird eine zusätzliche Verifikation gefordert. In der Regel muss der Nutzer ein zusätzliches Token einzugeben, 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 2-Faktor-Authentifizierung, da sie im Normalfall nur das Passwort eingeben müssen. 2-Faktor-Auth. wird in der Regel nur bei hohen Sicherheitsanforderungen akzeptiert.

RBA ist bei vielen großen Plattformen (Google, Amazon, PayPal, LinkedIn...) und auch bei Projekt 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 2-Faktor-Auth. verwendet, wird RBA meist deaktiviert.

RBA wird häufig *ein Art 2-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 zwischen:

- *Harter Besitz* ist ein physisch vorhandenes, individuell konfiguriertes *Token*, welches nicht kopierbar ist (Yubikey, U2F-Stick, ePA, NitroKey...)
- *Weicher Besitz* ist eine Anhäufung speziell konfigurierter Bits und Bytes, die evtl. auf einem anderen Gerät gespeichert sind 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 gegen Mitleser unter den Bedingungen der Videoüberwachung. Es schützt nicht(!) bei Einbrüchen auf dem Server. Da bei OTP-Server und Client den gleichen Algorithmus ausführen, könnte ein Angreifer bei erfolgreichem Einbruch auf dem Server die Parameter auslesen und clonen.

Die modernere Variante ist U2F 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 U2F nur von wenigen Anbietern und bisher nur vom Browser Google Chrome 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 Sperrbildschirm via Fingerabdruck Scan. In diesem Fall würde ich die Verwendung des Fingerabdruck 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.

6.1 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 einen Zettel "speichern".

Was ist ein starkes Passwort

Diese Frage muss man unter Beachtung des aktuellen Stand der Technik beantworten. Wörterbuchangriffe sind ein alter Hut. Das Passwort darf kein Wort aus einem Wörterbuch wie z. B. dem Duden sein, das ist 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 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, 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 mind. 65 Bit Entropie nötig.

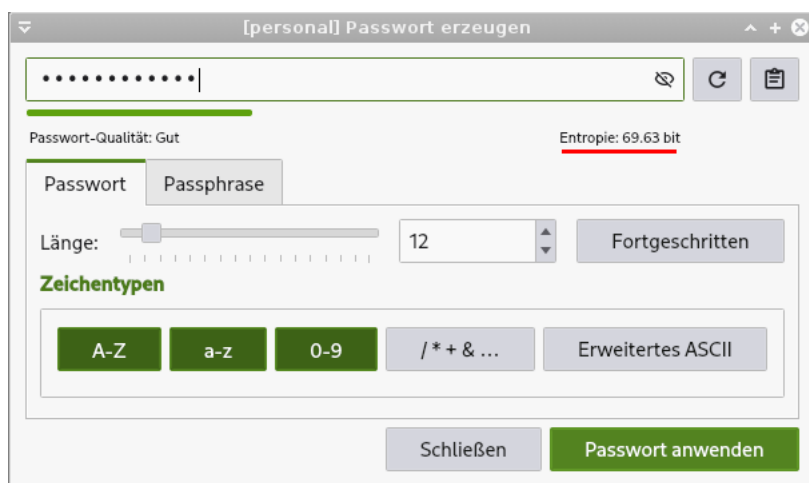


Abbildung 6.1: KeepassXC Passwortgenerator

Passwortspeicher sind die einzig 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 verwendet die Anfangsbuchstaben der Wörter von einem leicht merkbaren Satz ableiten 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 verwendet statt zufälliger Zeichenkombinationen. Wortkombinationen kann man sich leichter merken als sinnlose Zeichenkombinationen.

Für den klassischen Weg zur Erstellung einer Diceware Passphrase benötigt man eine Wortliste (beispw. die *DeReKo Liste*¹ mit den häufigsten deutschen Wörtern laut Leibniz Institut) und einen Würfel. Für jedes Wort würfelt man 5x und erhält damit eine Zahlenkombination. Diese Zahlenkombination 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

Nicht ein Passwort 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... Die veröffentlichten 60.000 E-Mails waren peinlich für HBGary.³
- Im Sommer 2018 kursierten mehrere tausend Logindaten (Benutzername, Passwort) für den Dienst MEGA in den einschlägigen Darknet Foren. Die Login Credential 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.

6.1.1 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.

Wenn man in der Konfiguration ein Masterpasswort 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 Usernamen wird dann als nicht löschbare, eindeutige Tracking-ID genutzt.

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>

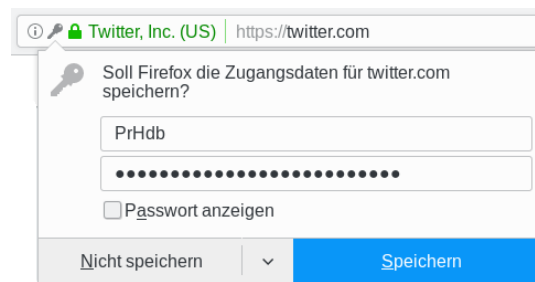


Abbildung 6.2: Login Credentials für eine Webseite in Firefox speichern

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 Masterpasswort gesichert werden. Das schützt die Passwörter, der Angreifer erhält aber trotzdem die Informationen, welche Accounts das Opfer auf welchen Webseiten nutzt.

Anpassungen Firefox Konfiguration

- Wer kompromisslos auf strenge Privatsphäre Wert legt, kann den Passwortspeicher von Firefox deaktivieren und memorisierbare Passwörter verwenden oder externe Passwortspeicher wie KeePassXC. Zur Deaktivierung des Passwortspeichers setzt man unter *about:config* folgenden Wert:

```
signon.rememberSignons = false
```

- Wer es lieber etwas moderater bevorzugt und den built-in Passwortspeicher verwenden möchte, kann 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 Passwort übernehmen.

```
signon.rememberSignons = true
signon.autofillForms = false
```

6.1.2 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:

- 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.

⁴<https://freedom-to-tinker.com/2017/12/27/no-boundaries-for-user-identities-web-trackers-exploit-browser-login-managers/>

- 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 Bezahl-dienstleistern.
- In der Regel enthalten Passwortspeicher eine Passwortgenerator, der wirklich zufällige und starke Passwörter generieren kann.
- Das Backup wird deutlich vereinfacht. Man muss nur die verschlüsselte Datenbank auf ein externes Backupmedium kopieren.
- Im Gegensatz zum Firefox Build-in Speicher werden alle Informationen verschlüsselt gespeichert, nicht nur die Passwörter.

Mir gefallen **KeePassX2** (für ältere Linux Distributionen) oder **KeePassXC** (Windows, MacOS, Ubuntu 18.04+, Fedora 28+) sehr gut. KeePassXC ist eine Weiterentwicklung der Community, für die es auch das Add-on *KeePassXC-Browser*⁵ zur Integration in Firefox gibt. Bei Verwendung dieses Add-on entfallen die Risiken bei der Übergabe von Passwörter via Zwischenablage (siehe unten). Die Konfiguration für das Add-on ist in der Dokumentation von KeePassXC beschrieben.⁶

Um kryptoanalytische Angriffe zu erschweren, wird die gesamte Passwortdatenbank mehrere 10.000x mit AES256 verschlüsselt.

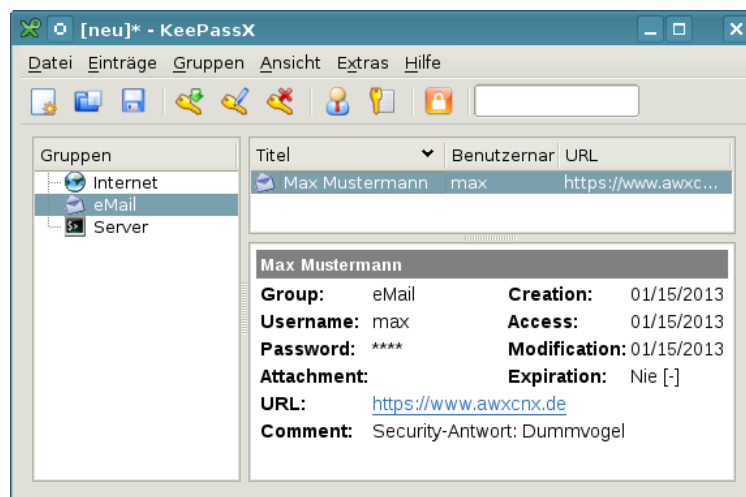


Abbildung 6.3: KeePassX Hauptfenster

Einige Passwortspeicher werben mit der Möglichkeit, die Datenbank zwischen verschiedenen Rechnern und Smartphones zu synchronisieren. Dabei wird die Datenbank *in der Cloud* gespeichert. Das ist für mich ein Graus, vor allem, weil der geheimdienstliche Zugriff auf Daten *in der Cloud* immer mehr vereinfacht wird.

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 Festplatte.

- Klipper (KDE Desktop) speichert die Daten in `$HOME/.kde/share/apps/klipper/history2.lst`

⁵<https://addons.mozilla.org/de/firefox/addon/keepassxc-browser>

⁶<https://keepassxc.org/docs/keepassxc-browser-migration>

- 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.

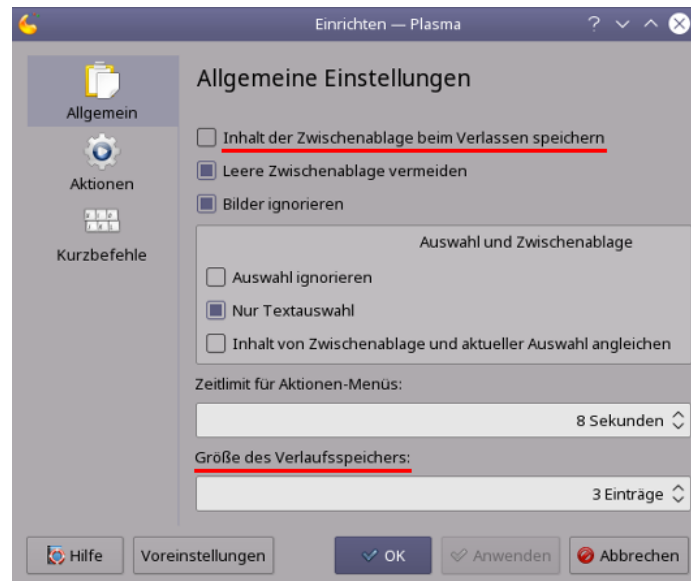


Abbildung 6.4: Konfiguration der KDE Zwischenablage Klipper

Als Beispiel zeigt Bild 6.4 die Konfiguration für die KDE Zwischenablage Klipper und Bild 6.5 zeigt, wie man den automatischen Start der Verwaltung der Zwischenablage Clipman in den XFCE Einstellungen für Sitzung und Startverhalten deaktiviert.

6.2 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. Internet verwendet man statt Chipkarte meist One-Time-Passwort Generatoren oder SecuritySticks (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.

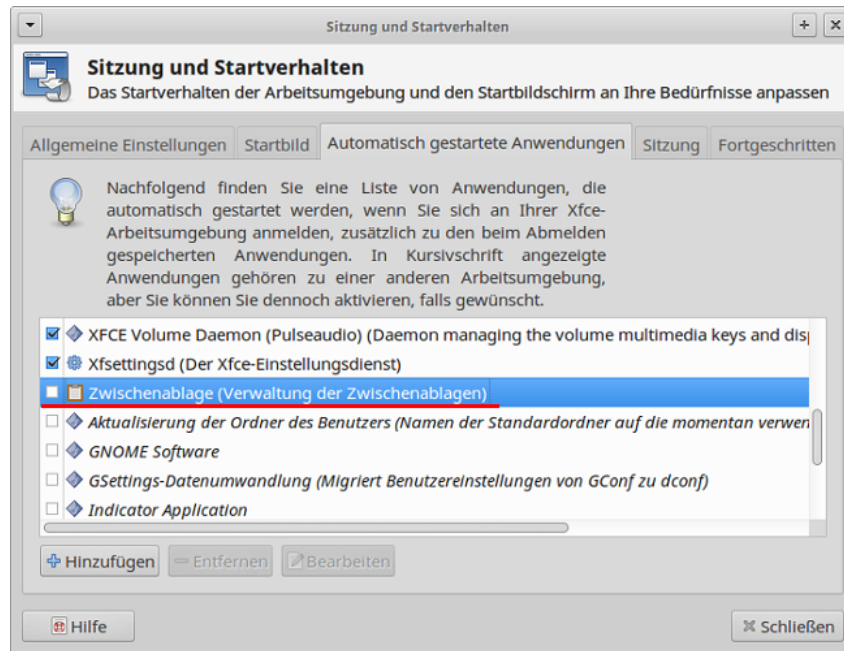


Abbildung 6.5: Starten von Clipman deaktivieren (XFCE Desktop)

2-Faktor-Authentifizierung für das Online Banking

Mit der europäischen Zahlungsrichtlinie PSD2 wird für die Online-Abwicklung von Bankgeschäften die 2-Faktor-Auth. auch für den Login bei Webseiten zur Zahlungsabwicklung zwingend vorgeschrieben. Banken haben unterschiedliche Lösungen entwickelt, die sich von den üblichen Lösungen für 2-Faktor-Auth. bei anderen Webdiensten unterscheiden. Banken verwenden in der Regel einen TAN-Generator als 2. Faktor und definieren den Geschäftsfall *Login*, da die Technik für 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 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 bei 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 2-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. Der erste Teil ist üblicherweise ein 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-Auth. 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 kurze 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 30sec bzw. 60 sec Zeit.

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. 2018 haben potente Hacker begonnen, 2-Faktor-Auth mit OTP in größerem Umfang auszutricksen.

Angriffe auf 2-Faktor-Auth. mit OTP Token:

- Die Sicherheitsfirma CERTFA berichtete Dez. 2018 in dem Blogartikel von einer Spear-Phishing Kampagne iranischer Hacker gegen Google und Yahoo! Accounts, welche die 2-Faktor Auth. austricksen konnte.⁷
- Amnesty International berichtete ebenfalls von einer Phishing Angriffswelle aus Nahost gegen die Accounts von Aktivisten, welche die 2-Faktor-Auth von ProtonMail, Tutanota, Google und Yahoo! austricksen konnte.⁸
- Im Januar 2019 wurde auf Github die Software Muraena und NecroBrowser⁹ als Open Source veröffentlicht, die Phishing Angriffe auf 2-Faktor-Auth mit OTP automatisiert ausführen kann. Der Angreifer lockt das Opfer mit Phishing E-Mails o.ä. zum Login auf seine Webseite. Dort arbeitet Muraena als Reverse-Proxy, der sich unbemerkt zwischen Nutzer und Webdienst einschleicht und die Authentifizierung an den richtigen Server weiterleitet. Nachdem die Session aufgebaut wurde, extrahiert Muraena die Session Cookies oder Session-IDs und reicht sie an eine Instanz des NecroBrowsers weiter. Das Schließen der Session (Logout) wird von Muraena blockiert und dem Nutzer wird vorgegaukelt, er hätte sich abgemeldet. Danach kann der Angreifer mit dem NecroBrowser 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.

⁷<https://blog.certfa.com/posts/the-return-of-the-charming-kitten/>

⁸<https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/>

⁹<https://github.com/muraenateam>

1. Die abgeschorchelten Token schreibt man zusammen mit den 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 ?1?1?1?1?1?1
```
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 5min 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 Client den gleichen Algorithmus zur Berechnung und Verifizierung des One-Time-Passworts ausführen, kann ein Angreifer bei einem erfolgreichem 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 2-Faktor-Auth mit OTP nicht beim Zugriff staatlicher Behörden auf Passwort Hashes, wie es in dem Feb. 2020 von der Regierung beschlossenen *Gesetzes zur Bekämpfung von Rechtsterrorismus und Hasskriminalität*¹⁰ vorgesehen ist. Und das schließt die Parameter zur Berechnung der OTP ein. Gegen diesen Angriff ist ausschließlich die Stärke des ersten Faktors (Passwort) relevant und das Hashverfahren, welches der Provider zum Schutz des gespeicherten Passwortes einsetzt.

- **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 genutzt werden kann und auch als U2F SecurityStick.

Der Webdienst, bei dem man sich anmeldet, sendet das Einmalpasswort in der Regel 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.

FIDO-U2F: ist ein kryptografisches Privat/Public Key Verfahren zur Authentifizierung mit einem kleinen SecurityStick (z. B. *Nitrokey U2F*¹¹ oder verschiedene *Yubikeys*¹²), das im Okt. 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. Diese Signatur wird als Response an den Server zurück geschickt 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:

¹⁰<https://www.golem.de/news/hasskriminalitaet-regierung-will-passwortverschlüsselung-nicht-aushebeln-2002-146727.html>

¹¹<https://www.nitrokey.com/de>

¹²<https://www.yubico.com/products/yubikey-hardware/>

1. Da asymmetrische Kryptografie genutzt wird, kennt der Server nur einen public Key. Wenn ein Angreifer den Server kompromittiert, kann er die U2F Auth. 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 Auth. 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.

Auf der Testseite von Yubico¹³ kann man ein bisschen und prüfen, ob man mit U2F einen Account erstellen den U2F-Stick für einen Dummy Login nutzen kann.

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 / Passwort Kombinationen komplett ersetzen können.

Das Protokoll nutzt asymmetrische Kryptografie ähnlich wie FIDO-U2F und verwendet gleichfalls Security Token. Es können FIDO2 USB-Sticks verwendet werden oder das Trusted Platform Module des Computers (TPM), um die privaten Keys zu speichern. Außerdem ist WebAuthn kompatibel mit FIDO-U2F. Für Testzwecke kann man auch mal Soft-Token nutzen.

WebAuthn/FIDO2 erweitert FIDO-U2F um folgende Punkte:

1. Die User-ID (Username) wird ebenfalls auf dem Security Token gespeichert und beim Login automatisch an den Server gesendet. Der Username muss damit nicht mehr in einem Login Formular eingegeben werden.
2. Außerdem ist der Zugriff auf das Security Token mit einer PIN bzw. Passwort zu sichern. Damit wird der erste Faktor der Authentifizierung (Wissen) lokal beim Nutzer überprüft und muss nicht mehr durch den Server validiert werden.

Auf der Webseite <https://WebAuthn.io> kann man spielerisch mit seinem Token einen Account erstellen und sich mit dem Umgang beim Login vertraut machen.

Hinweis für Linuxer: Wenn FIDO2 oder U2F Sticks nicht out-of-the-box funktionieren, muss man die UDEV Regeln installieren. Meistens reicht es, folgende Pakete zu installieren:

```
Ubuntu: > sudo apt install libu2f-udev  
Fedora: > sudo dnf install u2f-hidraw-policy
```

SMS: SMS-basierte Verfahren zur Authentifizierung gelten als nicht mehr sicher. Es gibt mehrere Publikationen zu dem Thema. Das NIST, BSI u.a. empfehlen, SMS nicht mehr für die Authentifizierung zu nutzen.¹⁴

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 2-Faktor-Auth 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 2016 und dem erheblichen Einfluss 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 Benutzernamen/Passwort-Verfahren nicht mehr gegeben. Im Rahmen Cyber-Sicherheitsstrategien will die Regierung die Bürger stärker zur Nutzung der Onlineausweisfunktion des Personalausweises animieren.

¹³<https://demo.yubico.com/u2f>

¹⁴<https://pages.nist.gov/800-63-3/sp800-63b.html>

Bezüglich des klassischen Benutzername/Passwort-Verfahren stimmen wir mit der Bundesregierung überein. Wir empfehlen aber die Onlineausweisfunktion des ePerso nicht. Statt dessen sollte man Hardware Token nutzen, die nicht an eine ID-Karte gebunden und vollständig durch den Nutzer konfigurierbar sind.

6.3 Phishing Angriffe

Phishing ist eine der Plagen im Internet. Der Lagebericht des BSI zur IT-Sicherheit 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 Kontakt Netzwerk zu analysieren und die Kommunikation zu beobachten. Mit diesem Hintergrund wurden die Twitter Accounts von Erdogan-Kritikern von türkischen Hackern angegriffen.¹⁵
- 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 Zahlung auf andere Konten umzuleiten. B. Schneier beschreibt in seinem Blog ein Beispiel für einen erfolgreichen *CEO-Hack* gegen eine Galerie.¹⁶

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.

- 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...*

¹⁵<https://netzpolitik.org/2017/angriffe-gegen-twitter-accounts-von-erdogan-kritikern>

¹⁶https://www.schneier.com/blog/archives/2017/11/cybercriminals_.html

- *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.



Abbildung 6.6: Beispiel für eine Phishing Mail

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 auszurufen. 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 2-Faktor-Authentifizierung nutzen, wenn der Webdienst es unterstützt. Das erschwert einfache, primitive Phishing Angriffe. (Es gibt allerdings technisch ausgefeiltere Angriffe, die auch die 2-Faktor-Auth. mit OTP aushebeln können.)

Wenn man diese Regeln beherzigt, ist man gegen Phishing gut geschützt.

Kapitel 7

Bezahlen im Netz

PayPal.com ist zweifellos der bekannteste Bezahl Dienstleister im Internet. Die Firma wurde von Peter Thiel gegründet, der u.a. den Datensammler Rapleaf.com aufgebaut hat, als einer der Hauptinvestoren die Entwicklung von Facebook maßgeblich mitbestimmt hat und zum Steering Committee der Bilderberg Konferenzen gehört. Das Credo von P. Thiel ist eine totale Personalisierung des Internet.

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 an mehr als 100 Firmen übertragen zum Monitoring der Überweisung.

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 gesperrt¹, 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 Bezahl-dienst zu kündigen.

Zukünftig möchte PayPal.com auch in der realen Welt präsent sein. Das Bezahlungssystem soll die Geldbörse in zwei Jahren 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 privacy-freundliche Bezahlungsmethoden, da nur die beiden Kreditinstitute von Käufer und Verkäufer in den Bezahlprozess eingebunden sind. Außerdem sind es sichere Bezahlungsmethoden, 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 Processoren übernommen. Teilweise sammeln diese Payment Processoren Daten über online und offline Einkäufe und verkaufen die Daten an große Datensammler wie Acxiom oder Blue-Kai, wo sie mit anderen persönlichen Daten zusammengeführt werden.

Die Kreditkartenfirma Mastercard demonstriert mit einem Patent (Dez. 2016), wie man sich die Monetarisierung des gesammelten Datenreichtums vorstellen könnte.

¹<http://heise.de/-1320630>

In dem Patent wird beschrieben, wie die Kreditkartenfirmen aus den Einkäufen anhand der Konfektions- und die 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-Kontraktor 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 erstmal 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 verschiedene Kreditkarten Online und Offline nutzt.

Disposable Virtual Cards werden von besonders innovativen Kreditinstitute angeboten. Bei diesen Kreditkarten ändert 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 privacy-freundlicher aber nicht anonym.

Google Pay und **Amazon Pay** sind aus technischer Sicht ebenfalls Payment Processoren für Kreditkarten. In der Google Datensch(m)utz Policy wird benannt, welche Daten dabei Nutzung dieser Bezahlmethode gesammelt werden:

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. Bei dem 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.

²<https://www.golem.de/news/datenleck-daten-von-millionen-hotelgaesten-ungeschuetzt-im-netz-2011-152005.html>

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, 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 es in einem Urteil klar formuliert, das 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 weiter geleitet. 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, kleinere Guthaben bei Bedarf zu kaufen. Das verhindert auch eine technisch mögliche Verkettung mehrerer Einkäufe über den gleichen Gutscheincode.

Nach praktischen Erfahrungen von sind die Verkäufer im Supermarkt, Tankstellen u.ä. nicht immer über die angebotene Möglichkeit des Verkaufes von Paysafecard Gutscheinen informiert. Hartnäckig bleiben und die Verkäuferin auf das Paysafecard Symbol im GUI der Kasse hinweisen hilft.

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 Sept. 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.

7.1 Anonyme Online-Zahlungen vor dem Aus?

Die Bundesregierung bereitete unter dem Deckmantel des Kampfes gegen Geldwäsche ein Gesetz vor, das für anonyme Bezahlungen im Internet das Aus bedeutet hätte. Künftig sollen Verkaufsstellen von Paysafecards und UKash Vouchers die Käufer identifizieren und die Daten für eine mögliche Prüfung 5 Jahre bereithalten. Im Gegensatz zu Bareinzahlungen, die statt bisher ab 15.000 Euro zukünftig ab 1.000 Euro berichtspflichtig werden, sollten für E-Geld keine Mindestgrenzen gelten.³

Nach Ansicht von Udo Müller (Paysafecard-Geschäftsführer) wären diese Anforderungen auch für die Vertriebsstruktur das AUS. 95% der Partner wie Tankstellen, Geschäfte usw. würden unter diesen Bedingungen den Verkauf von Paysafecard Gutscheinen und UKash Vouches einstellen.

Unklar ist, wie die bei E-Geld üblichen Kleinbeträge in nennenswertem Umfang für Geldwäsche genutzt werden können. Die Regierung hat dafür keine sinnvolle Erklärung geliefert. Nach den vom BKA vorgelegten Zahlen zum Missbrauch von Prepaidkarten zur Geldwäsche ist der Missbrauch sehr gering. Nur in 94 von 14.000 Verdachtsfällen, die gemeldet wurden, spielten Prepaidkarten eine Rolle. Das sind 0,7% aller Verdachtsfälle. Der Bundesdatenschutzbeauftragte Schaar hat sich gegen den Entwurf ausgesprochen:

Ich appelliere an den Gesetzgeber, den überzogenen Ansatz der neuen Vorschläge entsprechend zu korrigieren.

Die 82. Konferenz der Datenschutzbeauftragten Ende September 2011 verfasste zu diesem Gesetzentwurf eine Stellungnahme:

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts.

Am 01. Dez. 2011 hat der Deutsche Bundestag das Gesetz in einer etwas entschärften Version beschlossen. Für den Kauf von Prepaidkarten bis 100 Euro ist keine Identifizierung der Käufer nötig. Für Prepaidguthaben von mehr als 100 Euro sind die Käufer zu identifizieren. Die Daten sind 5 Jahre lang zu speichern. Der Bundesdatenschutzbeauftragte kommentierte die Verabschiedung des Gesetzes u.a. mit folgenden Worten:

So begrüßenswert es ist, dass der anonyme Erwerb von E-Geld damit nicht generell abgeschafft wird, so kritisch sehe ich die nach wie vor bestehende Tendenz, individuelles Handeln in immer stärkerem Maße zu registrieren. . .

Die Diskussion über Identifikationspflichten - vor allem bei der Inanspruchnahme des Internets - ist damit aber sicherlich noch nicht beendet.

³<http://heise.de/-1269409>

Der EU-Rat hat im Dez. 2016 in den *Verhandlungspositionen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung*⁴ die Gangart deutlich verschärft und fordert die **Aufhebung der Anonymität von virtuellen Währungen** wie Bitcoin u.ä. Die Umtausch-Plattformen für virtuelle Währungen und Anbieter elektronischer Geldbörsen müssen zukünftig gemäß den Richtlinien für Banken die Identität ihrer Kunden verifizieren. Die Umsetzung in nationale Gesetze soll 2017 in allen EU-Ländern erfolgen.

7.2 Bargeld

Man kann im Internet nicht mit Bargeld bezahlen, trotzdem soll es kurz erwähnt werden, weil das anonyme Bezahlen mit Bargeld schrittweise immer weiter eingeschränkt wird. Angesichts der ungebremsten Schuldenentwicklung und 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 wird 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 wird die dänische Notenbank ab 2016 keine Geldscheine mehr drucken.

Der Wirtschaftsweisenrat Bofinger und der US-Ökonom Rogoff haben im Mai 2015 nachdrücklich die Abschaffung des Bargelds gefordert. Sie appellierten an Bundeskanzlerin Merkel, dass Sie sich auf dem G7-Gipfel in Elmau für eine weltweite Abschaffung des Bargelds einsetzen soll. Dafür wurden folgende Gründe genannt:⁵, 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 ihre eigentliche Funktion zurück zu führen.

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.

⁴<http://www.consilium.europa.eu/de/press/press-releases/2016/12/20-money-laundering-and-terrorist-financing/>

⁵<http://www.manager-magazin.de/finanzen/artikel/bofinger-und-rogooff-fordern-abschaffung-des-bargelds-a-1034135.html>

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.⁶

Noch etwas deutlicher:

Es geht dem ehemaligen Chefökonom des Internationalen Währungsfonds (IWF) und dem IWF längst neben einer umfassenden Kontrolle der Bevölkerung auch darum, die Grundlage für die finanzielle Repression zu schaffen, um die ausufernde Verschuldung über die Enteignung der Sparer zu lösen.⁷

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. 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 Januar 2016 wurde ein Plan der Bundesregierung bekannt, europaweit die Obergrenze für Barzahlungen auf max. 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.
- Außerdem fordert W. Schäuble zentrale Bankkontenregister in allen Mitgliedsstaaten der EU und die bessere Kontrolle von anonymen Prepaid-Zahlungsmittel und Kryptowährungen wie Bitcoin und Ripple zur *Terrorbekämpfung*.

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 als 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 Kofferchen 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 Kofferchen übergeben, dass 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 Grenze für Barzahlungen aber nicht wirklich verhindern können.

⁶<http://bitcoinblog.de/2015/05/18/bargeld-ist-macht>

⁷<http://www.heise.de/tp/artikel/45/45089/1.html>

- Die Steuerfahndung hat in Deutschland aber ganz andere Probleme. Der Fall Zumwinkel ist schönes Beispiel. Der Steuerfahnder wurde von seinen Vorgesetzten ausdrücklich angewiesen, den Fall Zumwinkel nicht weiter zu verfolgen. 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: 978-3-86883-105-4) von Frank Wehrheim und Michael Gösele nachlesen. Die Probleme liegen jedenfalls nicht in der Verfügbarkeit von Bargeld.

7.3 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*. Die Software löst mit kryptografischen Methoden vor allem zwei Probleme:

1. Das Kopieren und mehrfache Verwendung der Bits und Bytes, die ein 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 man 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 30-60min, 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 Dez. 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.⁸

Transaktionsgebühren von 15 US-Dollar sind inzwischen normal. Damit liegen die Gebühren deutlich über den Kosten anderer Zahlungsmittel.

⁸<https://www.heise.de/ct/ausgabe/2018-3-Allzeit-Hoch-bei-Kurs-und-Gebuehren-Taugt-Bitcoin-noch-als-Zahlungsmittel-3942392.html>

- Die Sicherheit vieler Bitcoin Markplätze liegt deutlich unter dem Niveau anderer Bezahlendienste und Banken. Prominentestes Beispiel ist die Insolvenz von MtGox nachdem Bitcoins im Wert von 368,4 Millionen Euro verloren gingen. Möglicherweise handelte es sich dabei um einen Betrug der Betreiber. Die Betreiber der Bitcoin Börse MyCoin sind ebenfalls in betrügerischer Absicht mit den Einlagen der Kunden verschunden und haben Bitcoins im Wert von 342 Mio. Euro mitgenommen.

Weitere Beispiele sind die Börsen Flexcoin oder Poloniex oder die südkoreanische Bitcoin Börse Yobit, die alle nach virtuellem Bankraub geschlossen wurden.

Die Bitcoins nur lokal in einem Wallet auf dem eigenen Rechner zu speichern ist auch nicht immer sicherer. So konnte im Jan 2018 ein Angreifer mit ein bisschen Javascript Code in einer Webseite aus dem Browser heraus die Wallets von Electrum leerräumen.⁹

- Der Wettkampf der Bitcoinminer beim Schürfen neuer Coins ist völlig außer Kontrolle geraten und ist ein sinnloser Einsatz von immer mehr Rechenleistung, um sich gegenseitig zu übertrumpfen. Es ist nur noch eine gewaltige Energieverschwendung. Die Webseite Bitcoin Energy Consumption Index¹⁰ schätzte den Energieverbrauch im Nov. 2017 auf 30 Terrawattstunden pro Jahr (Energieverbrauch von Irland: 25 TWh, Marokko: 29 TWh oder Dänemark: 34 TWh jährlich). Ende Januar 2018 wurde der Energieverbrauch von Bitcoin auf 40 Terrawattstunden pro Jahr geschätzt, Tendenz weiter steigend. Wenn die Tendenz weiter anhält, könnte Bitcoin noch vor Ende des Jahres 2020 den Energieverbrauch der USA übertreffen ohne irgendeinen Nutzwert zu liefern außer Umverteilung von Geld durch Spekulation.

Auch wenn man die absoluten Zahlen zur Berechnung des Bitcoin Energy Consumption Index von Enthusiasten der Kryptowährung in Frage gestellt werden und man meint, es wären eher 10 TWh statt 30 TWh jährlich, kann man nicht leugnen, das Bitcoin Energie in gigantischem Ausmaß verbrennt für nichts.¹¹

Schlussfolgerung: die real existierende Menschheit ist noch nicht in der Lage, mit einer Technologie wie Bitcoin umzugehen.

⁹<https://www.heise.de/ct/ausgabe/2018-3-Bitcoin-3942380.html>

¹⁰<https://digiconomist.net/bitcoin-energy-consumption>

¹¹<https://bitcoinblog.de/2017/11/27/bitcoin-verbraucht-mehr-strom-als-159-laender-wirklich>

Kapitel 8

E-Mail Kommunikation

E-Mail ist eines der meistgenutzten Kommunikationsmittel. Die folgenden Seiten sollen zum Nachdenken über die Auswahl des E-Mail Providers anregen und Hinweise für die Konfiguration von Mozilla Thunderbird geben.

8.1 E-Mail Provider

Als erstes braucht man eine oder mehrere E-Mail Adressen. 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 sehr privaten E-Mail Adresse für Freunde könnte man weitere E-Mail Adressen für Einkäufe im Internet nutzen oder für politische Aktivitäten. Um nicht ständig viele E-Mail Accounts abfragen zu müssen, kann man die für Einkäufe im Internet genutzten E-Mail Accounts auch an die private Hauptadresse weiterleiten lassen. Alle Mail-Provider bieten diese Option. Bei den großen deutschen Mail Providern GMX.de und WEB.de gibt es bis zu 100 Fun-Domains extra für diesen Zweck. Bereits mit der kostenlosen Version kann man bis zu 3 Fun-Adressen nutzen.

Wenn eine E-Mail Adresse nur für die Anmeldung in einem Forum oder das Veröffentlichen eines Kommentars in Blogs benötigt wird, kann man *temporäre Mailadressen* nutzen.

Eine kleine Liste von empfehlenswerten E-Mail Providern:

- **Mailbox.org** ¹ (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, PGP verschlüsselte Inbox, verschlüsselter Mailversand und -empfang nur über SSL/TLS aktivierbar, DANE, IP-Adressen der Nutzer und User-Agent werden aus dem Mail Header entfernt, anonyme Accounts möglich, Bezahlung per Brief oder Bitcoin, OTP-Login mit HW-Token und FreeOTP für Webinterface, Tor Hidden Service für POP3, IMAP, SMTP und XMPP)
- **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, außerdem unfreundliche Reaktion auf Kritik ³)

¹<https://mailbox.org>

²<https://posteo.de>

³<https://www.privacy-handbuch.de/diskussion.htm#take-down-notiz-von-posteos-anwaelten>

- **Mailfence.com**⁴ (belgischer Provider, kostenlose Accounts möglich, Premium ab 2,50 Euro pro Monat allerdings mit mehr Speicherplatz als die 1,- Euro Accounts der Mitbewerber, POP3, IMAP und SMTP nur für bezahlte Accounts, OpenPGP im Webinterface möglich mit eigener Implementierung, OTP-Login mit FreeOTP für Webinterface, anonyme Bezahlung via Bitcoin oder ohne Anonymität via Kreditkarte)
- **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)
- **runbox.com**⁶ (privacy-engagierter norwegischer E-Mail Provider, Server stehen ebenfalls in Norwegen, Accounts ab 1,66 Dollar pro Monat)
- **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, dass kostenfreie, spendenfinanzierte E-Mail Dienste (wie SecureMail.biz, Xalia u.a.) nur für ein paar Jahre verfügbar sind und dann eingestellt werden könnten.)

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 zuviele 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 EmailPrivacyTest⁷ zeigt, dass Web.de und GMX.de bei der Nutzung des Web-GUI nicht gegen Tracking Elemente in E-Mails schützen und ermöglichen es damit vielen Diensten, 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 zuviel 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 Attachements
 3. Betreffzeilen aller E-Mails (nicht verschlüsselbar)
 4. URLs aus dem Text unverschlüsselter E-Mails
 5. ... and any other information that we deem necessary

⁴<https://mailfence.com>

⁵<https://kolabnow.com>

⁶<https://secure.runbox.com>

⁷<https://www.emailprivacytester.com>

Diese Daten werden bei der Kündigung eines Account 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 Drittseiten ein. Die ID des Hushmail Account 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 beschneffeln. Dabei ist es unerheblich, ob der Cloud- bzw. 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.⁹

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...

- Weitere Beispiele werden auf der Webseite des Handbuches genannt.¹⁰

8.2 ProtonMail und Tutanota

Die E-Mail Dienste ProtonMail (Schweiz) und Tutanota (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 erfolgt primär im Webinterface mit einem Webbrowser. Einen E-Mail Client wie Thunderbird kann man nur über Umwege verwenden. Das ermöglicht die Realisierung einer einfach nutzbaren E-Mail Verschlüsselung.

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 euch 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.
- 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.

⁸<http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050>

⁹<https://netzpolitik.org/2017/datenschuetzer-raetseln-schafft-trump-datenschutz-abkommen-zwischen-usa-und-eu-ab/>

¹⁰https://www.privacy-handbuch.de/handbuch_31.htm

- 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 ProtonMail möglich. Dafür muss man die ProtonMail 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 ProtonMail Server.
- Die SSL/TLS-Verschlüsselung für die Webseiten wird vom Qualys 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 ProtonMail 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 Model bei ProtonMail 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 ProtonMail.

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 kompromittiert¹¹. 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.com¹² ausführlich dargelegt.

¹¹<http://www.wired.com/2007/11/encrypted-e-mai>

¹²http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/

Tutanota und ProtonMail 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 *ProtonMail Bridge* als Mail-Gateway installieren oder die Software von Tutanota 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?

- ProtonMail 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.¹³
- 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 Account könnte sich Zugriff auf die Daten verschaffen, aber die Administratoren von Tutanota haben keine konzeptuelle Backdoor für den Zugriff auf die Daten.¹⁴

Somit gibt es bei beiden Services keine konzeptuelle Backdoor.

8.3 Mozilla Thunderbird

Alle E-Mail Provider bieten die Möglichkeit, die E-Mail Kommunikation im Webinterface mit einem Browser zu verwalten, aber trotzdem 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, das 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 Projektes¹⁵ für Windows, Linux und MacOS zur Verfügung. Linux Distributionen enthalten Thunderbird. Mit der Paketverwaltung kann Thunderbird und die deutsche Lokalisierung installiert werden.

¹³<https://protonmail.com/support/knowledge-base/resetting-mailbox-password>

¹⁴<https://tutanota.uservoice.com/knowledgebase/articles/470716-was-passiert-wenn-ich-mein-passwort-vergesse-k%C3%B6nnte>

¹⁵<https://www.mozilla.org/de/thunderbird/>

Da Thunderbird den gleichen Code wie Firefox verwendet, wäre es möglich, dass der Downloads in gleicher Weise mit einer individuellen Kennung für die Telemetrie markiert werden wie Firefox. Windows und MacOS Nutzer können es vermeiden, indem man Thunderbird aus dem FTP Archiv¹⁶ herunterlädt. (Linuxer, die die Repositories der Distribution zur Installation verwenden, sind nicht betroffen.)

8.3.1 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 Account sollten einige Punkte beachtet werden.

Die Grafik im Bild 8.1 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.

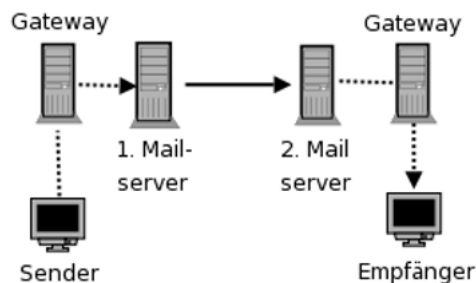


Abbildung 8.1: Der Weg einer E-Mail durch das Web

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 abrufen 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.

Diese Abkürzungen SMTP oder POP3 und IMAP sind für Laien erstmal 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 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 herunter zu laden. Auch die versendeten E-Mails und die E-Mail Entwürfe werden bei der Nutzung von IMAP auf dem Mailserver des Providers gespeichert.

¹⁶<https://ftp.mozilla.org/pub/thunderbird/releases/>

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 erkaufte 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 ¹⁷.

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 erlauben, diese Daten abzurufen. Es wäre u.U. unschön, wenn man dort die gesamte Kommunikation der letzten 15 Jahre vorfindet.

Kompromiss: ist möglich, um mit mehreren Geräten (PC zuhause, Smartphone unterwegs...) 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 ¹⁸.

Alle brauchbaren Mail-Server bieten 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 unverschlüsselt übertragen.

Es werden keine Daten über eine unverschlüsselte Verbindung gesendet und der Server muss sich zuerst authentifizieren, bevor der Client irgendwelche Daten sendet.

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
```

¹⁷<https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-079.html>

¹⁸<http://tim.geekheim.de/2007/04/24/netzwerksicherheit-auf-der-republica/>

```
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 aktivieren¹⁹. 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 8314²⁰ 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.

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.

8.3.2 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 Mail-server (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

¹⁹<https://heise.de/-206233>

²⁰<https://tools.ietf.org/html/rfc8314>

enthält Thunderbird keine Konfigurationsdateien für die E-Mail Provider. Wir haben eine zusammengestellt: man kann sich das Archiv `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, versucht der Assistent danach 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 Parameter 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, ist aber meiner Meinung nach keine gute Idee bei normaler Nutzung des E-Mail Account, da die Autokonfiguration die Erstellung des E-Mail Account 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 das auch 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
```

8.3.3 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*²¹ 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: 8.2). Das erleichtert auch die Erkennung von Phishing E-Mails.

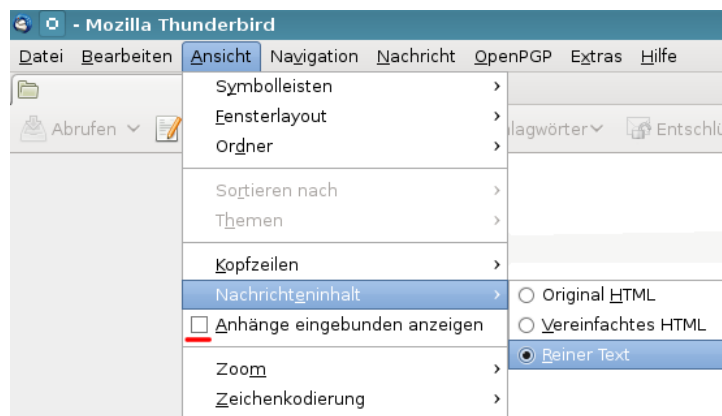


Abbildung 8.2: E-Mails als reinen Text darstellen

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:

```
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 beispw. 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 Thunderbird Add-on **Allow HTML Temp**²² vereinfacht die Umschaltung für das Lesen einer E-Mail, indem es einen Button für die HTML Ansicht über der E-Mail einblendet und beim Wechsel zu einer anderen Mail automatisch wieder auf die Textansicht zurück schaltet.

Nach der Installation kann man in den Einstellungen des Add-ons anpassen, welches die Standardansicht ist und welche Ansicht temporär mit einem Klick aktiviert

²¹<https://emailprivacytester.com>

²²<https://addons.thunderbird.net/de/thunderbird/addon/allow-html-temp>

werden soll. Standardmäßig wechselt man nach der Installation mit einem Klick von der Darstellung als reiner Text auf Original HTML. Es reicht aber in der Regel das vereinfachte HTML (Abb: 8.3).

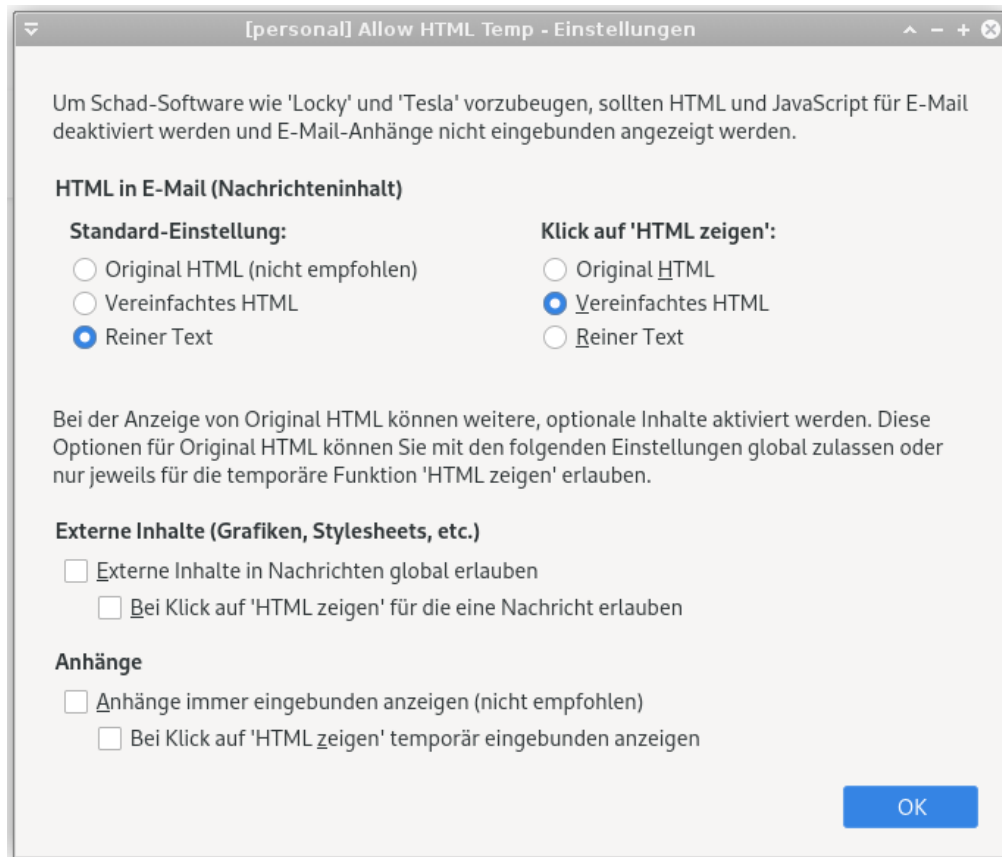
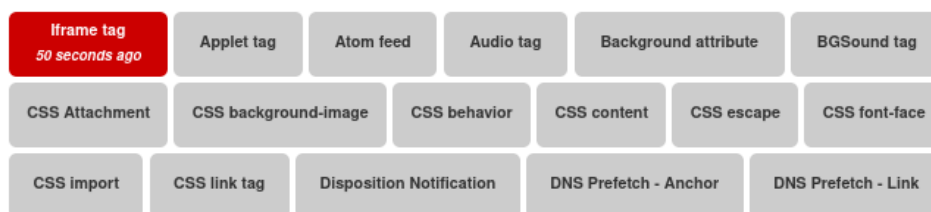


Abbildung 8.3: Einstellungen für das Add-on Allow-HTML-Temp

- In der Ansicht *Original HTML* blockiert Thunderbird 91 nicht alle für das Tracking geeignete HTML Elemente zuverlässig, wie der E-Mail Privacy Test zeigt:



- Außerdem können folgende Features in den *Erweiterten Einstellungen* deaktiviert werden, die jedoch nur für die Darstellung von HTML E-Mails in der Ansicht *Original HTML* relevant sind oder für andere Komponenten, die den HTML-Viewer nutzen:

```

javascript.enabled           = false
network.cookie.cookieBehavior = 2
beacon.enabled               = false
layout.css.visited_links_enabled = false
media.hardware-video-decoding.enabled = false
media.navigator.enabled      = false
media.video_stats.enabled    = false

```

```
gfx.downloadable_fonts.enabled      = false
network.IDN_show_punycode          = true
network.http.sendRefererHeader      = 0
security.family_safety.mode         = 0
```

Da JavaScript generell deaktiviert wird, muss man im Gegensatz zu Firefox die Geolocation, DOMStorage, IndexedDB, AudioContext-API, Timing-APIs, Gamepad-API ... usw. nicht einzeln abschalten.

8.3.4 Sichere Konfiguration als E-Mail Client

Einige Hinweise für die sichere Nutzung des Mediums E-Mail mit Mozilla Thunderbird:

- Gespeicherte Passwörter für den Zugriff auf SMTP-, POP- oder IMAP-Server müssen mit einem **Masterpasswort** geschützt werden.
- 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
```

- 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 Wanzeln genutzt werden. Einen deartigen 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 Link 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.

- 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 in den *Erweiterten Einstellungen* eine neue String Variable anlegen und einen Fake definieren:

```
mail.smtpserver.default.hello_argument = [127.0.0.1]
```

Privacy-freundliche 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 Empfänger Adressen eingibt.

Wenn man die E-Mail Adressen der Empfänger nicht automatisiert speichern möchte, dann kann man das kann man das Feature in den Einstellungen in der Sektion *Verfassen* 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.

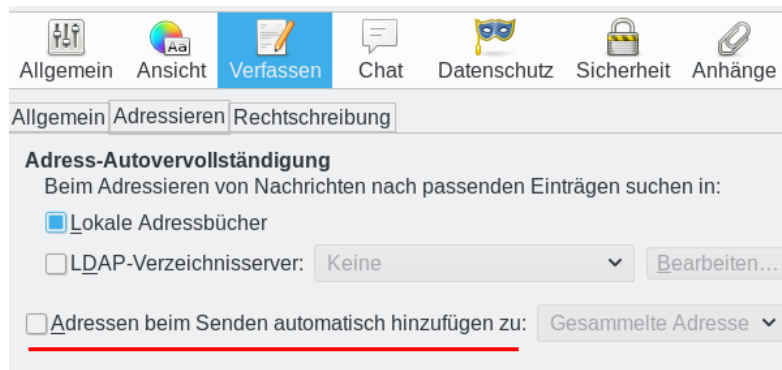


Abbildung 8.4: Sammeln von E-Mail Adressen abschalten

- 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 achtsamer Umgang mit seltsamen Anhängen, regelmäßige Updates des Systems besser als Virens Scanner oder Block-Listen.

```
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 = 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 den 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 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
```

8.3.5 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 Internet wird diese Verschlüsselung ständig weiterentwickelt und an neue, moderne Erkenntnisse der Kryptografie angepasst. Gleichzeitig werden 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 Suites als uneingeschränkt sicher eingestuft werden. Gemäß IETF RFC 7525 und BSI TR-03116-4 nur folgende Ciphersuiten 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 Ciphersuiten mit CHACHA20-POLY1305 von D.J. Bernstein können ebenfalls als sicher eingestuft werden. Bei DHE-Ciphersuiten 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 und TLS 1.1 gelten als unsicher und sollten nicht mehr verwendet werden. Leider sind diese TLS Versionen nicht bei allen E-Mail Providern abgeschaltet, aber Thunderbird 78.x verwendet diese veralteten Protokolle nicht mehr.

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_Ortt_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 grotteschlechte 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.

Außerdem kann es Probleme beim Abrufen von einigen RSS Feeds geben, wenn der Webserver, der den Feed bereit stellt, 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 Suites des TLS 1.2 Standard deaktivieren. Folgende Einstellungen sind in diesem Fall empfehlenswert:

```
security.tls.version.min = 3 (default ab Thunderbird 78.x)

security.ssl3.dhe_rsa_aes_128_sha      = false
security.ssl3.dhe_rsa_aes_256_sha      = false
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
```

Weiterer Einstellungen für die TLS Verschlüsselung

- Insecure Renegotiation 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 Certificate 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 verbietet::

```
security.mixed_content.upgrade_display_content = true
dom.security.https_only_mode                  = true
```

Verbindungsprobleme mit sicheren TLS-Einstellungen

Wenn man die im Bild [8.5](#) 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.

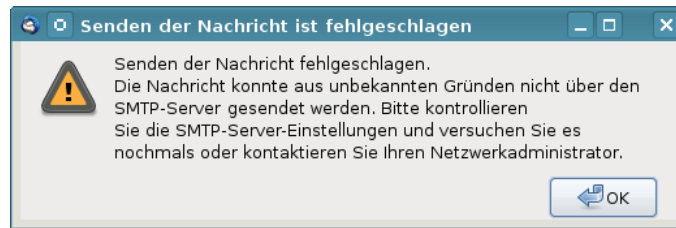


Abbildung 8.5: Fehlermeldung bei unsicherer Verbindung

8.3.6 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 zu klicken und der 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`.

8.3.7 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 Sprachvariationen in einem Paket zusammen:

```
> sudo dnf install hunspell-de
```

- Für andere Betriebssysteme kann man fehlende Wörterbücher von der Webseite für Language Tools²³ herunterladen. Nach dem Download der Wörterbücher

²³<https://addons.mozilla.org/de/thunderbird/language-tools/>

ist Thunderbird als zu starten. Der Menüpunkt *Extras* -> *Add-ons* öffnet den Dialog für die Verwaltung. Wenn man oben rechts auf das kleine Werkzeugsymbol klickt (Bild 8.6, kann man die Dateien mit den Wörterbüchern als Add-on installieren.

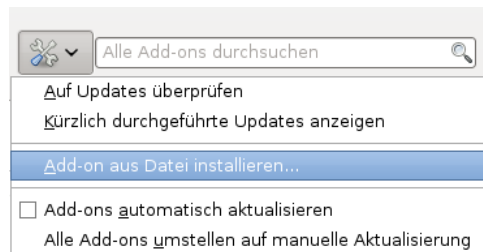


Abbildung 8.6: Wörterbücher in der Add-on Verwaltung installieren

Danach kann man in den Einstellungen von Thunderbird die Rechtschreibprüfung aktivieren und die bevorzugte Sprache auswählen. Die Auswahl der Sprache kann man beim Schreiben einer Mail jederzeit ändern.

8.3.8 Spam-Filter aktivieren

Das Mozilla Team bezeichnet nicht erwünschte E-Mails (Spam) als Junk. Den integrierten lernfähigen Filter kann man in Account Einstellungen unter *Junk-Filter* aktivieren, wenn der E-Mail Provider keinen guten Spam-Filter einsetzt.

(Ich nutze lieber einen guten E-Mail Provider und brauche daher diesen Spam-Filter seit längerer Zeit nicht mehr.)

8.3.9 Spam vermeiden

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.

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.

E-Mail Aliases nutzen

Jeder brauchbare E-Mail Provider bietet die Möglichkeit, Aliases für einen E-Mail Account anzulegen. Man kann im Webinterface in den Konfigurationseinstellungen einen oder mehrere Aliases für den Account erstellen, diese Adressen für die Kommunikation mit bestimmten Zweck (z.B für Hotel Reservierung oder Flug Buchung) für eine begrenzte Zeit nutzen und dann löschen. Konkrete Anleitungen findet man in den FAQ oder der Online Hilfe des Mail Providers.

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 Anbiters kontaktieren muss. Mit temporären Adressen kann man in der Regel nur Nachrichten empfangen.

- E-Mail Aliases werden nicht gesperrt. In vielen Diskussionsforen (z.B. bei Zeit.de) 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 in der Regel 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 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 Adresse 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 ²⁴ kann ein E-Mail Account für den Empfang von einer Nachricht erstellt werden. Der Account ist bis 24:00 Uhr des folgenden Tages gültig (24-48h) 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 nochmal nachschauen möchte.

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 als Datei speichern, wie in Bild 8.7 gezeigt. Die Datei ist mit der Endung **.eml** zu speichern und kann dann in einem E-Mail Client wie z.B. Mozilla Thunderbird geöffnet werden (Bild 8.8).

Sicherheit unterliegt bei der AnonBox.net starken Schwankungen:

- Die SSL-Konfiguration des Webservers von AnonBox.net war früher mal auf dem aktuellen Stand der Technik mit Forward Secrecy und starken DH-Parametern und ist jetzt (Sept. 2018) katastrophal.
- Die TLS-Verschlüsselung des Mailservers hatte ich vor einiger Zeit schon einmal kritisiert, wurde danach auf den aktuellen Stand gebracht und ist jetzt (Sept. 2018) wieder kaputt.

²⁴<https://anonbox.net>

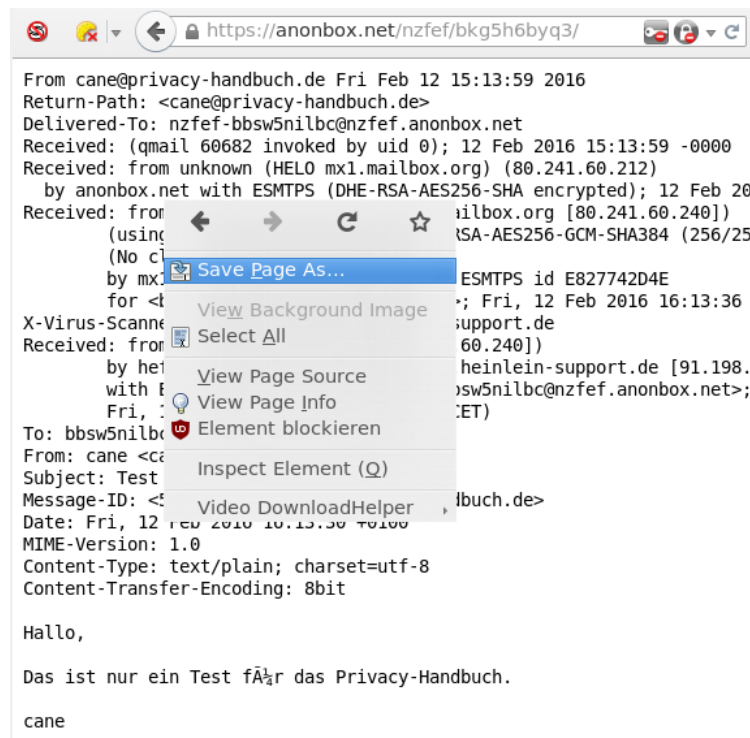


Abbildung 8.7: E-Mail im Web-GUI der AnonBox.net als Datei speichern

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 Account genutzt wurde, könnte ein Angreifer problemlos die Passwort Recovery Funktion nutzen!

Nachrichten werden nach 6-12h automatisch gelöscht. Man muss also regelmäßig den Posteingang prüfen, wenn man eine Wegwerf-Adresse nutzt.

Liste einiger Anbieter (unvollständig):

- <https://discard.email> (SSL-Verschlüsselung für Webserver aber nicht für Mailserver, Passwortschutz, E-Mail schreiben möglich, Session-Cookies und JavaScript erforderlich)
- <https://www.trash-mail.com> (HTTPS, Cookies und JavaScript freigeben, Schreiben von E-Mails möglich)
- <https://www.guerrillamail.com> (HTTPS, Cookies und JavaScript freigeben, Schreiben von E-Mails möglich)
- <http://crapmail.dk> (Antwort schreiben möglich, Cookies freigeben)

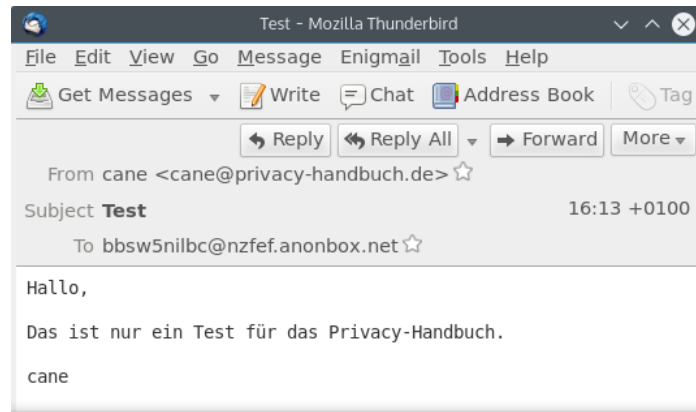


Abbildung 8.8: E-Mail aus AnonBox.net in Thunderbird geöffnet

- <http://vsimcard.com/trashmails.php> (bietet auch Wegwerf-SMS Nummern)
- <http://www.7mail7.com> (Cookies und JavaScript freigeben, RSS-Feed für Inbox)
- <http://www.mailcatch.com> (keine Cookies oder JavaScript nötig, E-Mails können gelöscht werden)
- <http://www.mailinator.com/> (JavaScript nötig freigeben, E-Mails können gelöscht werden)

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 Anonymisierungsdienste.

Temporäre Adressen

Im Gegensatz zu Wegwerf-E-Mail-Adressen muss man eine temporäre E-Mail Adresse zuerst auf der Webseiten des Anbieter erstellen, die dann für 10min bis zu mehreren Stunden gültig ist. Erst danach kann diese 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. Session-Cookies sind für diese Website freizugeben, mit JavaScript sind die Webseiten oft besser bedienbar. Nachdem man eine neue temporäre 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 Mailadresse und wartet auf die eingehende Bestätigungsmail. In der Regel enthält diese Mail einen Link zur Verifikation. Auf den Link klicken - fertig. Wenn der Browser-Tab mit der temporäre E-Mail Adresse geschlossen wurde, hat man keine Möglichkeit mehr, ankommende Mails für diese Adresse zu lesen.

Die folgenden Anbieter erlauben nur zufällig erstellter 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:

- <https://temp-mail.ru> (2h, HTTPS, Cookies und JavaScript freigeben, russisches GUI)
- www.10minutemail.com (10min gültig, verlängerbar)

- <http://www.10minutemail.com/> (10min gültig, verlängerbar, Cookies und JavaScript freigeben)
- <http://tmpeml.info> (60min gültig, Cookies freigeben)
- <http://disposable.pingfu.net> (60min gültig, JavaScript freigeben)
- <http://getairmail.com> (24h gültig, Cookies und JavaScript freigeben)

Bei den folgenden Anbieter kann man neben zufällig generierten E-Mail Adressen auch selbst definierte E-Mail Adresse nutzen. Man kann damit einen bestimmten E-Mail Account mehrfach verwenden. Das ist für einige Anwendungsfälle ein Vorteil, manchmal eher ein Nachteil:

- <http://www.tempmailer.de> (60min gültig, Session-Cookies freigeben)
- <http://www.squizzly.de> (60min gültig, Session-Cookies freigeben)
- <http://dontmail.net> (24h, Cookies und JavaScript freigeben)
- <http://www.migmail.net> (24h, Cookies und JavaScript freigeben)

8.3.10 RSS-Feeds

RSS-Feeds bieten die Möglichkeiten, sich schnell über Neuigkeiten in häufig gelesenen Blogs zu informieren ohne die Webseiten einzeln abklappen 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....*



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 sollen und ob die RSS-Feeds 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 im Bild 8.9 dargestellt.

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, verringert aber man 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).

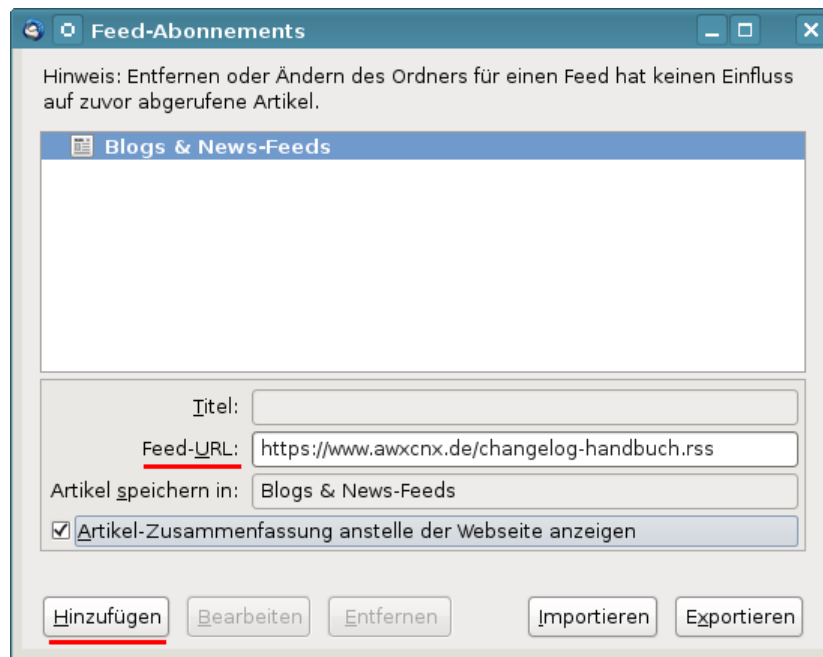


Abbildung 8.9: RSS-Feed hinzufügen

```

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
```

8.3.11 Filelink

Seit Version 13.0 bietet Thunderbird die Möglichkeit, große Dateianhänge bei einem Filehoster hochzuladen und dem Empfänger nur den Link zum Download per E-Mail zu senden. Aktuelle Thunderbird Versionen nutzen dafür den Filehoster *Box.com*²⁵ standardmäßig. Weitere Dienste wie OwnCloud, DropBox, FileRun oder WebDAV Speicher können via Add-ons genutzt werden. Eine Liste findet man im Support Bereich von Mozilla²⁶.

Ich kann dieses Feature nicht empfehlen.

1. Filelink ist nicht in die E-Mail Verschlüsselung integriert. Auch wenn man eine verschlüsselte E-Mail schreibt, werden die Uploads unverschlüsselt auf dem Server abgelegt. Man muss sich selbst um die Verschlüsselung der Dateien kümmern und könnte sie dann gleich zu einem 1-Click-Hoster hochladen.
2. Die bei einem Cloud-Service gespeicherten Dateianhänge unterliegen nicht dem besonderen Schutz des Post- und Fernmeldegeheimnisses.
3. Der standardmäßig unterstützte Dienst *Box.com* erfordert die Registrierung eines Accounts. Aufgrund der euphemistisch als Datenschutzerklärung²⁷ bezeichneten

²⁵<https://www.box.com>

²⁶<https://support.mozilla.org/de/kb/filelink-fuer-grosse-dateianhaenge>

²⁷<https://www.box.com/de-de/legal/privacypolicy>

Auflistung der Datensammeltechniken kann man von diesem Dienst nur abraten.

Es werden neben Cookies auch moderne Tracking Techniken wie HTML5 EverCookies eingesetzt. Do-Not-Track Header werden ausdrücklich ignoriert. Dabei wird nicht nur der Absender von Dateianhängen getrackt, sondern auch der Empfänger, der damit möglicherweise nicht einverstanden ist.

In Thunderbird 78.x kann man FileLink mit folgender Option komplett abschalten:

```
mail.cloud_files.enabled = false
```

8.4 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 Monitoringprogramme 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*²⁸ der Firma *insophia* nutzen. Man schreibt die Nachricht auf der Webseite des Anbieters und klickt auf den Button *Create Note*. JavaScript muss dafür frMan 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 dieses Passwort dann nutzen, bis man ein neues Passwort austauscht. Das Passwort könnte man 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, das ist Bullshit.

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 nur EINMALIG lesbar. Darauf sollte man den Empfänger hinweisen. Wenn der Empfänger die Nachricht nicht abgerufen, wird sie nach 30 Tagen gelöscht.

Man kann den Link NICHT über irgendwelche Kanäle in Social Networks (z.B. Facebook) versenden. Wenn man 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

²⁸<https://privnote.com>

The screenshot shows the 'privnote' web interface. At the top, a red banner contains the 'privnote' logo and the text 'Send notes that will self-destruct after being read.' Below this, the 'New note' section features a yellow text area with the placeholder text 'Hallo Du, das ist eine private Nachricht...'. To the right of the text area is a question mark icon. Below the text area, the 'Note self-destructs' section has a dropdown menu set to 'after reading it' and a checked checkbox for 'Do not ask for confirmation before showing and destroying the note. (Privnote Classic behaviour)'. The 'Manual password' section includes two password input fields; the first has a green 'Good' feedback message below it. The 'Destruction notification' section has two optional input fields for an email and a reference name. A tip at the bottom reads: 'Tip: bookmark the page now so you don't have to input these advanced options again.' At the bottom right, there are two buttons: a red 'Create note' button and a grey 'Disable options' button.

privnote Send notes that will self-destruct after being read.

New note ?

Hallo Du, das ist eine private Nachricht...

Note self-destructs

after reading it ☐ Do not ask for confirmation before showing and destroying the note. (Privnote Classic behaviour).

Manual password

Enter a custom password to encrypt the note

Confirm password

Good

Destruction notification

E-mail to notify when note is destroyed

Reference name for the note (optional)

Tip: bookmark the page now so you don't have to input these advanced options again.

Create note **Disable options**

Abbildung 8.10: Eine Private Note schreiben

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 geeignet für geheime oder streng vertrauliche Informationen.

Kapitel 9

E-Mails verschlüsseln

Weltweit wird der unverschlüsselte E-Mail Verkehr systematisch gescannt. Führend ist die NSA mit *Echelon*, das auch zur Industriespionage sowie zum Abhören von NGOs verwendet wird, und Abhörschnittstellen bei allen großen amerikanischen ISPs. 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 abgeschnorcelten Datenmengen. Für Saudi Arabien, Syrien, Iran, Tunesien und Ägypten wurden entsprechende Aktivitäten nachgewiesen und die *Great Firewall* von China verfügt ebenfalls 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 unterschiedliche Schlüssel 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 die 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, Software selbst konfigurieren muss, sich selbst die notwendigen Schlüssel erstellen muss oder beglaubigen lassen muss, sich um die Verteilung der Schlüssel selbst kümmern muss 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. Es wurden bei Sicherheit und Flexibilität teilweise erhebliche Einschränkungen in Kauf genommen, ohne dabei das Ziel einer nennenswert größeren Verbreitung von OpenPGP zu erreichen.

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 wurden 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

¹<https://autocrypt.org>

die E-Mail Provider per Definition als vertrauenswürdig deklariert und damit das wesentlich Ziele einer Ende-zu-Ende Verschlüsselung über Board geworfen. Der Schutz gegen den E-Mail Provider war und ist 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 die Nutzung von OpenPGP für sicherheitskritische Anwendungen (beispielsweise Whistleblower) kaputt gemacht hat.

In der Entwickler Community sind die Ansichten gespalten. Bei dem Mailvelope Browser Add-on wurde Autocrypt implementiert und standardmäßig aktiviert. Die Thunderbird Entwickler haben diesen Schlüsseltausch nicht implementiert.

Mit **contermitm**² gibt es eine Erweiterung für den Autocrypt Schlüsseltausch, die eine Verifizierung von Schlüsseln einführt und ein *Network of Trust*, um bei Autocrypt mögliche Man-in-the-Middle Angriffe für verifizierte Schlüsseln zu verhindern. *contermitm* gehört nicht zum Autocrypt Standard und wird unabhängig davon entwickelt.

9.1 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 Client 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.

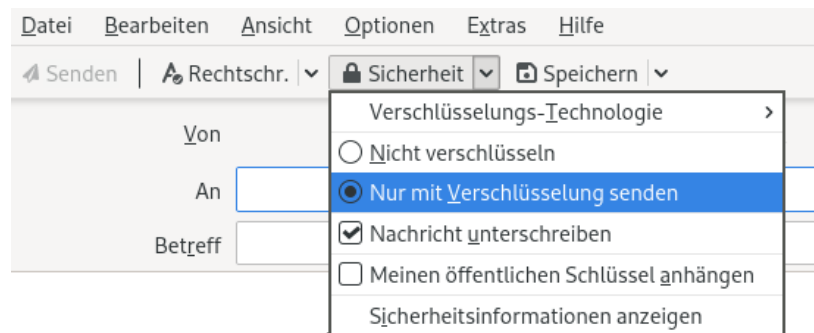
Schlüssel erstellen: Um die Verschlüsselung von E-Mails zu aktivieren, muss man in den Kontoeinstellungen in der Sektion *Ende-zu-Ende Verschlüsselung* einen PGP-Schlüsselpaar generieren oder importieren oder ein S/MIME Zertifikat importieren.

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.
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.

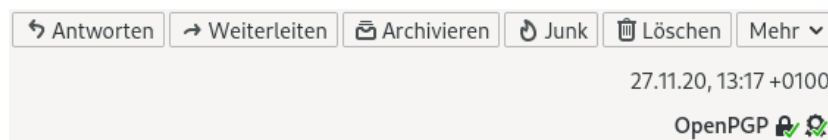
E-Mails schreiben: Wenn man die Hürden beim Austausch der Schlüssel überwunden hat, kann man beim Schreiben die Verschlüsselung mit zwei Klicks aktivieren:

²<https://contermitm.readthedocs.io/en/latest/index.html>



Leider bietet Thunderbird (noch) keine Möglichkeit, Präferenzen zur Verschlüsselung für bestimmte Empfänger zu definieren. Man muss vor dem Versenden einer E-Mail kurz innehalten und über die Verschlüsselungsoptionen nachdenken.

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.

9.1.1 Eigenen OpenPGP Schlüssel erstellen oder importieren

Um OpenPGP zu aktivieren, muss man in der Verwaltung des E-Mail Account unter *Ende-zu-Ende Verschlüsselung* einen Schlüsselpaar für OpenPGP erzeugen oder importieren.

Wenn man ein neues Schlüsselpaars erstellt, gibt es nicht viele Fragen (Abb. 9.1).

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@sever.tls > mein-key.asc
```

Die Datei mit dem Schlüssel kann man als eigenen Schlüssel importieren.

9.1.2 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
```

Persönlichen OpenPGP-Schlüssel hinzufügen

OpenPGP-Schlüssel erzeugen

Identität Max <mustermann@mailbox.org> - mailbox.org

Ablaufdatum

Legen Sie das Ablaufdatum Ihres neu erzeugten Schlüssels fest. Sie können das Datum später weiter in die Zukunft verschieben, falls nötig.

☒ Schlüssel läuft ab in 3 Jahren

☐ Schlüssel läuft nicht ab

Erweiterte Einstellungen

Erweiterte Einstellungen für Ihren OpenPGP-Schlüssel festlegen

Schlüsseltyp: RSA

Schlüsselgröße: 4096

Zurück Abbrechen Schlüssel erzeugen

Abbildung 9.1: Neues OpenPGP-Schlüsselpaar in Thunderbird erstellen

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. 9.2). 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.

9.1.3 Den eigenen öffentlichen Schlüssel verteilen

Damit Kommunikationspartner mir verschlüsselt schreiben oder die Signatur meiner E-Mail verifizieren können, muss man ihnen den eigenen öffentlichen Schlüssel zusenden oder zum Download anbieten. Dafür gibt es mehrere Möglichkeiten:

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<https://keys.openpgp.org>

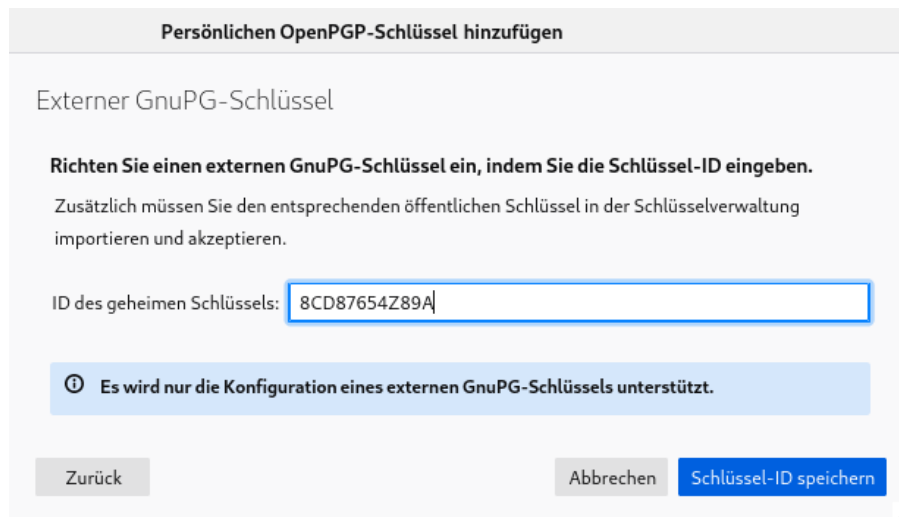


Abbildung 9.2: Privaten OpenPGP Schlüssel mit GnuPG verwalten

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 an eine E-Mail 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.)

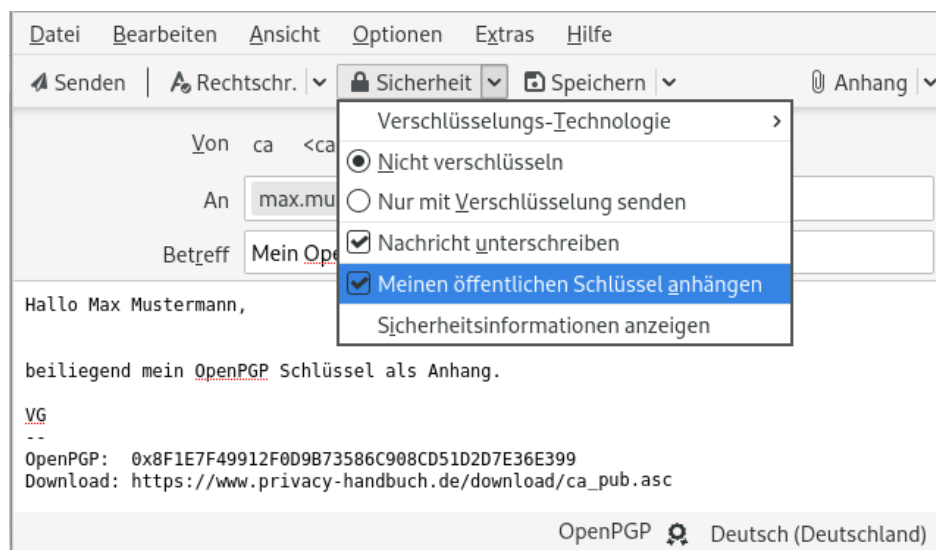
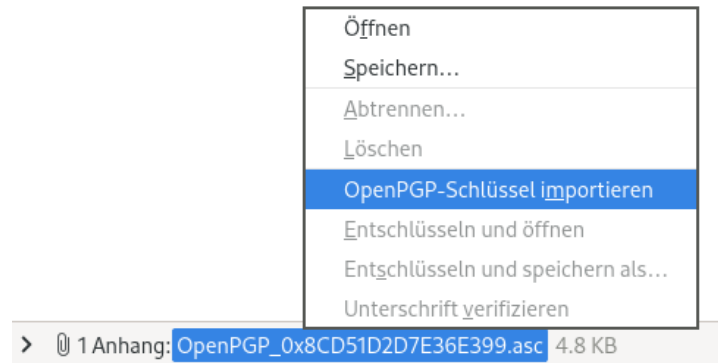


Abbildung 9.3: Öffentlichen OpenPGP Schlüssel per E-Mail verteilen

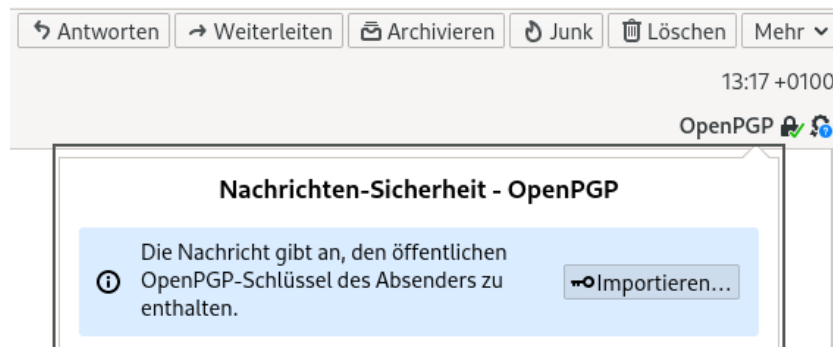
9.1.4 Fremde Schlüssel importieren

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.



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, wenn man die Download URL auf einer Webseite findet oder in der Signatur einer E-Mail.
 - Man kann den Schlüssel anhand der E-Mail Addr. via Web Key Discovery (WKD) und auf OpenPGP Keyservern suchen und importieren.

9.1.5 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 Fingerabdruck den Schlüssel 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 Schlüssel verifiziert hat und dass man sicher ist, den richtigen Schlüssel zu verwenden (Abb. 9.4).

9.2 Gedanken zum Mailvelope Browser Add-on

Mailvelope ist ein Add-on für die Browser Mozilla Firefox und Google Chrome, das OpenPGP Verschlüsselung im Webinterface ermöglicht.

| | |
|---------------------------------------|---|
| Vorgeblicher Schlüsselbesitzer | Max Mustermann <mustermann@server.tld> |
| Typ | öffentlicher Schlüssel |
| Fingerabdruck | C5DF 0BB0 11B7 3F49 3A37 AFC4 4472 A2E8 8A02 F3F6 |
| Erzeugt am | 18.06.2016 |
| Läuft ab am | Der Schlüssel läuft nicht ab. |

| | | |
|-----------------------|------------------|----------|
| Ihre Akzeptanz | Zertifizierungen | Struktur |
|-----------------------|------------------|----------|

Akzeptieren Sie diesen Schlüssel für das Verifizieren von digitalen Unterschriften und das Verschlüsseln von Nachrichten?

Akzeptieren Sie nur vertrauenswürdige Schlüssel. Verwenden Sie einen anderen Kommunikationskanal als E-Mail, um den Fingerabdruck des Schlüssels Ihres Kontakts zu verifizieren.

☐ Nein, diesen Schlüssel zurückweisen.
☐ Nicht jetzt, vielleicht später
☒ Ja, aber ich habe nicht überprüft, dass es sich um den korrekten Schlüssel handelt.
☐ Ja, ich selbst habe überprüft, dass der Schlüssel über den korrekten Fingerabdruck verfügt.

OK

Abbildung 9.4: Importierten OpenPGP Schlüssel akzeptieren oder verifizieren

Mailvelope kann die interne OpenPGP.js Implementierung nutzen oder eine externe GnuPG Installation. OpenPGP.js hat konzeptuell bedingt einige Schwächen und ist nicht für hohe Sicherheitsanforderungen geeignet. Konzeptuelle Schwächen von OpenPGP.js:

- **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 ermöglichen.
- **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 Securitybug (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* gezeigt haben.

Mit JavaScript ist es nicht möglich, einen geheimen Schlüssel nach der Benutzung aus dem Hauptspeicher zu löschen (Overwriting memory - why?). Das normale Verhal-

ten von Mailvelope wurde bei Tor Onion Router als Security Bug eingestuft.⁴

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.

9.2.1 Mailvelope mit GnuPG nutzen

Mailvelope bietet die Möglichkeit, eine lokale Installation von GnuPG zu verwenden statt der traditionelle Variante mit der OpenPGP.js Implementierung. Damit vermeidet man die oben genannten Schwächen von OpenPGP.js. Auch das Mailvelope Team empfiehlt in den FAQ⁵ die Verwendung von GnuPG zur Verbesserung der Sicherheit. Die Verwendung von OpenPGP Smartcards ist nur 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.

9.2.2 Mailvelope und Autocrypt

Standardmäßig verwendet Mailvelope den Autocrypt Schlüsseltausch. Da Autocrypt die Sicherheit von OpenPGP massiv schwächt, so dass die Verschlüsselung nur noch *some protection most of the time* bietet und keinen Schutz mehr gegen einen böartigen E-Mail Provider, ist die Deaktivierung von Autocrypt im Dashboard dringend zu empfehlen.

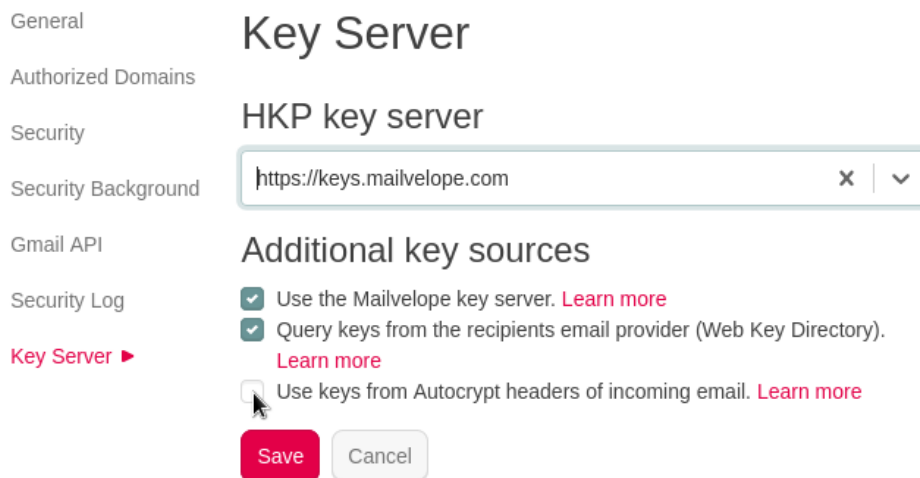


Abbildung 9.5: Autocrypt in Mailvelope deaktivieren

⁴<https://heise.de/-1746523>

⁵<https://www.mailvelope.com/de/faq#gupg>

9.3 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` ⁶ stellt ein Paket für Windows bereit mit GnuPG, dem GNU Privacy Assisten für die Schlüsselverwaltung und einer Erweiterung für MS Outlook.

Linux, BSD: installieren GnuPG 2.x nicht immer vollständig. Manchmal muss man etwas nachinstallieren. Für Debian/Ubuntu funktioniert:

```
> sudo apt install gnupg2 gpg-agent pinentry-gtk2 sdaemon
```

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 10min (600s) gespeichert. GPA ändert den Wert aus Sicherheitsgründen auf 300s.

```
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)
keyserver-options no-honor-keyserver-url, no-auto-key-retrieve, no-include-revoked

# Empfohlene Präferenzen 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
```

⁶<http://www.gpg4win.org>

```
# 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 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 vor einigen Jahren seinen Schlüssel erstellt hat, dann wird in diesem Fall beispielsweise 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 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
```

9.3.1 Gedanken zur Auswahl und Stärke von Schlüsseln

Aktuelle GnuPG Versionen unterstützen neben RSA und DSA Schlüsseln mit bis zu 4096 Bit Länge auch Schlüssel auf 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 verwendet. Bei ausreichender Schlüssellänge > 2000 Bit gelten diese Schlüssel als sicher.
2. Das BSI ist derzeit der Meinung, dass RSA Schlüssel mit einer Länge von 2048 Bit bis 2022 eingesetzt werden können (BSI TR-02102-1). (Wenn man also jetzt einen neuen Schlüssel generiert, der für 5 Jahre gültig ist und dann möglicherweise verlängert werden soll, dann sollte man mindestens 3072 Bit Schlüssellänge wählen.)
3. Schlüssel auf Basis elliptischer Kurven werden nur in aktuellen PGP Implementierungen unterstützt, die sich aber noch nicht überall durchgesetzt haben.
4. 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 GnuPG Team hat mit RFC 4880bis Draft eine Erweiterung vorgeschlagen, auch die Unterstützung für die Kurven Ed25519 und Curve25519 zu integrieren. Dieser Draft ist bisher nur in GnuPG 2.1.x umgesetzt worden.

Wer jetzt schon Schlüssel auf Basis elliptischer Kurven verwendet, muss mit Problemen bei einigen Empfängern rechnen, insbesondere mit den elliptischen Kurven Ed25519 und Curve25519. Empfehlenswert für langfristige Nutzung sind RSA Schlüssel mit 4096 Bit Länge.

9.3.2 GnuPG Smartcards nutzen

Die Sicherheit asymmetrischer Verschlüsselung hängt von der sicheren Aufbewahrung des privaten Schlüssels ab. Es gibt mehrere Möglichkeiten, wie privaten 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.org⁷ verhindern können.

Ein paar Angebote für OpenPGP Smartcards:

⁷<http://heise.de/-2817797>

- Die **GnuPG-Smartcard** gibt es von kernelconcepts.de⁸. Die Bestellung erfolgt per E-Mail und man braucht zusätzlich einen Smartcard Reader oder den ebenfalls dort erhältlichen Gemalto USB Adapter.
- Der **NitroKey**⁹ ist ein Open Source Hardware Projekt und der Nachfolger des Cryptostick. Der NitroKey Pro enthält zusätzlich einen OTP-Generator und Passwortspeicher. (Für diese Zusatzfunktion ist die NitroKey App¹⁰ zu installieren.)
- Der **Yubikey** ist ein One-Time-Passwordgenerator (OTP), den man für Logins bei Webdiensten nutzen kann. Er enthält zusätzlich eine OpenPGP Smartcard.¹¹

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 ...: D27600xxxxxxxxxxxxxxxx
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).

Funktionen für Genießer

Die Nutzung von *gpg2* auf der Kommandozeile bietet etwas mehr Möglichkeiten, als die GUIs von Enigmail oder GPA zur Verfügung. Natürlich stehen auch die mit dem GUI durchführbaren Funktionen auf der Kommandozeile zur Verfügung. Einen Überblick über alle Smartcard-Funktionen gibt die Hilfe mit dem *help* Kommando. 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 zurück setzen 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

⁸<https://www.floss-shop.de/de/search?sSearch=OpenPGP>

⁹<https://www.nitrokey.com/de>

¹⁰<https://www.nitrokey.com/de/download>

¹¹<https://www.yubico.com/products/yubikey-hardware/>

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 weiter verwenden

Wenn man bereits PGP für die Verschlüsselung nutzt und einen vorhandenen Schlüssel weiter verwenden möchte, dann kann man die Private Keys dieses Schlüssel 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 Schlüssel zum Signieren, einen Schlüssel zum Verschlüsseln und einen Schlüssel zum Authentifizieren. Man muss den von GnuPG erstellten Haupt- und Unterschlüssel einzeln auf die korrespondierenden Plätze auf der Smartcard schieben.

Als erstes ruft man *gnupg2* mit der *edit-key* Funktion 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

```

9.3.3 Adele - der freundliche OpenPGP E-Mail-Roboter

Adele ist der freundliche OpenPGP E-Mail-Roboter der G-N-U GmbH. Man kann mit dem Robot seine ersten verschlüsselten Mails austauschen und ein wenig üben ohne Freunde mit Anfängerproblemen zu belästigen.

1. **Den eigenen Schlüssel an Adele senden:** Als erstes schickt man den eigenen öffentlichen Schlüssel per E-Mail an *adele@gnupp.de*. Den Schlüssel hängt man als Anhang an die Mail an, indem man die Option *OpenPGP - Meinen öffentlichen Schlüssel anhängen* vor dem Versenden der Mail aktiviert (Bild ??)
2. **Verschlüsselte Antwort von Adele:** Als Antwort erhält man nach einigen Minuten eine verschlüsselte E-Mail von Adele. Die E-Mail wird nach Abfrage der Passphrase entschlüsselt und enthält den Schlüssel von Adele:

```

Hallo,

hier ist die verschlüsselte Antwort auf Ihre E-Mail.

Ihr öffentlicher Schlüssel wurde von mir empfangen.

Anbei der öffentliche Schlüssel von adele@gnupp.de,
dem freundlichen E-Mail-Roboter.

Viele Grüße,
adele@gnupp.de

```

```

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (GNU/Linux)

mQGibDyFlIkRBACfVHJxv47r6rux7TwT4jHM7z/2VfyCrmcRegQEsbdLfqu3mEmK
RouuaDQukNINWk2V2ErOWzFnJqdzpapeuPJiOWpOuIEvU3FRPhYlytw9dFfwAHv4
MJ7639tAx9PfXBmZOd1PAoE451+VLhIG1LQiFGFppJ57SZ1EQ71/+nkSwCg8Mge
....
EQIABgUCPIWU1QASCRD1czRpkqs/9wd1R1BHAAEBv20AoJJGeeZjMCSbXtmNSwfW
QsLOd0+4AKCdXwt552yi9dBfXPo8pB1KDnhtbQ==
=ERT8
-----END PGP PUBLIC KEY BLOCK-----

```

- 3. Schlüssel von Adele importieren:** Man kann die Zeilen von BEGIN PGP PUBLIC KEY BLOCK bis einschließlich END PGP PUBLIC KEY BLOCK mit der Maus markieren, in die Zwischenablage kopieren und in der Schlüsselverwaltung über *Bearbeiten - Aus Zwischenablage importieren* einfügen.

Alternativ holt man sich Adeles Schlüssel mit der ID 0x92AB3FF7 von einem Keyserver.

- 4. Adele verschlüsselte E-Mails schreiben** Jetzt kann man Adele verschlüsselte E-Mails schicken. Als Antwort erhält man umgehend eine gleichfalls verschlüsselte E-Mail mit dem gesendeten Text als Zitat.

Hallo,

hier ist die verschlüsselte Antwort auf Ihre E-Mail.

Ich schicke Ihnen Ihre Botschaft im Wortlaut zurück, damit Sie sehen, dass ich sie erfolgreich entschlüsseln konnte.

```

> Hello Adele,
>
> hope you are feeling well.

```

Hinweis: PGP/Inline statt PGP/MIME verwenden. Adele ist schon eine etwas ältere Dame und versteht nur das alte Format PGP/Inline während Enigmail inzwischen das modernere PGP/MIME Format verwendet.

Beim Schreiben einer E-Mail an Adele muss man deshalb immer auf PGP/Inline umschalten, anderenfalls kann Adele die Mail nicht interpretieren. Menüpunkt *Enigmail - Protokoll PGP/Inline* aktivieren!

9.3.4 Memory Hole Project

Eine E-Mail enthält im Header viele Informationen. Neben dem *Betreff*: steht dort auch, auf welche E-Mail geantwortet wurde (*In-Reply-To*: und *References*:). Diese Informationen sind für den Transport der E-Mail nicht nötig und könnten verschlüsselt übertragen werden.

```

To: Max Mustermann <mustermann@server.tld>
From: Maxi Mutterfrau <mutterfrau@server.tld>
Subject: Re: Plenum der K-Gruppe (KaG) am 32.02.2017 um 26:20 Uhr
References: <5cc396a27b873f3fa@mailbox.org>
In-Reply-To: <5cc396a27b873f3fa@mailbox.org>
Message-ID: <49e6a7bfbc433sfgcfcge@secure.mailbox.org>
Date: Wed, 29 Mar 2017 21:55:37 +0200
MIME-Version: 1.0

```



```
Content-Type: multipart/encrypted;
    protocol="application/pgp-encrypted";
...
```

Das Memory Hole Projekt möchte einen Ansatz entwickelt, um die für den Transport unwichtigen Informationen ebenfalls zu verschlüsseln. Die Headerzeilen werden dabei in dem verschlüsselten PGP/MIME Part versteckt und können nur vom Empfänger bei der Entschlüsselung der Mail gelesen und sichtbar gemacht werden.

Enigmail unterstützt dieses Feature bereits. Wenn man die folgenden Parameter setzt, wird der Mail Header *Betreff:* in OpenPGP verschlüsselten E-Mails durch die konfigurierte Floskel *Encrypted Message* ersetzt und der originale Text in den verschlüsselten PGP/MIME Part verschoben. Wenn die Mail entschlüsselt wird, wird der Betreff wieder hergestellt.

```
extensions.enigmail.protectedHeaders      = 2
extensions.enigmail.protectedSubjectText  = Encrypted Message
```

Außerdem kann man die Header *In-Reply-To:* und *References:* im PGP/MIME Part verstecken, indem man zusätzlich folgenden Parameter setzt:

```
extensions.enigmail.protectReferencesHdr   = true
```

Als Ergebnis würden dann die E-Mail Header aus dem oben gezeigten Beispiel wie folgt aussehen:

```
To: Max Mustermann <mustermann@server.tld>
From: Maxi Mutterfrau <mutterfrau@server.tld>
Subject: Encrypted Message
Message-ID: <49e6a7bfbc433sfgcfcge@secure.mailbox.org>
Date: Wed, 29 Mar 2017 21:55:37 +0200
MIME-Version: 1.0
Content-Type: multipart/encrypted;
    protocol="application/pgp-encrypted";
...
```

9.3.5 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 Validierung?) zu kümmern.

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 Mail Providern ständig routiniert manipuliert. Es werden neue Header eingefügt, einige Header werden gelöscht. . . In gleicher Weise könnten die Autocrypt Header von den versendenden oder empfangenen E-Mail Providern manipuliert werden und ein falscher Schlüssel 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 ein 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 zu 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 zugrunde liegenden Konzeptes.

Das 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 es, dass man dem E-Mail Provider vertrauen muss und führt damit Ende-zu-Ende Verschlüsselung mit OpenPGP ad absurdum, es kompromittiert die Sicherheit zugunsten (zweifelhafter) Vereinfachungen der Usability.

9.3.6 Verschlüsselung in Webformularen

Auch bei der Nutzung eines Webmail Accounts oder Webforms für die Versendung anonymer E-Mails muss man auf Verschlüsselung nicht verzichten.

Einige grafische Tools für die Schlüsselverwaltung wie GPA¹² (*GNU Privacy Assistant*) 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.

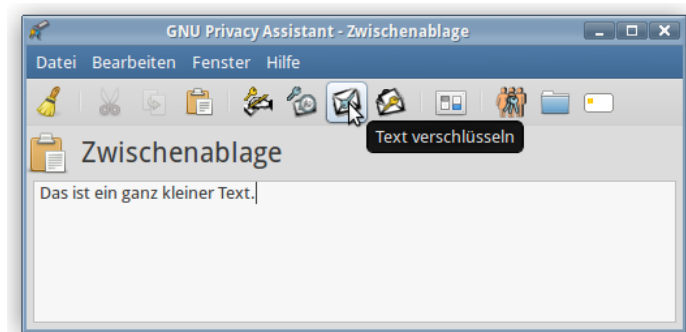


Abbildung 9.6: Text mit GPA verschlüsseln

¹²http://www.gnupg.org/related_software/gpa/index.de.html

Andere grafische Tools wie *Kleopatra* von 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, kwriter...), 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: 15.2). 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.

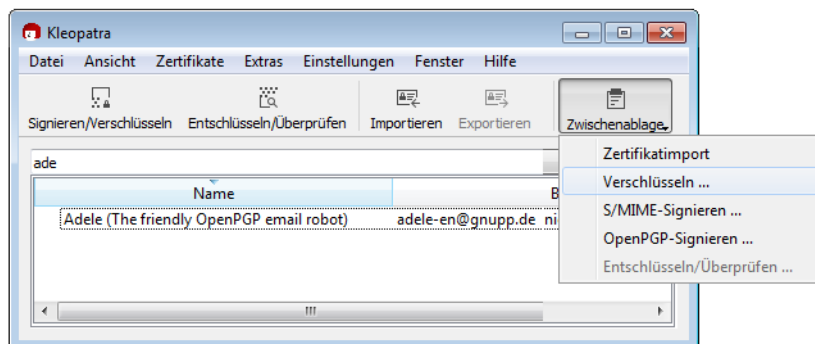


Abbildung 9.7: Kleopatra GnuPG GUI: Assistent zur Verschlüsselung von Dateien

Linuxer könnten auch das GnuPG Desktop Applet von den TAILS Entwicklern nutzen, das ebenfalls den Text in der Zwischenablage ver- oder entschlüsseln kann. Das Applet kann unter Debian/Ubuntu mit dem bevorzugten Paketmanager installiert werden:

```
> sudo apt install openpgp-applet
```

9.3.7 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 allgm. 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 Wordpress Plug-ins für Kontaktformulare, einfache PHP-Skripte oder fertige Perl-CGI Skripte. 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 Skripte 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 SSL-Verschlüsselung für einen kleinen Aufpreis 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 zu aktivieren 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 Beschlagnahmung 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 Sicherheit, 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 OpenPGPjs¹³ ist bei Github auszuchecken und aus dem Verzeichnis *dist* auf den eigenen Webserver kopieren.
2. Das JavaScript Schnipselchen *encrypt_message.js* von der Webseite im Privacy Handbuch¹⁴ 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 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");
```

¹³<https://github.com/openpgpjs/openpgpjs>

¹⁴https://www.privacy-handbuch.de/handbuch_32v.htm

```

    if(message.value == "") {
        window.alert("Kein Text gefunden, das Textfeld ist leer!");
    } else {
        # Verschlüsseln des Textes im Textarea
        var options = { data: message.value,
            publicKey: 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 Skripte zu laden:

```

...
<script src="openpgp.min.js" async></script>
<script src="encrypt_message.js" async></script>
...

```

4. Im 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 ein 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.

9.3.8 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. DOS-Box kann man nach OpenPGP Schlüsseln anhand der E-Mail Adresse suchen und einen der gefundenen Schlüssel importieren:

```
> gpg2 --search cane@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 0x8F1E7F49912F0D9B73586C908CD51D2D7E36E399
```

- 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-Mail 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 hkps://zkaan2xfbuxia2wpf7ofnkbz6r5zdbbvxunvp5g2iebopbfc4iqmbad.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 beendet evtl. 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 u.ä. veralteten Servern nach Schlüsseln anhand E-Mail Adressen, 8-stellige oder 16-stellige Key IDs oder bekannten Fingerprints 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 Okt. 2013 ist korrekt (nicht der neueste Schlüssel!), wie Fefe in seinem Blog schreibt.¹⁵

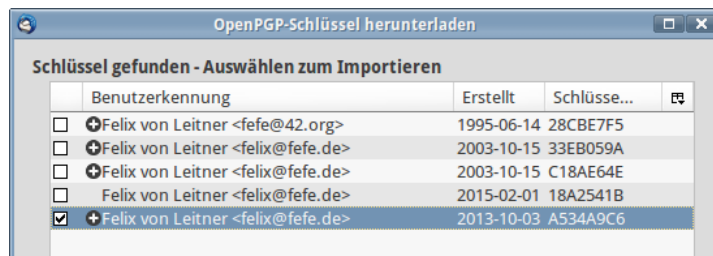


Abbildung 9.8: Fünf OpenPGP-Schlüssel für eine E-Mail Adresse

J. Schmidt von Heise.de beklagt, dass ein Scherzkeks OpenPGP Schlüssel für seine E-Mail Adresse auf die Keyserver hochgeladen hat und dass er 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 Keyserver publiziert.¹⁶

Gavin Andresen signierte die Bitcoin Binaries, für seine E-Mail Adresse wurden ebenfalls Fake Schlüssel auf den Keyserver publiziert.¹⁷

2. Statt E-Mail Adressen kann man auch nach der 8-stelligen Key-ID suchen (zB. 0xA534A9C6). Diese Methode liefert besser 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.¹⁸
3. Die 16-stellige Key-ID (zB. 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 Fingerprint sucht (zB. 0x68995C53D2CEE11B0E4182F62146D0CD2B3CAA3E). Diese Suche liefert als einzige Variante vertrauenswürdige Ergebnisse.

9.3.9 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. Es bildet sich ein kleines Netz von Vertrauensbeziehungen. Die Grafik 9.9 zeigt eine mögliche Variante für den Key von Anton (A).

- Anton (A) vertraut dem Schlüssel von Conrad (C), weil er von Beatrice (B) unterschrieben wurde und Beatrice für Anton eine vertrauenswürdige Person ist.

¹⁵<https://blog.fefe.de/?ts=aa27d652>

¹⁶<https://lists.torproject.org/pipermail/tor-talk/2014-March/032308.html>

¹⁷<http://gavintech.blogspot.ch/2014/03/it-aint-me-ive-got-gpg-imposter.html>

¹⁸<http://heise.de/-2473281>

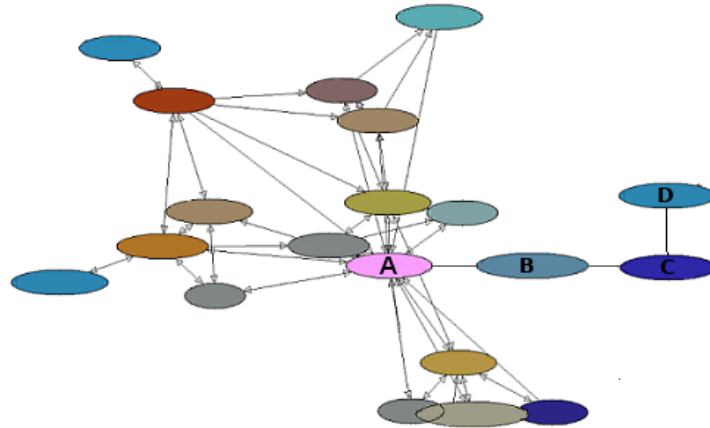


Abbildung 9.9: Beispiel für ein Web of Trust

- Anton (A) vertraut dem Schlüssel von Doris (D) nicht, obwohl er von Conrad unterschrieben wurde und der Schlüssel 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 Arbeitsgruppe oder 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)

9.4 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, das 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. 15.1).

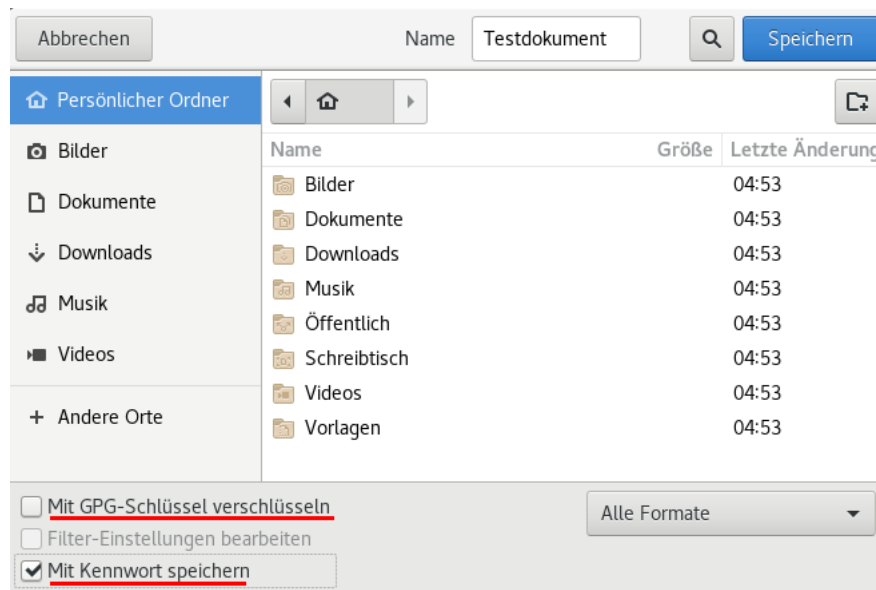


Abbildung 9.10: Verschlüsselte Speicherung in LibreOffice aktivieren

Wenn man keine OpenPGP Schlüssel verwendet sondern ein Kennwort, dann muss man dem Empfänger das Kennwort zu 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, man kann ein einmal sicher ausgetauschte Passwort natürlich auch über einen längeren Zeitraum verwenden. Das ist sicherer, als immer wieder unsichere Methoden für den Passworttausch zu nutzen.

Kapitel 10

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/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 in der Regel keine Gruppenchats und keine Kommunikation in Gruppen.
3. Videokonferenz Systeme können in der Regel 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 die Erreichbarkeit ist eine wesentliche Voraussetzung für InstantMMessaging. Desktop Clients sind in der Regel auch vorhanden, aber manchmal nur als Zusatzoption zur Smartphone App.

Threema ist einer der sichersten Messenger und hat eine 7-stellige Nutzerbasis. Es wird eine zufällig Buchstabenkombination als Kennung für den Account generiert, der optional mit einer Telefonnummer verknüpft werden kann. Neben Messaging Funktionen gibt es verschlüsselte Audio- und Videotelefonie. Threema ist eine sehr gute Lösung für vertrauliche, private Kommunikation.

Die Client Apps sind Open Source und die gesamte Software wurde mehrfach auditiert.

Es gibt außerdem eine kommerzielle Version für Unternehmen und mit Threema On-Prem eine Version für hohen 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.

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.

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 Teilnehmern 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 ist der bevorzugte Messenger der Bundesregierung und vom BSI für VS-NfD zugelassen. Wire ist eine gute Collaboration Plattform für Unternehmen.

Jabber/XMPP, matrix sind ebenfalls kostenlos und Open Source. Im Gegensatz zu Threema, Signal App oder Telegram wird die förderale 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 förderale 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 förderale 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 Regeln², 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 **Sichere Mobile Kommunikation** 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.

Briar (nur für Android) 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.

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.

¹<https://www.signal.org/blog/the-ecosystem-is-moving>

²<https://www.presseportal.de/pm/76712/4764023>

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 seit 2011 mit der Standardisierung des SRTP/ZRTP Protokolls vorhanden gewesen wären. Aktuell bieten Messenger (siehe oben) eine einfach nutzbare Möglichkeit für verschlüsselte Audio- und Videotelefonie und machen die Installation zusätzlicher 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, sollten 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 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.

Tox ist ein offenes Protokoll für verschlüsselte Telefonie und Chats. Die Kommunikation läuft direkt von Client zu Client. Es gibt keine zentralen Server und keinen Provider, der Kommunikationsprofile erstellen könnte. Tox ist ein Protokoll, das für hohe Sicherheitsansprüche und Anonymität entwickelt wurde.

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.

³https://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/>

Eine durchgehende Ende-zu-Ende Verschlüsselung gibt es bei Videokonferenzen nicht. In der Regel können die Server Betreiber die Konferenzen beobachten. Man könnte den Server selbst aufsetzen oder eine 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, 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 Sept. 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.

10.1 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 entgegen zu setzen. 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 beispw. in einigen Gebieten von Frankreich, in VAE oder Saudi Arabien üblich ist.

Verschiedene Forschungsergebnisse wie *Language Identification in Encrypted VoIP Traffic* (2007), *Recovering Spoken Phrases in Encrypted VoIP Conversation* (2008) und *Phonotactic Reconstruction of Encrypted VoIP Conversations* (2011) zeigen, dass es bei der Verschlüsselung

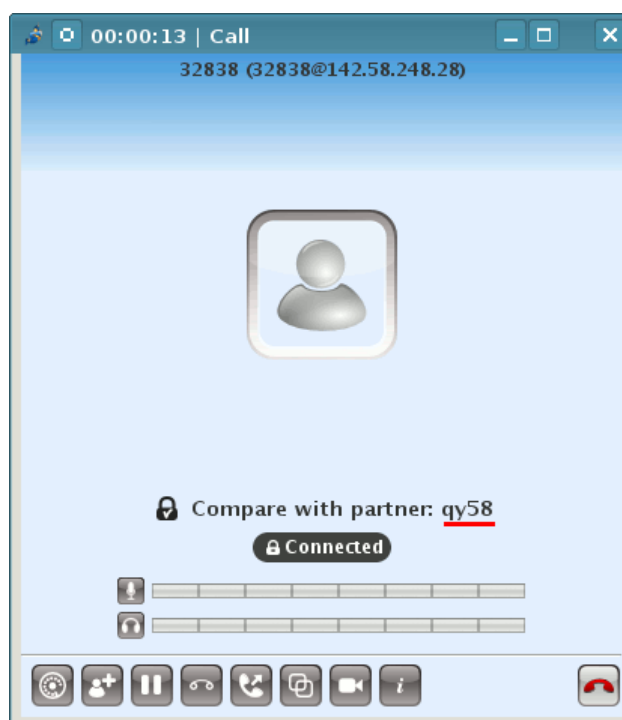


Abbildung 10.1: SAS Authentication bei Jitsi als Beispiel

von Telefonie Angriffsmöglichkeiten gibt, um gesprochene Phrasen anhand der variierenden Datenrate aus dem verschlüsselten Datenstrom zu rekonstruieren ohne die Verschlüsselung knacken zu müssen. Deshalb wird für hohe Sicherheitsanforderungen die Verwendung einer festen Datenrate empfohlen. Diese Technik ist auch bei den Geheimdiensten seit mehreren Jahren im Einsatz.

10.1.1 SRTP/ZRTP Verschlüsselung

Das SRTP/ZRTP-Protokoll⁶ 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 ZRTP-Protokoll beherrscht, wird die Verschlüsselung automatisch ausgehandelt. Kurze Erläuterung der Begriffe:

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 ersten beiden Buchstaben und der Angerufenen die beiden letzten Buchstaben. Wenn die Zeichenfolge

⁶<https://tools.ietf.org/html/draft-zimmermann-avt-zrtp-22>

identisch ist, kann man davon ausgehen, dass kein Man-in-the-Middle das Gespräch belauschen kann.

10.1.2 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 könnte 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** am besten. Für Android gibt es **Antox** (im Google Playstore) und den **TRIfA Tox Client** im F-Droid-Store und Playstore. 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 Repositories zur Installation an. Man kann den bevorzugten Paketmanager nutzen, um das Programm zu installieren und aktualisieren:

```
Fedora: > sudo dnf install qtox
Ubuntu: > sudo apt install qtox
```

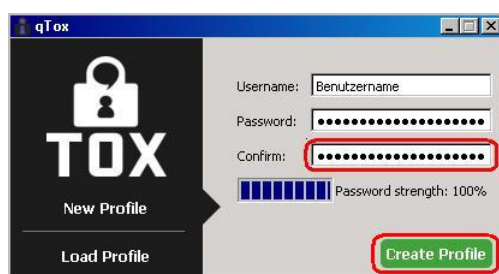
Anwender von Fedora sollten das RPMFusion Repository vorher aktivieren, damit die notwendigen Codecs für Audio- und Videotelefonie mit installiert werden.

***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.

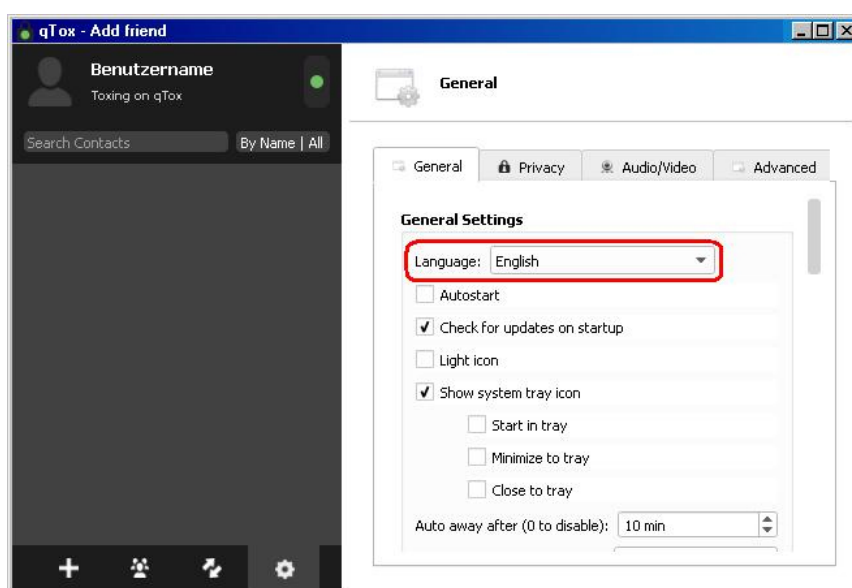


Es sollte ein starkes Passwort gewählt werden - je größer die Basis der möglichen Zeichen (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen), je zufälliger diese Zeichen gewürfelt werden und je mehr Stellen das Passwort hat, desto stärker das Passwort.

Konfiguration von qTox

Im Hauptmenü wählt man in den Einstellungen, die man jederzeit durch Klick auf das Zahnradchen erreicht, zunächst die Registerkarte *General*. Bei *Language* lässt sich die Sprache umstellen und man auf *English* klickt und die Sprache *Deutsch* wählen.

Hier lässt sich nun auch einstellen, ob man qTox bei jedem Systemstart mitstarten lassen möchte, ob man regelmäßig nach Updates suchen möchte, ob in der Systemleiste ein Icon angezeigt werden soll, ob qTox bei Programmstart zunächst nur in 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 Schreibenachrichtungen für Chats deaktivieren.

Auf der Registerkarte *Audio/Video* kann man die Audio- und Videoeinstellungen konfigurieren und testen.

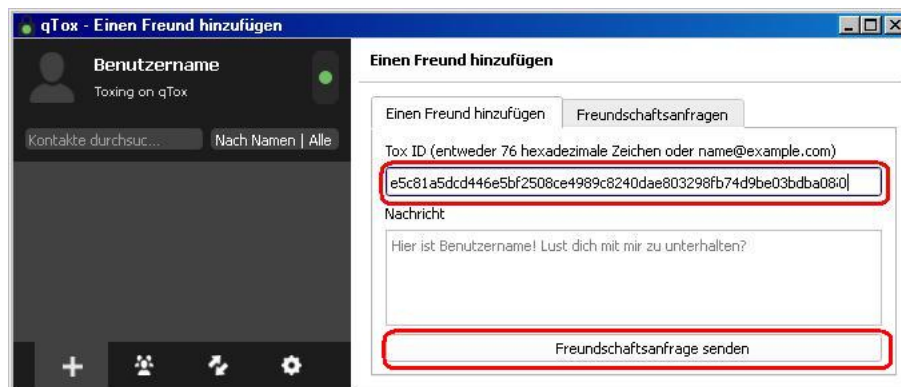
Auf der Registerkarte *Erweitert* kann man qTox in eine portable Programmversion umwandeln, die man auf dem USB-Stick mitnehmen kann.

Kontakt aufnehmen

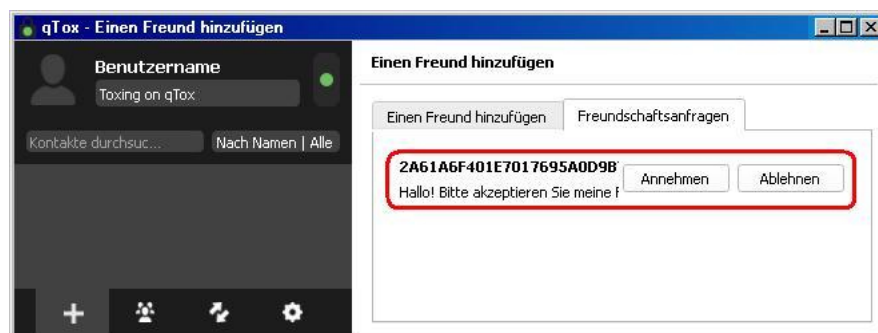
Wenn Anton und Beatrice Tox für die Kommunikation nutzen wollen, müssen sie die Tox-ID austauschen. Das könnte in folgenden Schritten ablaufen:

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.

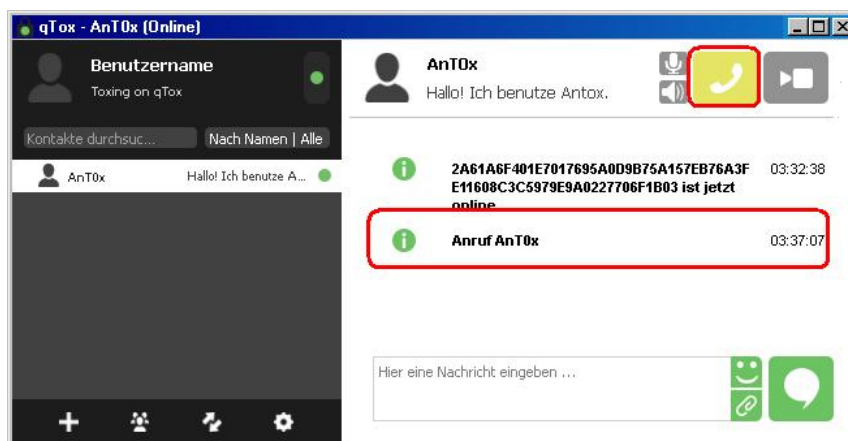


Erhält man eine Freundschaftsanfrage eines anderen Benutzers, so wird oben links im Programmfenster ein grünes Feld mit der Aufschrift *1 neue Freundschaftsanfrage* angezeigt. Durch Klick auf diese grüne Schaltfläche werden weitere Infos zur Freundschaftsanfrage angezeigt - etwa die ID, eventuell auch den Benutzernamen und/oder einen 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.

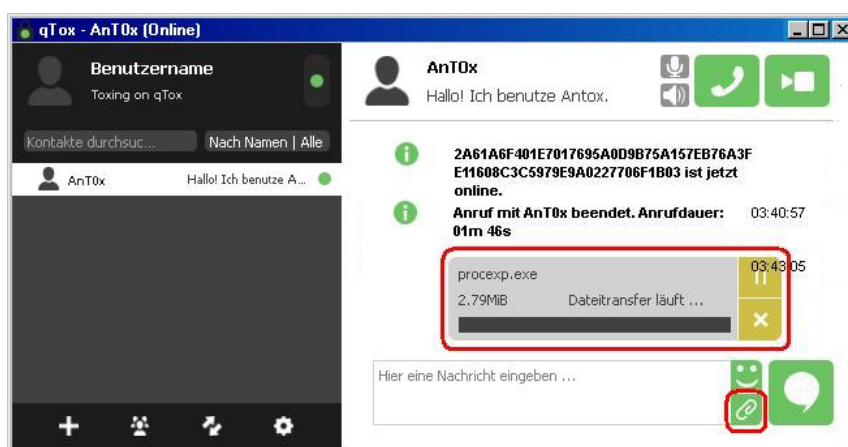


Kontakte anrufen, Dateien schicken oder chatten

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).



10.1.3 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 zensur-robuste 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 Mitlesen⁷ (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 Abhörmaßnahmen für einen Telefonanschluss waren ohne Kooperation der Telekommunikationsanbieter und ohne vorbereitete Schnittstellen nicht mehr möglich.

⁷<https://heise.de/-1857620>

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* ⁸ von 1994. In Deutschland wurde 1995 auf Initiative des Verfassungsschutz die *Fernmeldeverkehr-Überwachungsverordnung* (FÜV) ⁹ beschlossen, die 2002 durch die *Telekommunikations-Überwachungsverordnung* (TKÜV) ¹⁰ 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 Nov. 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.¹¹

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 der Skype verdreifacht werden.¹²

10.2 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.¹³

In korrektem Juristen-Deutsch könnte man es DSGVO-konform z. B. so formulieren:¹⁴

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 so ablaufen:

- Anton: *Du hast doch nichts dagegen, wenn ich Facebook Deinen Namen mit der Telefonnummer schicke und das wir Freunde sind - oder?*
- Beatrice: *Eyhh man, alles ok - mache ich doch auch.?*

⁸<https://secure.wikimedia.org/wikipedia/en/wiki/Calea>

⁹<http://www.online-recht.de/vorges.html?FUEV>

¹⁰<https://de.wikipedia.org/wiki/Telekommunikations-%C3%9Cberwachungsverordnung>

¹¹<http://www.lawblog.de/index.php/archives/2010/08/17/skype-staat-hort-mit>

¹²<https://heise.de/-1916340>

¹³<https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/whatsapp-will-infos-mit-facebook-teilen-12995>

¹⁴<https://www.lareda.hessenrecht.hessen.de/bshe/document/LARE190000030>

Anforderungen an einen guten Messenger

Unter Berücksichtigung der massiven Überwachung von Instant Messaging, welche durch E. Snowden bekannt gemacht wurde, und des Crypto War 3.0 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-Fundus¹⁵ zeigt, dass Geheimdienste die Messenger Kommunikation massiv überwachen.

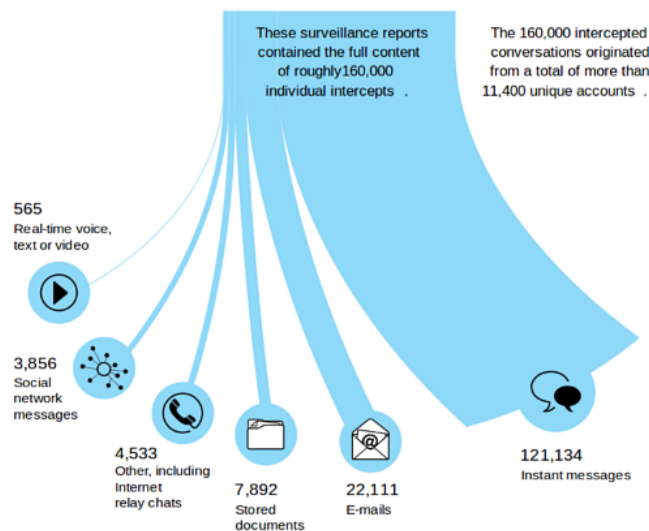


Abbildung 10.2: Auswertung von 160.000 Überwachungsberichten

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 und die Zuordnung zu einer Person. Außerdem schützt die Weitergabe eines Pseudonyms statt Telefonnummer gegen Stalking.
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 Infrastruktur sind nur schwer von Regierungen durch Gesetze kompromittierbar, um Geheimdiensten die Überwachung zu ermöglichen wie z. B. mit BlackBerry in Indien oder in Kanada, Skype weltweit oder die Gesetze zu Backdoors für alle Messenger in Russland oder Australien.

¹⁵<http://apps.washingtonpost.com/g/page/world/communication-breakdown/1153/>

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 Admin von Jabber oder [matrix] Servern per Definition zu Heiligen erklärt, die niemals nie etwas anderes installieren würden als die offizielle Serversoftware und nie 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, haben wir gehofft, das die Admins der Server nicht mit dem Modul *mod_otr*¹⁶ - *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.* und 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.)

8. Es wäre schön, wenn die Bedienung so einfach wäre, dass auch meine Tante und ihre Kaffeekranz Freundinnen ohne lange Erklärungen damit umgehen können.

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 ein 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 wie¹⁷: die Behörden gaben die Telefonnummer der Zielperson in der Telegram Web-App eingeben und die SMS zur Authentisierung des Zugriffs abfangen. 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 hat 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 können. Dafür brauchte das BKA allerdings kurzzeitig einen unbeobachteten Zugriff auf das entspernte 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.
- Das Audit der OMEMO Verschlüsselung 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

¹⁶https://www.ejabberd.im/mod_otr

¹⁷<https://www.youtube.com/watch?v=wBaj0LxcnY8>

Alice, ein neues Gerät mit einem eigenen Key für Bob in die Liste aufzunehmen. Alice sendet in Zukunft alle Nachricht 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 Geräte-ID, bevor sie die Nachricht an Bob weiterleitet (Abb. 10.3). Diese Manipulation ist bei OMEMO möglich, weil die Nachrichten nicht kryptografisch authentifiziert werden. (Hat man das einfach vergessen?)

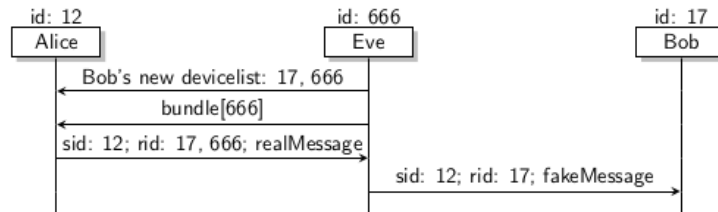


Abbildung 10.3: Man-in-the-Middle Angriff auf OMEMO Verschlüsselung

- Ein kleiner Test von Riot ([matrix]) zeigte ebenfalls erhebliche Hürden in der Usability beim Schutz gegen das Einschleusen eines bössartigen Gerätes. (Wobei man noch hinzufügen muss, dass beide Teilnehmer in dem Chat als Krypto-Experten gelten und wirklich verstanden haben, wie sichere Krypto funktionieren könnte.)
 - Anton: *Ok - habe Riot installiert und bin drin!*
 - Beatrice: *War doch ganz einfach - oder?*
 - Anton: *Aber der Chat ist unverschlüsselt. Sollte das nicht E-2-E sein?*
 - Beatrice: *Du musst die E-2-E Verschlüsselung erst aktivieren.*
 - Anton: *Habe ich in den Einstellungen aktiviert.*
 - Beatrice: *Nee - DU musst es für JEDEN Chat einzeln aktivieren.*
 - Anton: *Wie? Wo? Finde nix.*
 - Beatrice: *Chat Settings, ganz runter scrollen, unten die letzte Option.*
 - Anton: *Ok - hab's gefunden.*
 - Beatrice: *Ist halt BETA, kann man noch verberssern.*
 - Anton: *Hmmm - sehe gerade, dass Du hier mit 6 Geräten chattest!!! 2x Linux, 3x Ubuntu und ein seltsames Phone. Bist Du sicher, dass die alle von Dir sind - oder...???*
 - Beatrice: *Kann schon sein, keine Ahnung - ich nutze Riot schon länger...*
 - Anton: *Arrrghhhh...*

Es ist eine alte Weisheit, dass eine Kommunikation erst dann wirklich vertrauenswürdig ist, wenn man gegenseitig die Schlüssel verifiziert hat und sicherstellt, dass nur diese verifizierten Schlüssel verwendet werden. Die meisten Messenger bieten irgendwie eine Möglichkeit, bei einem Treffen die Schlüssel zu verifizieren, allerdings ist das nicht immer DAU-kompatibel.

Außerdem kann man bei vielen Multi-Device fähigen Messengern eine zweistufige Bestätigung für das Hinzufügen weiterer Geräte aktivieren. Damit ist eine zusätzliche Passphrase erforderlich, die sich vom Account Passwort unterscheiden sollte, wenn ein neues Gerät angemeldet wird.

Als Schutz gegen Angriffe bei (kurzzeitigem) physischem Zugriff auf ein entsperartes 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 heimlich 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.

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 Vertauen 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 zus. 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 einfach Messenger die public Keys der Nutzer auf den Servern zur Verfügung. Ein böstiger Betreiber könnte prinzipiell die Keys austauschen und den Datenverkehr umleiten, so dass Mallory wieder in der Mitte sitzt und als Reflektor agieren kann, der die Nachrichten umschlüsselt und mitliest.

Ob man derartige Angriffe für möglich hält, hängt vor allem vom Vertrauen in den Provider ab. Da Ende-zu-Ende Verschlüsselung auch gegen böstige Provider schützen soll, ist es aber legitim, diese Angriffe in Erwägung zu ziehen und zu diskutieren.

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 Kanal wirklich die gewünschte Person sitzt. Der Kanal muss verifiziert sein.

Die Notwendigkeit der Verifikation hängt wesentlich vom Verfahren des Schlüsseltausch beim Aufbau der Kommunikation ab und von den Sicherheitsanforderungen.

- 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.¹⁸

Bei X3DH könnte ein böartiger Provider die Verbindungsaufnahme blockieren. Es ist aber (nach aktuellem Stand) nicht möglich, modifizierte Keys einzuschleusen.

- 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 ein Link Preview, wenn man eine URL in das Eingabefeld tippt oder kopiert. Man kann den hübschen Preview versenden oder vor dem Versand löschen.

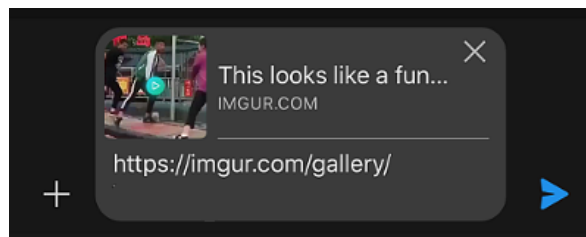


Abbildung 10.4: Link Preview in einem Chat in Signal App

Voraussetzung für einen Link Preview ist, dass 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">
    ...
```

¹⁸<https://signal.org/docs/specifications/x3dh/>

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 beispw. 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/Riot macht es ähnlich wie Telegram. Bei unverschlüsselten Chats werden die Link Previews vom Matrix Server generiert. Dieses Feature kann in den Einstellungen von Riot deaktiviert werden. Bei Ende-zu-Ende verschlüsselten Chats sollen laut Spezifikation keine Link Previews generiert werden.

10.2.1 Messenger Threema

Threema ist ein privacy-freundlicher Messenger aus der Schweiz. Chats, Gruppenchats und 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 auditiert¹⁹. Die Finanzierung erfolgt durch geringe, einmalige Kosten beim Download der App. Außerdem gibt es mit *Threema Work* und *Threema OnPrem* kommerzielle Lösungen für sichere Unternehmenskommunikation, mit der 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/Broadcast²⁰ 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, ohne die eigene Identität zu kompromittieren und gleichzeitig anderen eine Möglichkeit zur anonymen Kontaktaufnahme zu geben.

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 verbinden** oder E-Mail Adresse. 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

¹⁹https://threema.ch/de/faq/code_audit

²⁰<https://broadcast.threema.ch/de>

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 Telefonnummern 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:

- **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/gehackt wurde, ist es unmöglich, dass ein Dritter die Nachrichten fälschen oder mitlesen kann.

Bei Threema speichert der Client alle Informationen zu Kontaktlisten, Mitgliedschaften in Gruppenchats usw. lokal. Die Server haben keine Informationen. Wenn man das Smartphone wechselt, ist es wichtig, dass man ein Backup der lokalen Daten erstellt und auf dem neuen Smartphone einspielt. Wenn man das nicht macht, beginnt man komplett neu an mit einem neuen Account und verliert alle Kontakte und Gruppenmitgliedschaften.

Das **Backup** wird mit einem Passwort verschlüsselt und kann auf dem Threema Server gespeichert werden oder auf einem beliebigen WebDAV Server. 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 Verz. 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 angeben inklusive Login Credentials für den WebDAV Server (Abb. 10.5).

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 das Backup gehört. Trotzdem kann die Datei beim Restore eindeutig gefunden werden. Dieses Konzept ist bisher unter Messengern einmalig.

Für Android Smartphones bringt Threema 4.71+ einen eignen **Threema Push Service** mit, der die Probleme für Privatsphäre und die mögliche Denonymisierung anonymer Threema Accounts durch Googles Push Service (FCM) vermeidet und den Akku Verbrauch nur wenig erhöht.

- Threema Push statt Google FCM kann man in den Einstellungen unter *Über Threema > Fehlerbehebung > Threema Push benutzen* aktivieren. (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 Akku Betrieb für Threema die Option *nicht einschränken* aktivieren.

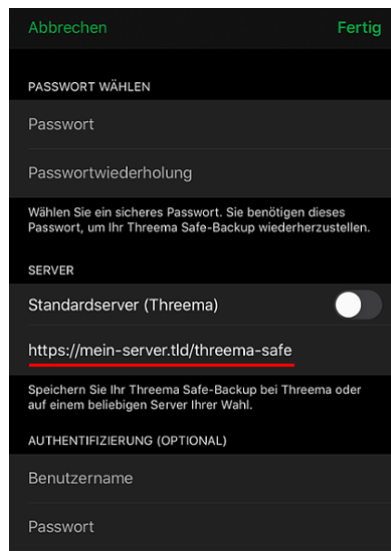


Abbildung 10.5: Eigenen WebDAV Server für Threema Backup auswählen

- Weitere Hinweise für spezielle Smartphonetypen finden man in den FAQ.²¹

Im Webshop²² von Threema kann man die App für Android Smartphones kaufen, wenn man keinen Google Play Store verwenden möchte.

Parallel zur Smartphone App kann man **Threema Desktop**²³ auf dem PC oder Laptop installieren, was nach dem Download relativ simple 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 die aktiven Desktop Clients verwalten.

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 außerdem fügt er 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, die jeweilige Gruppe zu verwenden, 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.

10.2.2 Messenger Signal App

Signal App ist kostenlos. Betrieb und Entwicklung werden von der Signal Foundation finanziert. Die Kapitaleinlagen der Fondation stammen u.a. von Brian Acton (105 Mio.

²¹https://threema.ch/de/faq/push_andr2

²²<https://shop.threema.ch/>

²³<https://threema.ch/de/download>

Dollar) und von der Shuttleworth Foundation. Der Quellcode ist bei Github verfügbar.²⁴

Signal App wird von Security-Experten aufgrund der guten Ende-zu-Ende Verschlüsselung empfohlen. Moxie Marlinspike entwickelte die Ende-zu-Ende Verschlüsselung, die inzwischen zum Quasi-Standard für KryptoMessenger wurde. Für die Forensikexperten von Elcomsoft und Cellbrite ist Signal *state of the art* unter den Messengern.

I'm not really into advertising for stuff here but the recent update of TextSecure made a gigantic impression on me. The application works well, is uber user friendly, and looks just great. (Collin R. Mulliner)

For the record - @moxie writes crypto software that blinds the #NSA & #GCHQ. He is their nightmare. Usable crypto developer with a backbone! (J. Appelbaum)

Für die Forensikexperten von Elcomsoft und Cellbrite ist Signal *state of the art*.

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).

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.

Dass Signal App die Telefonnummer als Identifier verwendet, wird oft kritisiert (Datensparsamkeit usw.) Dabei wird unterschlagen, dass die Verifizierung des Gegenüber anhand der Telefonnummer ein Sicherheitsfeature ist. Man kann sich relativ sicher sein kann, 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 Vorspielung einer falschen Identität Vertrauen erschleicht. Außerdem erleichtert es das Finden von Kontakten und Etablieren einer sicheren Kommunikation mit Freunden und Bekannten, was das Hauptziel von Signal App ist.

Signal bietet verschlüsselte **Audio- und Videotelefonie**. Videokonferenzen (Group Calls) mit bis zu 40 Teilnehmern sind möglich. Für eine Konferenz erstellt man eine Gruppe mit den Teilnehmern und tippt auf das *Group Call* Symbol (Abb. 10.6)

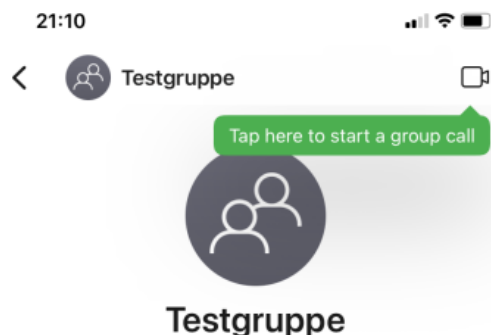


Abbildung 10.6: Videokonferenz mit bis zu 5 Personen starten

²⁴<https://github.com/WhisperSystems>

Für brisante Nachrichten, bei denen man verhindern möchte, dass Dritte sie durch Nachlässigkeit beim Umgang mit dem Smartphone zur Kenntnis nehmen könnten, bietet Signal App **selbstlöschende Nachrichten**. Wenn diese Option für einen Chat aktiviert wird, werden die danach geschriebenen Nachrichten eine einstellbare Zeit nach dem Lesen auf beiden Seiten automatisch gelöscht.

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 Privatsphäre. Wenn man nach neuen Kontakten sucht, werden die Hashwerte der Telefonnummern aus dem Adressbuch zu den Servern hochgeladen und dort niemals gespeichert. Ein Blogartikel erklärt das Verfahren.²⁵

Wenn man sein Smartphone verliert oder wechselt, dann verliert man auch alle Daten, die Signal App gespeichert hat. Es werden alle Daten nur lokal auf dem Smartphone gespeichert und nicht auf den Server. Deshalb braucht man ein Backup.

Das **Backup-Konzept** von Signal App ist dreistufig:

1. Das Adressbuch auf dem Smartphone dient als primäres Backup für den *Social Graph* (Liste der Kontakte). Mit einem Backup vom Adressbuch hat man sofort alle Kontakte in Signal wieder hergestellt (außer Gruppenchats). Signal ist primär ein Messenger für private Kontakte, deren Telefonnummern man im Adressbuch hat.
2. Optional kann man mit der Signal-PIN als zweite Backupstufe die Mitgliedschaften in Gruppen, Profilbild, 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 Blogartikel 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 alphanumerische Passphrase als PIN wählen.

Die Erinnerungsfunktion soll helfen, die PIN auswendig zu lernen. Wenn man die PIN in einem Passwortspeicher wie KeypassXC ablegt, braucht man es nicht.

Außerdem kann eine Registrierungssperre für die Übernahme des Account auf ein anderes Smartphone aktiviert werden. Nach Ansicht der Entwickler reichen 7 Tage aus, um alle Kontakt zu informieren, dass man einen neuen Account verwendet.

In den Einstellungen in der Sektion *Erweitert* kann man die PIN wieder deaktivieren.

3. 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 entspernte Smartphone eine Signal Desktop Instanz initialisiert, um die Kommunikation mitzulesen. (Das BKA hat einen vergleichbaren Angriff bei WhatsApp gegen einen Terrorverdächtigen bereits aktiv eingesetzt.)

²⁵<https://signal.org/blog/private-contact-discovery/>

- 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 über Signal Anrufe nicht in der Cloud von Google landen.

Signal App für Android verwendet keine Google Services für Push Notifications bei neu eintreffenden Nachrichten. Aus Sicht der Privatsphäre ist das erfreulich, bringt aber bei einigen Nutzern das Problem, dass sie keine Notifications bei neuen Nachrichten erhalten sondern immer in der App nachschauen müssen, ob es etwas Neues gibt. Um dieses Problem zu vermeiden, müssen folgende Voraussetzungen erfüllt sein:

- Signal App muss auch Hintergrund aktiv bleiben und sollte unter Android nicht durch Stromsparmaßnahmen abgeschossen werden. Bei einigen Android Smartphones muss man die Option *für Akku Betrieb nicht einschränken* aktivieren.
- Außerdem müssen für Signal App auf Android Smartphones *Hintergrundaktivität* und *Hintergrunddatenverkehr* erlaubt (aktiviert) sein.

Ein Support Artikel erläutert die Einstellungen für verschiedene Android Phones.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 App als Standard-SMS App (nur Android)

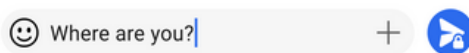
In der Studie *What Data Do The Google Dialer and Messages Apps On Android Send to Google?* vom Trinity College Dublin wurde analysiert, welche Daten die standardmäßig für SMS installierte Google Messaging App an Google sendet:

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.

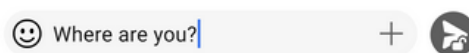
Statt Google Messaging kann man Signal zum Senden/Empfangen von SMS verwenden.

1. In den Einstellungen für das eigene Profil in Signal App aktiviert man dieses Feature unter *Unterhaltungen - SMS und MMS - Als Standard-SMS App verwenden*
2. In den Signal Kontakten werden alle Kontakte aus dem Adressbuch angezeigt und nicht nur Signal Kontakte. In den Unterhaltungen sieht man den Unterschied am *Senden* Button.

- Nachricht wird via Signal verschlüsselt gesendet: **blauer** Senden-Button

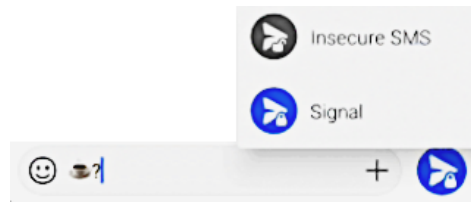


- Nachricht wird unverschlüsselt via SMS geschickt: **grauer** Senden-Button



- Man kann auch an einen Signal-Kontakt eine SMS senden, indem man lange auf den blauen Senden-Button drückt und in dem aufklappenden Menü den unverschlüsselten SMS Versand wählt. (Keine Ahnung, warum man das tun sollte, aber möglich wäre es.)

²⁶<https://support.signal.org/hc/de/articles/360007318711-Problembeseitigung-bei-Benachrichtigungen>



Signal-Desktop installieren und verwenden

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.

Installation

- Für **Windows** gibt es auf der Download Seite²⁷ 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. Als erstes ist der Signaturschlüssel des Repositories in den APT-Keyring einzufügen und das Repository als Paketquelle anzulegen. Dann kann man sie Anwendung signal-desktop installieren:

```
> sudo su
# curl -s https://updates.signal.org/desktop/apt/keys.asc | apt-key add -

# echo "deb [arch=amd64] https://updates.signal.org/desktop/apt xenial main" > \
/etc/apt/sources.list.d/signal-xenial.list

# apt update
# apt install signal-desktop
# exit
```

- Für alle anderen **Linux** Systeme gibt es ein Snap-Paket, das neben Signal-Desktop auch alle notwendigen Bibliotheken enthält. Um dieses Pake zu nutzen, muss man zuerst Snap installieren (falls nicht vorhanden) und den Rechner neu starten.

Für Fedora Nutzer erledigen das die folgenden Befehle:

```
> sudo dnf install snapd
> sudo ln -s /var/lib/snapd/snap /snap
```

Nach dem Neustart kann man das Snap-Paket signal-desktop installieren:

```
> sudo snap install signal-desktop
```

Signal-Desktop verwenden

Beim ersten Start von Signal-Desktop zeigt das Hauptfenster einen QR-Code, den man mit der Signal App auf dem Smartphone 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 Angreifer aber auch mehr Möglichkeiten.

Man muss die Signal App auf dem Smartphone öffnen, in den *Einstellungen* den Menüpunkt *Gekoppelte Geräte* öffnen und ein Gerät hinzufügen. Mit der Kamera scannt man den

²⁷<https://signal.org/de/download/>

QRCode, um Signal-Desktop mit dem Account auf dem Smartphone zu verbinden.

Nach dem Scan des QRCode fragt das Smartphone nach der PIN für die Registrierungssperre, die man hoffentlich in den Datenschutzeinstellungen aktiviert hat.

Anschließend gibt man dem Signal-Desktop noch einen Namen. Unter diesem Namen wird die Desktop App in der Liste der *Gekoppelte Geräte* auf dem Smartphone angezeigt. Hier kann man ein Gerät auch wieder rauswerfen, wenn man es nicht mehr verwendet.

Dann kann man Signal parallel auf dem Desktop und dem Smartphone nutzen. Das Hauptfenster (Abb: 10.7) ist spartanisch und bietet nicht alle Funktionen wie auf dem Smartphone. Man kann chatten, Dateien senden oder verschlüsselt telefonieren. Als erstes könnte man an als Test sich selbst eine kleine Nachricht schicken.

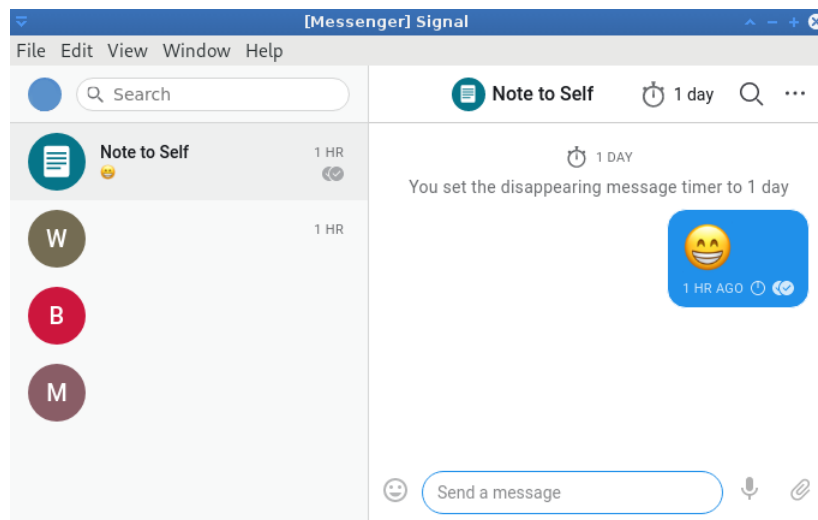


Abbildung 10.7: Hauptfenster von Signal-Desktop

Daten löschen, wenn der Account nicht mehr auf dem PC verwendet wird

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 dicken roten Button die Möglichkeit, diese Daten sicher zu entfernen.

10.2.3 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.

Telegram ist kostenlos nutzbar. Entwicklung und Betrieb wurden bisher aus dem Vermögen von Pavel Durov finanziert. Aber das Vermögen von P. Durov ist nicht unendlich und ab 2021 wird Telegram versuchen, eigene Einnahmen zu erwirtschaften, um die Unabhängigkeit zu sichern. Es soll eine eigene Werbeplattform aufgebaut werden und für die Einblendung von Werbung in öffentlichen Kanälen genutzt werden (private Kommunikation wird werbefrei bleiben). Die Werbung soll Content-sensitiv sein und nicht auf Usertracking basieren. Die Betreiber der Kanäle sollen als Content Ersteller in fairer Weise an den Werbeeinnahmen beteiligt werden.

Die **Registrierung** erfolgt mit einer Telefonnummer und erfordert ein Smartphone. Standardmäßig werden Chats und Gruppenchats nicht Ende-zu-Ende verschlüsselt und Telegram arbeitet als Cloud Messenger. Die Nachrichten liegen auf den Telegram Servern. Der Betreiber hat Zugriff auf die Chat History und kann Anfragen von Behörden beantworten. Telegram verkauft es als Privacy Feature, dass Anfragen aus einigen Ländern ignoriert werden, aber darauf kann man sich nicht verlassen.

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 Smartphone 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...

Nach der Registrierung kann man ein **Pseudonym** erstellen und muss nur dieses Pseudonym an Kommunikationspartner weitergeben. Die Zuordnung des Pseudonyms zum Account bzw. zur Telefonnummer wird auf den Telegram Servern gespeichert. Im Gegensatz zu Threema bietet ein Pseudonym keine Anonymität gegenüber dem Betreiber.

In den Einstellungen zur Privatsphäre kann man die **Anzeige der eigenen Telefonnummer** beim Gegenüber verbieten. Das schützt gegen Stalking auf anderen Kanälen und kann ein bisschen Anonymität gegenüber Kommunikationspartnern oder in Gruppenchats bieten. Da Telegram bei Terrorismusverdacht mit Behörden kooperiert, ist ein Pseudonym kein Sicherheitsfeature für politische 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.

Wenn der Angreifer eine Vermutung hat, zu welcher Gruppe von Personen ein Pseudonym gehört, könnte er bis zu 1.000 Telefonnummern im Adressbuch eingeben. Wenn die Telefonnummer im Adressbuch steht, wird sie auch in Chats unter dem Pseudonym angezeigt und über die Adressbuch-API kann der Angreifer den Namen herausfinden (s.o.)

Den Zugriff auf das **Adressbuch** zum Finden von neuen Kontakten kann unter *Privatsphäre - Dateneinstellungen* deaktiviert werden und das 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 Dez. 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 Panyayev* 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. Es wurden bereits mehrfach staatliche Angriffe nachgewiesen, welche die Multi-Device Unterstützung ausnutzten, um unbemerkt Chats mitzulesen, die nicht Ende-zu-Ende verschlüsselt waren. 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.

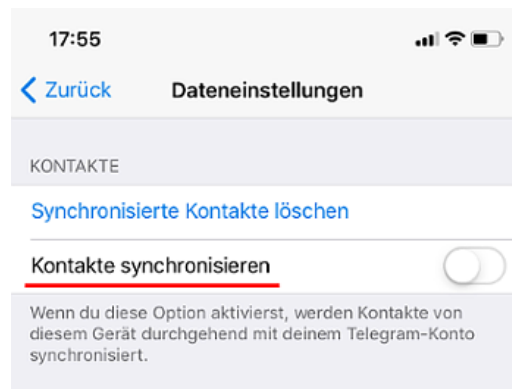


Abbildung 10.8: Deaktivierung des Upload der Kontakte in Telegram



Abbildung 10.9: Zweistufige Bestätigung für neue Geräte aktivieren

Features von Telegram

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*.

Diese *geheimen Chats* werden nicht in der Cloud gespeichert sondern nur auf dem Smartphone (unverschlüsselt). Diese Verhalten ist als *Mannings Bug* bekannt und ein Security Bug, da ein Angreifer mit physischem Zugriff auf das Smartphone die *geheimen Chats* auslesen kann. Elcomsoft oder Cellbrite liefern die nötigen Tools.

Für besonders brisante geheime Chats bietet Telegram *selbstlöschende Nachrichten*, die nach einer einstellbaren Zeit nach dem Lesen gelöscht werden.

Audio- und Videotelefonie in 1:1 Chats ist immer Ende-zu-Ende verschlüsselt. Zur Verifizierung der Verschlüsselung werden oben rechts vier Emojis angezeigt. Wenn beide Seiten die gleichen Emojis sehen, ist die Verschlüsselung sicher.

Telegram Gruppen können bis zu 200.000 Mitglieder enthalten. Teilnehmer mit Admin Status können mit einem Klick ein 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.

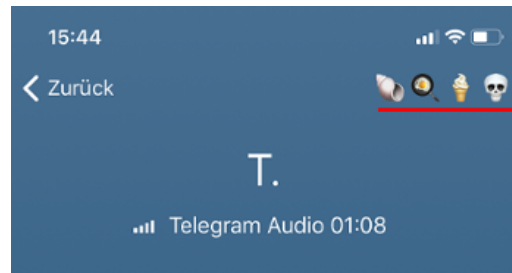


Abbildung 10.10: Verifizierung der Verschlüsselung für Audio- und Videotelefonie

Hinweis: 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 besondern Social Media Features des Messengers. Man kann diese Kanäle nutzen, um einem breiten Publikum seine Meinung vorstellen oder um Millionen Follower bei Protesten zu informieren ohne eine Beschränkung auf 200 Zeichen.

Kanäle können neben Text, Bildern und Videos auch Audiostreaming senden, so dass man eine 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.

- 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 privacy-freundlich konfigurieren, um die Tracking Parameter zu entfernen.
- Außerdem nutzen rechtsextreme Gruppen und viele Anhänger von Verschwörungstheorien dieses Medium, nachdem sie bei Facebook und Twitter wegen Verbreitung von Hass oder Fake News rausgeflogen sind.

Für die steigende Verbreitung der Telegram Kanäle als Social Media Tool zur Mobilisierung von (mehr oder weniger großen) Massen gibt es mehrere Gründe. Einerseits wird Telegram von Mio. 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. Es 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 Jan. 2021 wurden beispielsweise 19.672 Kanäle und Bots gesperrt, im Dez. 2021 waren es 23.082. Zahlen über gesperrte Kanäle werden vom *isiswatch bot* publiziert.²⁸

Europol vertritt die Einschätzung (2018), dass Telegram sich erfolgreich bemüht, Terror- und Hasspropaganda sowie Aufrufe zu Straftaten zu entfernen.²⁹

Telegram is no place for violence, criminal activity and abusers. The company has put forth considerable effort to root out the abusers of the platform by both bolstering its technical capacity in countering malicious content and establishing close partnerships with international organisations such as Europol.

Wenn man (zufällig) illegale Inhalte findet, kann man sie mit wenigen Klicks an das Telegram Abuse Team melden. Man öffnet die Channel Einstellungen und klickt auf *mehr*, dann auf *melden* und kann dann angeben, warum man den Kanal meldet.

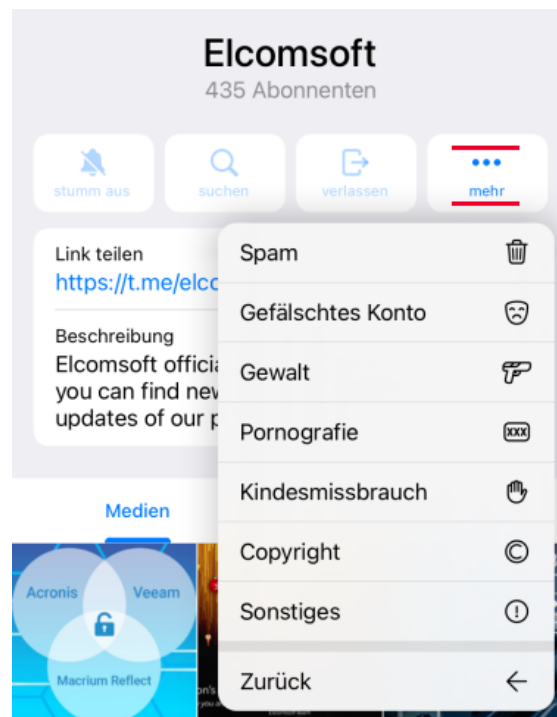


Abbildung 10.11: Illegale Inhalte bei Telegram melden

2. Google und Apple haben bei den Telegram Apps, die aus dem Play Store oder App Store 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:



Außerdem werden von Google und Apple Telegram Kanäle und Gruppen in den Smartphones Apps gesperrt, die als Fake News o.ä. klassifiziert werden aber von Telegram als freie Meinungsäußerung eingestuft und nicht gelöscht werden.

Um diese Sperren in den Smartphone Apps zu umgehen, gibt es Möglichkeiten:

²⁸<https://t.me/s/isiswatch>

²⁹<https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online>

- Für Android Smartphones gibt es Telegram FOSS³⁰ im F-Droid Store und auf der Telegram Webseite ein APK³¹ 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.³²
 - 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 verletzen, für die Nutzer mit einer Telefonnummer, die mit der jeweiligen Landeskenntung beginnt. Diese Sperrungen sind seit Feb. 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 des veganen Kochs 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 sondern... (Wir hatten die Diskussion vor 10 Jahren bei DNS-Sperren gegen Kipo.)
4. Vollständige Blockade von Telegram gibt es bisher nur in echten Diktaturen wie Iran, Saudi Arabien oder China. Unseren Bundesinnenministerin spielt auch mit dem Gedanken, Telegram staatlich zu blockieren, was die Reichweite des Messenger fraglos etwas einschränken könnte aber aus mehreren Gründe 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.
In Ländern wie Iran, Weißrussland oder China wird die notwendige technische Infrastruktur staatlich betrieben und nicht von den ISPs bereitgestellt.
In der EU gibt es bisher keine vergleichbaren Strukturen wie die Great Firewall von China oder wie die Kontrolle des Übergangs in das internationale Internet durch wenige staatliche Knotenpunkte im Iran.

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 *Daten und Speicher - Proxy*. Eine Liste von MTProxys kann man z.B. im Telegram Kanal MTProtoProxies³³, den man auch im Browser öffnen kann.

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 Gruppen bieten fliegende Händler oft Waren an, die sonst schwer zu bekommen sind.)

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 gehen und nach links) kann man den Standort interpolieren. Für Heise ist das ein Security Bug³⁴ 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.

³⁰<https://f-droid.org/de/packages/org.telegram.messenger>

³¹<https://telegram.org/android>

³²<https://desktop.telegram.org/>

³³<https://t.me/s/MTProtoProxies>

³⁴<https://heise.de/-5004687>

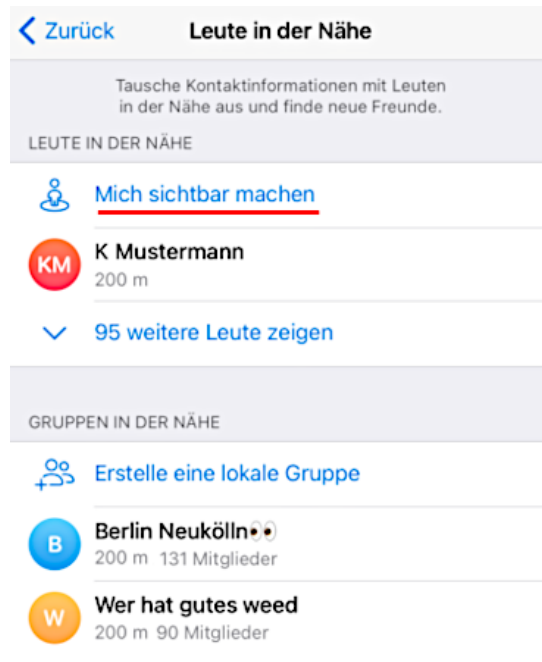
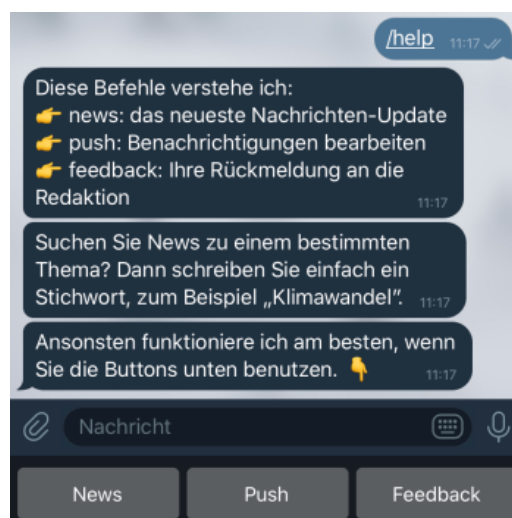


Abbildung 10.12: Personen und Gruppen in der Umgebung suchen

Telegram Bots sind ein weiteres, populäres Feature des Messengers. Ein Bot ist ein Chatpartner, der auf simple Kommando 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 man 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 dass 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 (beispw. Tor Onion Services), da ein zentraler Ansprechpartner als Betreiber existiert, der unter Umständen auch mit der Strafverfolgung kooperiert. Im Okt. 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 letzte Schritt wäre ohne Kooperation des Betreibers nicht möglich.

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:

Please [install Telegram](#) to use this option

 Sign up with Telegram

or

Email

10.2.4 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 (früher: Riot) die größte Verbreitung hat.

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. Über Identitätsserver kann man den Account auf Wunsch mit einer Telefonnummer oder E-Mail Adresse verbinden, so dass man leichter gefunden wird. Meistens wird der Server *vector.im* verwendet, der damit eine zentrale Funktion übernimmt.

Zentrales Konzept beim Chatten via [matrix] sind die *Räume*. Man kann sich auf seinem Homeserver neue *Räume* einrichten und dort erstmal 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 Rechte vergeben, wer administrieren darf, wer neue Mitglieder einladen darf usw.

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 Kontaklisten, 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*) haben auch Behörden im Rahmen von Auskunftsersuchen darauf Zugriff. Mit Umsetzung des im Dez. 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 Metadaten der Kommunikation für die Kommunikationsanalyse abgerufen werden. (Wer, wie häufig, mit wem...?)

Nach der Rechtssprechung 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 von Matrix weist aber darauf hin, dass damit nur ein Wunsch des Nutzers zum Ausdruck gebracht wird. Es kann nicht sichergestellt werden, dass die anderen Server diesen Wunsch auch befolgen.

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.

Im F-Droid Store gibt es eine Google-freie Version von Riot 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 der Häufigkeit der Aktualisierung und Energieverbrauch konfigurieren.

Hinsichtlich Sicherheit könnte man noch anmerken, dass Certificate Pining als Schutzmaßnahme gegen Man-in-the-Middle Angriffe auf die TLS Verschlüsselung 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 ist der Riot damit weiterhin anfällig für Angriffe, die 2009 in der wiss. Arbeit *Certified Lies - Detecting and Defeating Government Interception Attacks against SSL* beschrieben wurden.

Die Ende-zu-Ende Verschlüsselung ist Teil des Sicherheitskonzeptes von [matrix] und standardmäßig aktiviert. Für eine hohe Sicherheitsansprüche gibt es folgende Optionen:

1. Verifikation 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 Emoji, 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 herunter laden und lokal speichern. Die Signaturschlüssel werden verwendet, um eigene, neue Geräte zu signieren und das in die Vertrauensbasis bestehender Verifikationen einzuschließen.

Verifizierte Kommunikationspartner müssen nicht mehr jedes einzelne Gerät verifizieren, wenn man Cross-Signing aktiviert. 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.

Neben den Smartphone Clients, deren Krypto-Implementierung jemand im Rahmen eines Audits nach Vorliegen der finalen Version untersuchen könnte, gibt es eine Browserversion als Desktop Client oder für den Einsatz auf einem Webserver. Aufgrund konzeptueller Schwächen kann man bereits ohne Prüfung der finalen Version sagen, dass eine Webversion nicht für hohe Sicherheitsansprüche geeignet ist:

- Das 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.³⁵
- riot-web speichert die privaten kryptografischen Schlüssel für die Ende-zu-Ende Verschlüsselung im HTML5 Storage des Browsers. Im *HTML5 Security Cheat Sheet*³⁶ wird vom OWASP empfohlen, keine sensiblen Informationen im HTML5 Storage zu speichern, da es kein sicherer Speicher ist und diese Daten leicht kompromittiert werden könnten, beispielsweise z. B. 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.

10.2.5 Chatten mit Jabber/XMPP

Jabber/XMPP hat mich und andere Nerds seit vielen Jahren begleitet. Die Software ist OpenSource und ein weltweites Netz von tausenden Servern stellt sicher, dass Jabber nicht juristisch durch gesetzliche Vorgaben kompromittiert werden kann. Übergriffe auf die Privatsphäre durch Datendiebstahl (z.B. Adressbücher) hat es bei Jabber/XMPP nie gegeben und der Account kann frei gewählt werden, unabhängig von Telefonnummern.

Bei der Ende-zu-Ende Verschlüsselung gibt es mehrere Alternativen:

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 bei der Verschlüsselung von E-Mail behandelt. Die Erstellung und 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.

³⁵http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/

³⁶https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html

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 HTTPUpload. 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 Sicherheitsfeature 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 die Nachteile bezüglich Sicherheit zu erwähnen.

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 Verschlüsselung zu verhindern, bereits 2009 in der wiss. Arbeit *Certified Lies - Detecting and Defeating Government Interception Attacks against SSL* beschrieben wurden.

Threema und Signal App nutzen CA-Pinning, um diese Angriffe zu verhindern.

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 Client 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.)

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. Die im Rahmen des *Gesetzesentwurfes zur Bekämpfung von Rechtsterrorismus und Hasskriminalität* vorgelegten Anpassungen am Telemediengesetz sollen es jedem Dorfpolizisten ohne richterliche Prüfung erlauben, diese Daten abzurufen.

Bei Threema und Signal App werden diese Daten ausschließlich auf den Clients gespeichert. Die Server Betreiber haben keine Informationen über Kontaktlisten, Mitgliedschaften in Gruppenchats, Profilfotos o.ä. Das schränkt die Flexibilität bei der Verwendung unterschiedlicher Geräte ein zugunsten der Sicherheit.

3. Signal App und Threema haben ein Sicherheitskonzept, bei dem die Ende-zu-Ende Verschlüsselung der gesamten Kommunikation inkl. Audio- und Videotelefonie sowie 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

Implentierung von OTR in Jabber Client Gajim war nach 15 Jahren noch immer experimentell und wurde dann zugunsten von OMEMO ganz fallen gelassen.

- Teilweise sind die Standards selbst unvollständig und umfassen nicht die Verschlüsselung des gesamten möglichen Datenaustausch zwischen zwei oder mehreren Nutzen, 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.
 - Teilweise liegt es auch an mangelnder konzeptueller Vorarbeit. Es wird einfach erstmal 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 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, dass 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 Verifikation von Schlüsseln eingeführt, die den Multi-Device Support (ursprünglich ein Killerfeature von OMEMO) wieder einschränkt. (Ob die gegenseitige Verifikation der Fingerprints der Schlüssel für eine größere Gruppe von Nicht-IT-Nerds praktisch umsetzbar ist - naja. . .)

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.

Man sollte daraus nicht die Schlussfolgerung ziehen, dass XMPP unbrauchbar ist. 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 förderale Strukturen bestehen, ohne die Mängel in der Kryptografie einzugestehen.

10.2.6 Messenger Wire

Wire ist in erster Linie eine gute Collaboration Plattform für Unternehmen. Das in Berlin arbeitenden Entwicklerteam gehört zur Wire Swiss GmbH, die die Server der Infrastruktur betreut und eine Tochterfirma der Wire Group Holdings GmbH in München (DE) ist.

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 Geräte 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 25 Teilnehmern 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 Whitepaper³⁷ von Wire ausdrücklich nicht vorgesehen.

Das Whitepaper postuliert, dass unter Android der Schutzwall gegen Zugriffe auf die gespeicherten Daten durch anderen Apps ausreichend ist, und empfiehlt auf PCs und

³⁷<https://wire-docs.wire.com/download/Wire+Security+Whitepaper.pdf>

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 keine Hinweis, 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 Versprechungen auf förderale Infrastruktur der Server wurden auf unbekannte Zeit verschoben und Vorteile gegenüber WhatsApp sind gering. Als Argument könnte man anerkennen, das die Adressbücher nicht an Datensammler weitergegeben werden.

Wire Enterprise ist der bevorzugte Messenger der Bundesregierung und vom BSI für VS-NfD zugelassen. Wire ist eine gute Collaboration Plattform für Unternehmen.

10.2.7 Einige weitere Messenger (unvollständig)

WhatsApp ist mit 2 Mrd. Nutzern weltweit der populärste Messenger. Es folgen der Facebook Messenger mit 1,3 Mrd. Nutzern und WeChat mit 1,2 Mrd. auf den Plätzen. Telegram und Signal App sind unter den Top10 und Threema ist unter den Top20 (Stand Okt. 2020). Die Verteilung der Messengernutzung in Deutschland zeigt Abb. 10.13 (Stand: Nov. 2019).

Facebook Messenger ist keine Alternative zu WhatsApp. Man kann zwar eine Ende-zu-Ende Verschlüsselung aktivieren, aber trotzdem kann Facebook bei Bedarf die verschlüsselten Chats mitlesen. Dabei wird nicht die Krypto gebrochen sondern auf Anforderung eine unverschlüsselte Kopie der Nachricht an Facebook gesendet.

Delta-Chat vergewaltigt 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 *E-Mail Verschlüsselung mit OpenPGP* 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 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 förderale 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 privacy-freundlichen E-Mail Provider nutzt, ist man nicht gegen das Mitlesen nicht geschützt, weil:

Google has most of my emails, because it has all of yours.



Abbildung 10.13: Nutzung der Messenger in Deutschland (2019)

- 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 Mail Providern.

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.

10.3 Videokonferenzen mit Jitsi Meet und BigBlueButton

Für die Teilnahme an einer Videokonferenz benötigt man neben dem Link zur Webkonferenz, evtl. ein Passwort nur einen Webbrowser, der nicht zu restriktiv konfiguriert ist. Die wenigsten Probleme soll es mit dem Google Chrome Browser oder Chromium geben. Die Verwendung von Firefox ist aber auch möglich.

- Die Verwendung von WebRTC muss möglich sein und der OpenH264 Codec muss zur Verfügung stehen, was nicht bei allen Firefoxen Standard ist.
- 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 beispw. *videokonferenz* genannt hat, kann man es direkt mit folgendem Kommando starten oder als ein Starter-Icon auf dem Desktop anlegen:

```
> firefox --profile <Path> -no-remote
```

BigBlueButton Videokonferenz Server

Die Universität Darmstadt bieten einen öffentlichen Konferenzserver³⁸ mit BigBlueButton, der mit Spenden finanziert wird und für Teilnehmer an einer Konferenz auch Telefoneinwahl anbietet. Registrierte Nutzer können sich auch permanente Konferenzräume³⁹ einrichten.

Jitsi Meet Videokonferenz Server

Es gibt viele öffentlich verfügbare Jitsi Meet Instanzen⁴⁰. Hier eine kleine Auswahl an Empfehlungen für Server, die von vertrauenswürdigen IT-Professionals betrieben werden und hinsichtlich Sicherheitsfeatures wie DNSSEC, moderne TLS Ciphern, Server Konfiguration und Aktualität der Software auf dem Stand der Technik sind:

1. Single Server Instanzen ermöglichen Konferenzen mit bis zu 8-10 Teilnehmern:
 - Jitsi Meet Server der Nitrokey GmbH: <https://meet.nitrokey.com>
 - Jitsi Meet Server von Golem.de: <https://meet.golem.de>
 - Jitsi Meet Server von M. Kuketz: <https://www.kuketz-meet.de>
2. Einige spenden-finanzierten Servercluster sind auch für größere Videokonferenzen mit 50-70 Teilnehmern geeignet:
 - Jitsi Cluster vom Freifunk München: <https://meet.ffmuc.net>
 - Jitsi Meet Server der Horizon44 GmbH: <https://sichere-videokonferenz.de/>
3. Kunden von mailbox.org können sich im Web-GUI zwei Videokonferenzen anlegen und bis zu 25 Teilnehmer einladen. Diese Konferenzen bleiben dauerhaft erhalten und können wiederverwendet werden. (Ab März 2021 nur in Tarifen ab 2,50 Euro.)

³⁸<https://public.senfcall.de/>

³⁹<https://lecture.senfcall.de/signin>

⁴⁰<https://github.com/jitsi/jitsi-meet/wiki/Jitsi-Meet-Instances>

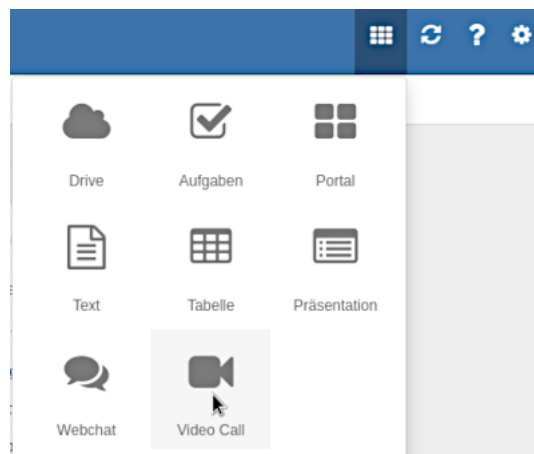


Abbildung 10.14: Videokonferenz beim mailbox.org starten

Kapitel 11

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...

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 Double-Click 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 Nutzung von Anonymisierungsdiensten identifiziert.

11.1 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 Avantar-Bildchens. Wenn man manche (besonders kreativen) Avantare der anonymen Teilnehmergruppen von Privacy-Foren durch eine inverse Bildersuche schickt und die Spuren weiter verfolgt, kann man in 10min den realen Namen finden, manchmal sogar den Wohnsitz...

2. Eve hat als Webmaster oder Hackerin Zugriff auf die Registrierungsdaten.

Anton schützt sich, indem er eine temporäre E-Mail Adresse oder einen E-Mail Alias exklusiv für die Registrierung des Accounts verwendet statt seiner realen E-Mail Adresse 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 Deanonmisierung anhand der IP-Adresse durch Auskünfte bei Telekommunikations Providern oder Korrelation mit Aktivitäten unter realem Namen (Einkäufe, Bankgeschäfte online usw.) zu verhindern, muss Anton sich ein bisschen mehr bemühen und für seine anonyme Aktivitäten mindestens ein VPN mit wechselnden Servern nutzen und zusätzlich ein separates Browserprofil.

4. Eve kann als potente (staatliche) Angreiferin einen erheblichen Teil des Internettraffic 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 führt. Unter Umständen reicht es aus, sein Smartphone im gleichen WLAN zu benutzen (Kevin D. Mitnick, Die Kunst der Anonymität) oder man wird von Metadaten in einem Fotos verraten (John McAfee, 2012).

Ein Student wollte beispw. 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.

11.2 Was können Anonymisierungsdienste wie Tor?

Anonymisierungsdienste verstecken die IP-Adresse des Nutzers und verschlüsseln die Kommunikation zwischen Nutzer und den Servern des Dienstes. Außerdem werden spezifischer Merkmale modifiziert, die den Nutzer identifizieren könnten (Browser-Typ, Betriebssystem....).

1. **Profilbildung:** Nahezu alle großen Suchmaschinen generieren Profile von Nutzern, Facebook u.a. Anbieter speichern die IP-Adressen für Auswertungen. Nutzt man Anonymisierungsdienste, ist es nicht möglich, diese Information sinnvoll auszuwerten.
2. **Standortbestimmung:** Die Anbietern von Webdiensten können den Standort des Nutzers nicht via Geolocation bestimmen. Damit ist es nicht möglich:
 - die Firma identifizieren, wenn der Nutzer in einem Firmennetz sitzt.
 - bei mobiler Nutzung des Internet Bewegungsprofile zu erstellen.
3. **Belauschen durch Dritte:** Die verschlüsselte der Kommunikation mit den Servern des Anonymisierungsdienstes verhindert ein Mitlesen des Datenverkehrs durch Dritte in unsicheren Netzen. (Cafes, WLANs am Flughafen oder im Hotel, TKÜV...)
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 unzensurierten Zugang zum Internet. Sie können sowohl die "Great Firewall" von China und Mauretanien durchtunneln sowie die in westeuropäischen Ländern verbreitet Zensur durch Kompromittierung des DNS-Systems.
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. Iran wertet Twitter-Accounts aus, um Dissidenten zu beobachten
7. **Leimruten:** Einige Websites werden immer wieder als Honeypot genutzt. Ein Beispiel sind die Leimrute des BKA. In mehr als 150 Fällen wurden die Fahndungseiten von LKAs oder des BKA als Honeypot genutzt und die Besucher der Webseiten in Ermittlungen einbezogen ¹. 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.

¹<http://heise.de/-1704448>

11.3 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 3 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.

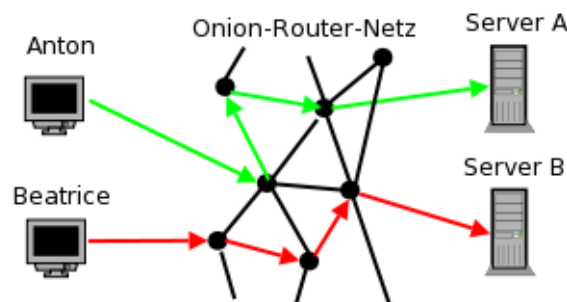


Abbildung 11.1: Das Prinzip von Tor Onion Router

Tor ist neben Surfen auch für IRC, Instant-Messaging, den Abruf von Mailboxen oder Anderes 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 mit zu nutzen.

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.²
- Auf der Black Hack 2009 wurde ein Angriff auf die HTTPS-Verschlüsselung beschrieben. In Webseiten wurden HTTPS-Links durch HTTP-Links ersetzt. Innerhalb von 24h konnten mit einen Tor Exit Node folgende Accounts erschnüffelt werden: 114x Yahoo, 50x GMail, 9x Paypal, 9x LinkedIn, 3x Facebook.³

2012 haben mehrere russische Extis-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)* einen schnüffelnden Tor Exit Node, um private Informationen von Google Nutzern zu gewinnen.⁴

²<http://heise.de/-95770>

³<http://blog.internetnews.com/skerner/2009/02/black-hat-hacking-ssl-with-ssl.html>

⁴<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 6 modifizierte Tor Nodes genutzt und innerhalb von 23 Tagen mehr als 10.000 User deanonymisiert.⁵

Man kann davon auszugehen, dass die Geheimdienste verschiedener Länder ebenfalls im Tor-Netz aktiv sind und sollte die Hinweise zur Sicherheit beachten: sensible Daten nur über SSL-verschlüsselte Verbindungen übertragen, Warnungen nicht wegklicken, Cookies und JavaScript deaktivieren. ... 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 an der Finanzierung durch die US-Regierung und erst durch diese langjährige Finanzierung durch das US-Verteidigungsministerium, US-State-Department, Broadcasting Board of Governors (BBG ist ein Spin-Off der CIA, das auch Medien wie Voice of America, Radio Free Europe oder Radio Liberty beaufsichtigt) und andere US-Behörden konnte das Projekt zum erfolgreichen, größten Anonymisierungsprojekt werden.⁶

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 normal 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.

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.

⁵<http://hal.inria.fr/inria-00574178/en/>

⁶<https://surveillancevalley.com/blog/fact-checking-the-tor-projects-government-ties>

2. Kriminelle nutzen in großen 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 Bild 11.2 sehen kann.

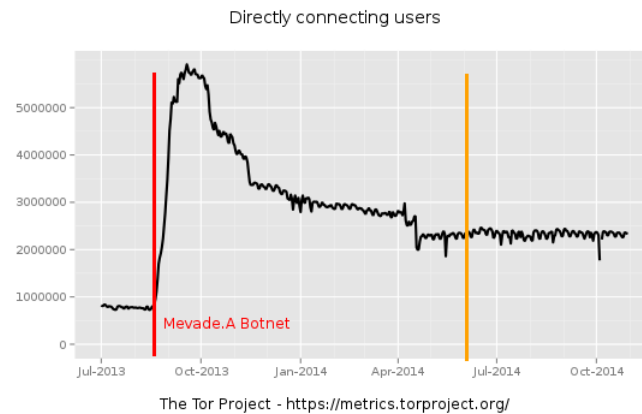


Abbildung 11.2: Mevada.A Botnetz von metrics.torproject.org

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 abgeschaltet werden. Das FBI hatte dabei technische Unterstützung von der Carnegie Mellon University 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 erheblichen 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 beispielsweise ein Botnetz in Russland hochgefahren, dass der russischen Gegenseite ernsthafte Probleme bereitet hat. In Bild 11.3 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 veröffentlichte FOIA Dokumente belegen, das insbesondere die CIA Tor Onion Router aktiv als Werkzeug bei Kampagnen zur Destabilisierung unbequemer Länder nutzt:

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 Europäische Menschenrechtskonvention deklarierte Recht auf unbeobachtet, private Kommunikation ist durch die staatlich organisierte Massenüberwachung und kommerzielle Datensammlungen praktisch abgeschafft. Bundesinnenminister Friedrich empfiehlt Selbstschutz, weil die technischen Möglichkeiten zur Ausspähung nun einmal existieren (die Bankrotterklärung der Politik), und Tor ist ein Technik zum Selbstschutz.

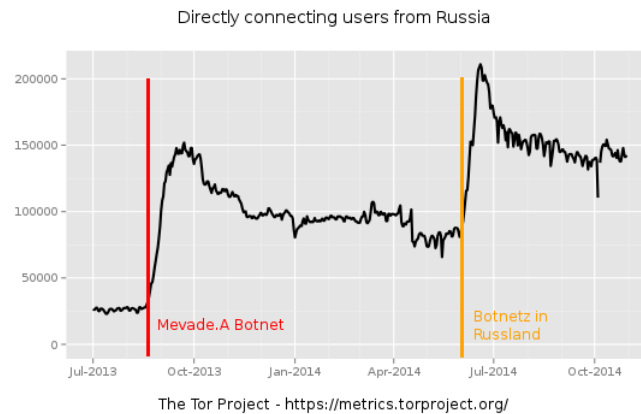


Abbildung 11.3: Botnetze mit Tor in Russland von metrics.torproject.org

2. Kriminalität wie Wirtschaftskriminalität, Eigentumsdelikte, Drogenkriminalität... oder ganz allgm. *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 Brauchbarkeit als Waffe geprüft. Tor war von Anfang 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 University 1 Mio. Dollar zur Verfügung stellt, um Tor Onion Services für die Operation Onymous zu deanonymisieren⁷, die Universität die wiss. Ergebnisse auf der BlackHat Konferenz aber nicht publizieren darf⁸, um die US-Cyberoperationen in Russland nicht zu gefährden, und die Entwickler bei TorProject.org auf Vermutungen angewiesen sind⁹, um die Bugs zu fixen, damit sie politischen Aktivisten wie Wikileaks eine vertrauenswürdige Infrastruktur bereit stellen können.

11.3.1 Security Notes

Die Sicherheit von IP-Anonymisierern wie Tor Onion Router ergibt sich nicht alleine aus der Qualität der Software und der Kryptografie. Durch Fehler bei der Nutzung oder durch falsche Konfiguration kann die Anonymität komplett ausgehebelt werden.

- Wer in seinem Standardbrowser nur die Proxy-Einstellungen anpasst um Tor zu verwenden, ist auch nicht sicher anonym. Eine Deanonymisierung ist mit WebRTC oder Java-Applets 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 und via UPnP Protokoll wird versucht, einen direkten Tunnel durch den Router zu bohren. Mit einem Audio- oder Videoanruf kann man also deanonymisiert werden.

⁷<https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users>

⁸<https://web.archive.org/web/20140705114447/http://blackhat.com/us-14/briefings.html>

⁹<https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/>

- 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 wiss. Arbeit zeigte, wie 10.000 BitTorrent Nutzer via Tor deanomisiert werden konnten.
- Der Assistent zur Einrichtung eines E-Mail Account in Thunderbird umgeht die Proxyeinstellungen 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.
- Durch Software aus fragwürdigen Quellen können Backdoors zur Deanonymisierung geöffnet werden. Eine Gruppe von ANONYMOUS demonstrierte es, indem sie eine modifizierte Version des Firefox Add-on TorButton zum Download anboten, dass wirklich von einigen Tor-Nutzern verwendet wurde. 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 Herbst 2011 im Internet veröffentlicht.

Schlussfolgerungen:

- TorProject empfiehlt für anonymes Surfen ausdrücklich das TorBrowserBundle. Das ist eine angepasste Version des Browser Mozilla Firefox zusammen mit dem Tor Daemon. Nur diese Konfiguration kann als wirklich sicher nach dem aktuellen Stand der Technik gelten. Die vielen Sicherheitseinstellungen dieser Softwarekombination kann man nur unvollständig selbst 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.

11.3.2 Anonym Surfen mit dem TorBrowserBundle

Das TorBrowserBundle enthält einen modifizierten Firefox als Browser sowie den Tor Daemon und ein Control Panel. Die Webseite stellt das TorBrowserBundle für verschiedene Betriebssysteme und in unterschiedlichen Sprachen zur Verfügung.

HINWEIS: man sollte die **englische Version des TorBrowsers (en-US)** herunter zu laden. In den letzten Jahren gab es immer wieder aufgrund von Bugs im TBB die Möglichkeit, Hinweise auf die Lokalisierung des Browser zu finden, z. B via Javascript `date.toLocale()` Funktion (Bug #5926) oder via Informationen aus dem HTTP Accept-Language Header (Bug #628) oder via `ressource://` URI (Bug #8725). Wenn man die deutsch lokalisierte Version des TorBrowsers nutzt, gibt man möglicherweise einen Hinweis auf die bevorzugte Sprache, und das möchte man natürlich vermeiden.

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. Für den produktiven Einsatz sollte man nur die stabile Version zu nutzen und warten, bis die Entwickler die neuen Features als ausreichend getestet einstufen und in die stabile Version 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 zu entpacken, keine Installation nötig.

- Unter Windows öffnet man nach dem Download das selbstentpackende Archiv mit einem Doppelklick im Dateimanager und wählt ein Zielverzeichnis. Nach dem Entpacken startet man alle Komponenten mit einem Doppelklick auf **Start Tor Browser.exe** im Dateimanager.
- Unter Linux entpackt man das Archiv mit dem bevorzugten Archiv-Manager oder erledigt es auf der Kommandozeile mit:

```
> tar -xaf tor-browser-*
```

Danach kann man das TorBrowserBundle starten, indem man das Startscript auf der Kommandozeile aufruft oder mit einem Klick im Dateimanager startet:

```
> tor-browser_en-US/start-tor-browser.desktop
```

Mit einem kleinen Kommando kann man den TorBrowser im Startmenü des Desktops in der Programmgruppe *Internet* hinzufügen, um den Start zu vereinfachen:

```
> tor-browser_en-US/start-tor-browser.desktop --register-app
```

- Für Debian und Ubuntu Derivate gibt es außerdem den *TorBrowser Launcher*, der sich um Download, Verifikation und Installation des TorBrowserBundles kümmert. Das Paket kann man mit dem bevorzugten Paketmanager installieren:

```
> sudo apt install torbrowser-launcher
```

In der Regel wird auch gleich ein Tor Daemon installiert. Diesen Tor Daemon braucht man evtl. nur für den ersten, initialen Download des TorBrowserBundle. Es ist aber kein Sicherheitsgewinn, wenn man das TorBrowserBundle via Tor herunter lädt und man kann diesen Tor Daemon gleich wieder entfernen, da das TorBrowserBundle eine aktuellere Version von Tor enthält.

```
> sudo apt purge tor
```

In der Programmgruppe *Internet* findet man zwei neue Menüpunkte. Wenn man den Menüpunkt *TorBrowser Launcher Settings* wählt, öffnet sich das in Bild 11.4 gezeigte Fenster. Den *Download over System Tor* kann man deaktivieren, man sollte die engli-

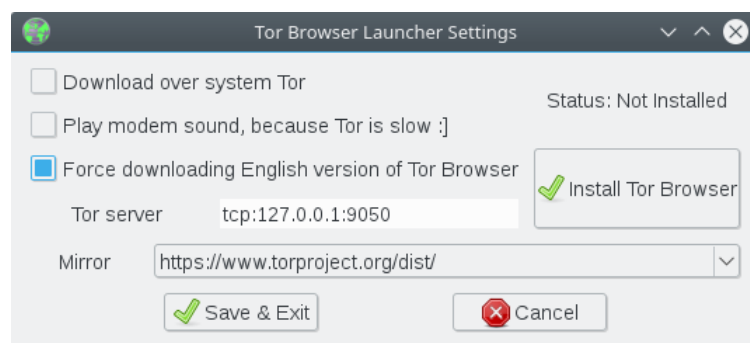


Abbildung 11.4: Start des TorBrowser

sche Version des TorBrowsers herunterladen und außerdem kann man einen Mirror wählen, falls die Webseite von TorProject.org nicht erreichbar ist. Ein Klick auf den *Install Button* lädt das TorBrowserBundle herunter, verifiziert die OpenPGP Signatur und installiert den TorBrowser. Zum Starten verwendet man zukünftig den Menüpunkt *TorBrowser* in der Programmgruppe *Internet*.

Wenn die Downloadseite für das TorBrowserBundle gesperrt ist, dann findet man unter GetTor¹⁰ alternative Downloadmöglichkeiten. Man kann z.B. per Jabber/XMPP oder E-Mail eine Nachricht mit dem gewünschten Betriebssystem (windows, linux, osx) an den Account gettor@torproject.org schicken und bekommt eine Liste alternativer Downloadlinks.

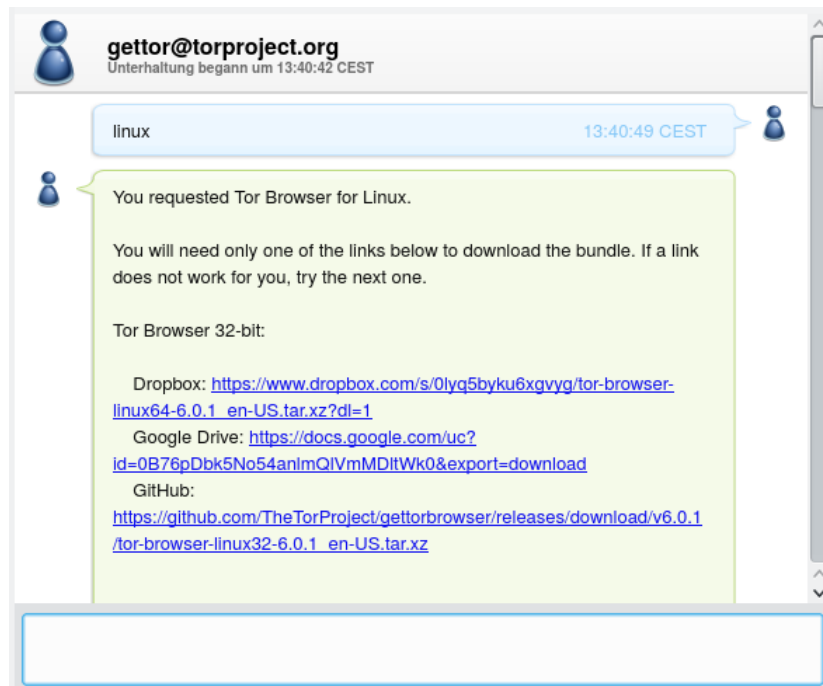


Abbildung 11.5: Alternative Downloadlinks via Jabber/XMPP abrufen

Beim ersten Start öffnet sich zuerst das Control Panel. Hier kann man bei Problemen Einstellungen zur Umgehung von Firewalls konfigurieren (z.B. wenn eine Firewall nur Verbindungen zu bestimmten Ports passieren lässt) oder man kann den Tor Daemon mit Klick auf den Button *Verbinde* ohne weitere Konfiguration starten.

Größe des Browserfensters

Der TorBrowser startet mit einer festgelegten Größe des Browserfensters. Die Fensterbreite sollte ein Vielfaches von 200px sein (max. 1000px) und die Höhe ein Vielfaches von 100px. 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 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*¹¹ erlaubt seit Dez. 2016 dem FBI das massenweise Hacken von Tor- und VPN-Nutzern unabhängig davon, in welchem Land die Tor-Nutzer sich befinden.

1. 2016 wurde auf der Tor Mailingliste¹² ein Javascript Bug gepostet, den das FBI aktiv mit Exploits ausnutzte, um einen Trojaner zu installieren, der Tor Nutzer deanonym-

¹⁰<https://gettor.torproject.org/>

¹¹<https://blog.torproject.org/blog/day-action-stop-changes-rule-41>

¹²<https://lists.torproject.org/pipermail/tor-talk/2016-November/042639.html>

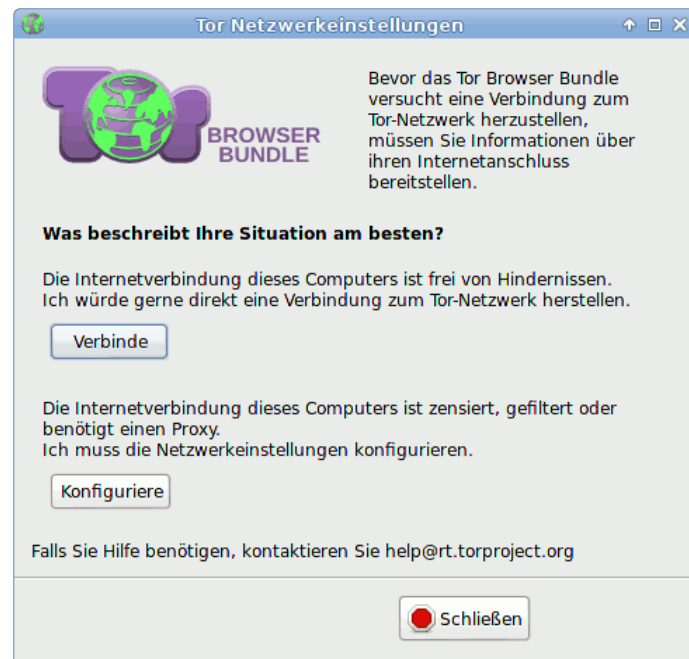


Abbildung 11.6: Start des TorBrowser

misiert. Der Einsatz wurde auf der vom FBI beschlagnahmten Onion Site Giftbox nachgewiesen.¹³

2. 2015 verwendete das FBI einen Zero-Day-Exploit im TorBrowser, um einen Trojaner zu installieren und die Tor-Nutzer damit zu deanonymisieren. Welcher 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.¹⁴
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 Tor-Browser 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.¹⁵
4. Aus den Snowden 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 konnten.¹⁶

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!).

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. Bei Bedarf kann man den

¹³https://motherboard.vice.com/en_us/article/9a3mq7/tor-browser-zero-day-exploit-targeted-dark-web-child-porn-site-giftbox

¹⁴<https://motherboard.vice.com/read/the-fbi-is-classifying-its-tor-browser-exploit>

¹⁵<http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi>

¹⁶<http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>

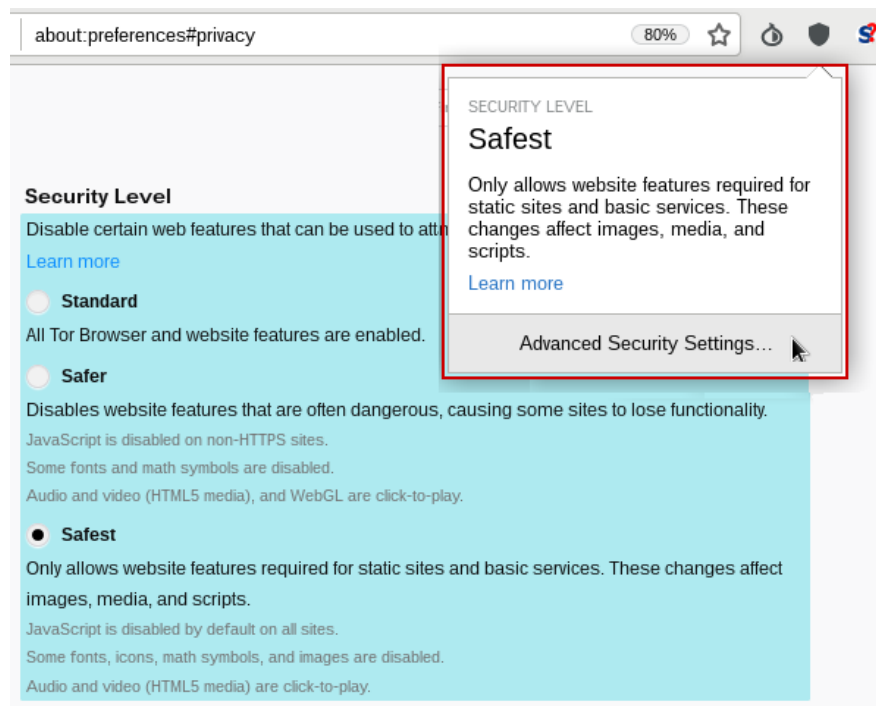


Abbildung 11.7: Sicherheitslevel im TorBrowser anpassen

Sicherheitslevel erhöhen.

Für sicherheitsbewusste Nutzer ist der umgekehrten 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.

Wenn man den Sicherheitslevel auf *Standard* verringert, könnten bösartige Exit Nodes unschöne Dinge in den HTML Code von Webseiten einfügen, die über unverschlüsselte HTTP-Verbindung geladen werden. Das ist nicht empfehlenswert. Neben der NSA und dem FBI betreiben auch andere Geheimdienste bösartige Tor Exit Nodes. Ein Leak von Daten des russischen Geheimdienstleisters Systec zeigte, dass auch der FSB diese Methode nutzt. Die Überwachungsichte 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.

HTTPS Security

sslstripe Angriffe durch Bad Tor Exit Nodes, die 2009 auf der Black Hack Konferenz demonstriert wurden, sind auch 2020 noch ein aktuelles Problem.

Als Schutz gegen diese Angriffe enthält der TorBrowser das Add-on HTTPSEverywhere, welches anhand von Regeln die Umschreibung von HTTP Adressen auf HTTPS für viele populäre Webseiten erzwingt (aber nicht für alle Webseiten, die HTTPS unterstützen).

Konzeptuell bietet die Verwendung von Regeln, die von Servern herunter geladen werden, einige Angriffsmöglichkeiten, die den Entwicklern von HTTPSEverywhere

bewusst sind. Ein Angreifer könnte bösartige Regeln einfügen und z. B. *www.privacy-handbuch.de* auf die Seite *https://www.privacy-handbuch-boese.de* umleiten oder unauffälliger auf... Deshalb warnt HTTPSEverywhere vor Regelsätzen von Dritten (Abb: 11.8).

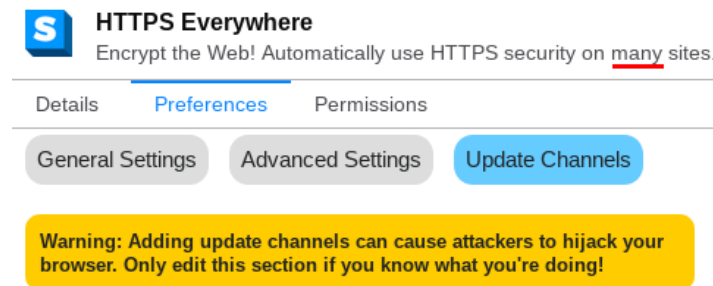


Abbildung 11.8: HTTPSEverywhere: Sicherheitswarnung vor Regelsätzen von Unbekannten

Aber sind die Regelsätze der Default Downloadserver der EFF.org vertrauenswürdig? Selbst wenn man der Qualität bei den Maintainern der Regelsätze vertraut, kann man nie zu 100% ausschließen, dass ein Hacker an diesem Punkt ansetzt und etwas manipuliert...

Alternative: Seit Firefox 78.5 ESR funktioniert der HTTPS-only-Mode zufriedenstellend gut. Damit wird bei Eingabe URL eine Umschreibung auf HTTPS für alle Webseiten erzwungen, die TLS Verschlüsselung unterstützen. Außerdem wird mixed content auf Webseiten, die via HTTPS geladen wurden, komplett blockiert. Wenn kein Upgrade auf eine HTTPS Verbindung möglich ist, wird eine Warnung angezeigt und man könnte die unverschlüsselte HTTP Seite trotzdem aufrufen, wenn man es wirklich will und das Risiko akzeptiert.

Man könnte daher das Add-on HTTPSEverywhere in der Add-on Verwaltung deaktivieren (also: deaktivieren(!) und nicht entfernen, sonst ist es nach dem nächsten Update vom TorBrowser wieder aktiv) und unter *about:config* folgende Optionen aktivieren:

```
dom.security.https_only_mode = true
security.mixed_content.upgrade_display_content = true
```

Ein Trackingdienst kann nicht erkennen, ob der Nutzer *https://www.privacy-handbuch.de* eingegeben hat oder ob die verkürzte Eingabe von *privacy-handbuch.de* durch den HTTPS-only-Mode umgeschrieben wurde. Aber es ergibt sich ein kleiner Unterschied zum Verhalten des originalen TorBrowsers, da die Entwickler bei TorProject.org entschieden haben, für *passive mixed content* (Bilder, CSS, Fonts...) auf HTTPS Webseiten kein Upgrade auf HTTPS zu versuchen und es nicht blockieren. Daraus ergibt sich aber kein individuelles Trackingmerkmal, da auch andere Nutzer diese Einstellungen nutzen.

AdBlocker und Trackingprotection

Der TorBrowser enthält keinen AdBlocker und alle Trackingprotection Features von Firefox sind vollständig deaktiviert. Es ist das Konzept vom TorBrowser, Werbung und Tracking-cripte 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 können 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...). Diese Daten bilden dann den sogenannten *Context*.
- Der Zugriff auf Daten in einem anderen *Context* bzw. 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 Menüpunkt *Neue Identität* der Zwiebel 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.

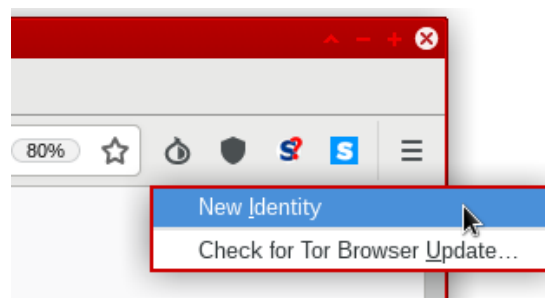


Abbildung 11.9: Neue Identität im TorBrowser wählen

Man sollte dem Anonymitätskonzept des TorBrowser folgen und gelegentlich alle Cookies und andere 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 TorBrowserBundles findet man unten einige Sicherheitshinweise¹⁷, 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.

¹⁷<https://www.torproject.org/download/download>

PDFs und andere Office Dokumente können Tracking Wanzen 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 Bug 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 zu ändern und auf *Speichern* setzen.

Die via Tor herunter geladenen 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 eine PDF Datei von Wanzen säubern, indem man die heruntergeladenen Dateien 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.

11.3.3 TorBrowser für Android Smartphones

Tor Browser für Android wird von TorProject.org entwickelt und ist wie die Desktop Version eine Kombination von sicher konfiguriertem Browser und Tor Onion Router.

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.

Für anonymes Surfen sollte man nur die von Torproject.org empfohlene App verwenden, die Browser und Tor Onion Router kombiniert. Nur mit einem modifiziertem und sicher konfiguriertem Browser kann die Anonymität gewährleistet werden.

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. (M. Kuketz hat in seinem Blog¹⁸ weitere Beispiele analysiert.)

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. Dazu zählen:

- K9Mail mit OpenKeyChain könnten mit Anonymisierungsdiensten für anonyme E-Mail Kommunikation genutzt werden.
- Mit Conversations oder Chatsecure könnte man evtl. anonym jabbern.

11.3.4 OnionBrowser für iPhones

Der Onion Browser von Mike Tigas ist die von TorProject.org empfohlene App für anonymes Surfen auf dem iPhone. Es ist ebenfalls eine Kombination von Browser und Tor.

¹⁸<https://www.kuketz-blog.de/>

Beim ersten Start nach der Installation fragt der Onion Browser, 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 Theme und in Europa nicht nötig. Danach wird abgefragt, welches Sicherheitslevel standardmäßig genutzt werden soll.

- Den *unsicheren* Level sollte man nicht nutzen, weil er wirklich unsicher ist. Damit ist der Onion Browser ungeeignet, um Youtube oder Youporn Videos zu konsumieren.
- Im Level *moderat* ist Javascript allgm. erlaubt, aber es sind einige Techniken wie XHR, Websockets, WebRTC und Videos verboten. Außerdem werden auf Webseiten mit HTTPS Verschlüsselung keine unverschlüsselten Inhalte geladen.
- Wenn man den höchsten Level *sicher* wählt, dann macht das Surfen einfach keinen Spaß, weil Javascript, Videos usw. komplett verboten werden.

Mit einem Klick auf das Icon oben links im OnionBrowser kann für die aktuell dargestellte Webseite individuelle Einstellungen für den Sicherheitslevel definieren.

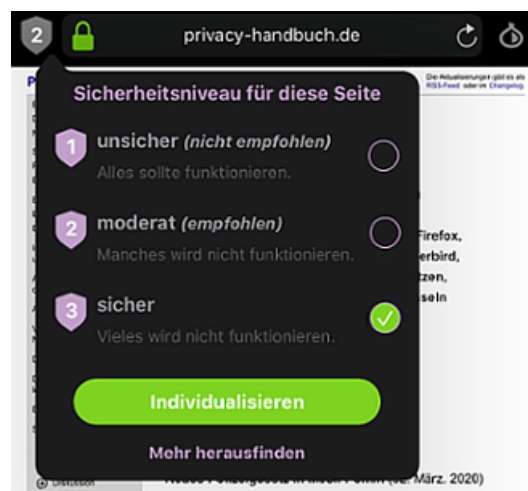


Abbildung 11.10: OnionBrowser: Sicherheitslevel für eine Webseite anpassen

Die Buttons zur Verwaltung der Tabs, Lesezeichen und Einstellungen findet man wie üblich unten in der Fußzeile. Der Onion Browser 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.

11.3.5 Sicherheitskonzept für hohe Ansprüche

Tor Onion Router schützt den Datenverkehr auch gegen Angriffe potenter Geheimdienste wie die NSA. Es ist nach dem aktuellen Stand der Technik nahezu unmöglich, die Verschlüsselung mathematisch zu brechen und Nutzer zu deanonymisieren.

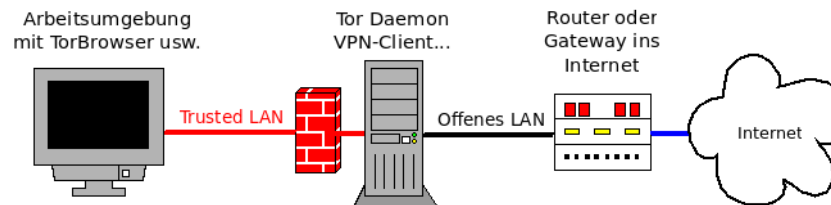
Angriffe zur Deanonymisierung von Tor Nutzern konzentrieren sich daher üblicherweise auf die Client Anwendung (z. B. den Webbrowser). In mehreren bekannten Fällen wurde durch Ausnutzung von Security Bugs im TorBrowser ein kleiner Trojaner auf dem Rechner von Zielpersonen installiert, der IP- und MAC-Adressen des Rechners ermittelt und an einen Server des Angreifers sendet.

Das FBI verwendet seit mehrere Jahre den *Magneto* Trojaner, 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 Projektes *Freedom Hosting* wurde vom FBI in Frankreich lokalisiert und ein direkter Zugriff in Kooperation mit dem Datacenter vor Ort eingerichtet.
Der Magneto Trojaner wurde in mehrere Onion Sites eingebaut und die Besucher deanonymisiert. Neben Webangeboten mit kinderpornografischem Material waren auch der E-Mail Service TorMail und die Bitcoin Börse OnionBank betroffen (2013).¹⁹
- 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 deanonymisiert (2015).²⁰
- Der Onion Service *Giftbox* wurde vom FBI übernommen, wie üblich den Trojaner installiert und die Besucher deanonymisiert. ... (2016).²¹

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 nicht nur das FBI diese Angriffe durchführen sondern auch andere, potente Angreifer.

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 Arbeitsumgebungen mit den Internet Anwendungen getrennt ist.



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) konfiguriert mit limitierter Bandbreite (für Cover Traffic) 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>
```

¹⁹<https://www.wired.com/2013/09/freedom-hosting-fbi/>

²⁰<https://netzpolitik.org/2016/fbi-nutzer-aus-120-laendern-mit-malware-infiziert/>

²¹<https://www.vice.com/en/article/9a3mq7/tor-browser-zero-day-exploit-targeted-dark-web-child-porn-site-giftbox>

```

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 TorBrowser wird StreamIsolation NICHT empfohlen, aber Thunderbird könnte z. B. Port 9101 verwenden, ein Messenger Port 9111, wget den Port 9112...

Der Router braucht evtl. einen DynDNS Namen und ein Port-Forwarding für den konfigurierten ORPort und 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...)

Warum ist Cover Traffic sinnvoll? Ein Beispiel: Es gab einen Studenten, der eine Bombendrohung per E-Mail an seine Universität sendete. Der *Sender-IP* im Header E-Mail verwies auf einen Tor Exit Node. Das Log des zentralen HTTP-Proxy 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 Student das Uni-Netz - FAIL.

11.3.6 Anonyme E-Mail Accounts

Es ist wenig sinnvoll, einen bisher ganz normal genutzten E-Mail Account plötzlich anonym zu nutzen. Es haben sich in den letzten Monaten 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, beispw. 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 sind bestehen zwei Anforderungen:

1. Anonymität: Es dürfen keine Lücken bei 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 eigenmächtigen 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 anbieten oder vergleichbare Lösungen, 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 entschlüsseln, wie bei Webformularen beschrieben, aber das macht kein Spaß. Besser wäre es, wenn der E-Mail Provider OpenPGP im Webinterface unterstützt.

Die im Kapitel E-Mail allgm. empfohlene Nutzung von POP3 zum Abrufen der E-Mail und lokale Speicherung ist damit unmöglich. Die Mails müssen auf dem Server des Providers verwaltet werden und sollten daher möglichst verschlüsselt gespeichert werden.

- **Empfehlung:** ProtonMail bietet mit <https://protonirockerxow.onion> einen Tor Onion Service, Verschlüsselung mit OpenPGP im Webinterface und verschlüsselte Speicherung von E-Mails und Adressbuch. Man kann kostenfreie Accounts nutzen.

Wenn man bei Protonmail einen neuen E-Mail Account anonym via TorBrowser erstellen will, muss man im TorBrowser den Sicherheitslevel *Standard* wählen. Zur Nutzung des Account kann man in den Sicherheitslevel *Safer* oder *Safest* wechseln.

- 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. Im Installationsverzeichnis des TorBrowsers die Datei "Browser/TorBrowser/Data/Tor/torrcmmit einem Texteditor öffnen und folgende Einträge am Ende hinzufügen:

```
MapAddress mailbox.org mailbox.org.85D4088148B1A6954C9BFFFCa010E85E0AA88FF0.exit
MapAddress *.mailbox.org *.mailbox.org.85D4088148B1A6954C9BFFFCa010E85E0AA88FF0.exi
```

- 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 die man die automatische Sammlung von Adressen in den Einstellungen deaktivieren. Die Optionen findet man in den Einstellungen unter *Email*.
 - 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 Hinweisen 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, so dass 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. Es wird der freie Platz auf dem TAILS Boot Medium für einen verschlüsselten Container zum Speichern der Daten genutzt.
2. Dann 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 böartige Tor Exit Nodes zu minimieren.

Thunderbird und Tor Onion Router???

Thunderbird ist nicht für anonyme E-Mails geeignet. Das Add-on TorBirdy ist nicht mehr kompatibel mit Thunderbird seit Version 68 und niemand hat die Gefahren der neuen Features von aktuellen Thunderbird Versionen in Kombination mit Tor Onion Router 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 2011zevon igte 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 nötig und eine neue, angepasste Version des Add-on TorBirdy, 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 privacy-freundlichen 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 ²² zukünftig alle E-Mails der GMail Accounts in das NSA-Datacenter in Bluffdale kopiert.

11.3.7 Anonym Bloggen

Es gibt viele Gründe, um anonym zu Bloggen. Auf die möglichen Gründe möchte ich nicht weiter eingehen und 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 diese neben einem fertig konfigurierten Browser für anonymes Surfen auch die nötigen Tools zur Anonymisierung von Bildern und Dokumenten enthalten und keine Spuren auf dem PC hinterlassen.

²²http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

- 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 und anonym z. B. mit Paysafecard bezahlt werden kann.

Wordpress.com ist empfehlenswert oder die kostenfreie Variante von *Twoday.net*. Für politische Aktivitäten ist der Bloghoster *blackblogs.org* geeignet. Um ein Blog bei diesem Host zu eröffnen, benötigt man eine E-Mail Adresse von einem Technik Kollektiv. Auf der Policy Seite von *blackblogs.org*²³ findet man eine Liste von akzeptierten E-Mail Providern. Diese E-Mail Provider bieten kostenlose Postfächer für politische Aktivisten. Um ein Postfach zu erstellen, muss man seine Gründe darlegen, aber man muss seine Identität nicht aufdecken.

- 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 Blogsoftware 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.
- 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 Blogartikeln ist es möglich, seinen individuellen Schreibstil zu verstellen und stilometrische Angriffe zu erschweren.

11.3.8 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, 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, weil ICE aggressiv versucht, eine Peer-2-Peer Verbindung mit oder ohne Proxy herzustellen und dabei die eigene IP-Adresse dem Kommunikationspartner mitteilt und via UPnP ein Loch in den Router bohren will. Somit kann ein Anruf zur Deanonymisierung führen.
ICE ist Bestandteil von WebRTC und der libjingle (XMPP, WhatsApp).
- DNS Leaks sind ein häufiges Problem bei Messenger, die nicht ausdrücklich für die Nutzung via Tor Onion Router vorbereitet wurden.

²³<https://blackblogs.org/policy/>

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 anonyme genutzte Account erst dann angelegt wird, wenn der Proxy via Tor konfiguriert wurde. Evtl. muss man zuerst einen Dummy Account erstellen, damit man die Einstellungen modifizieren kann und danach den richtigen Account.

UDP und IPv6 Support sind entgegen der Empfehlung bei der Konfiguration von Tor als Proxy zu deaktivieren, da beides von Tor nicht unterstützt wird (Abb: 11.11).

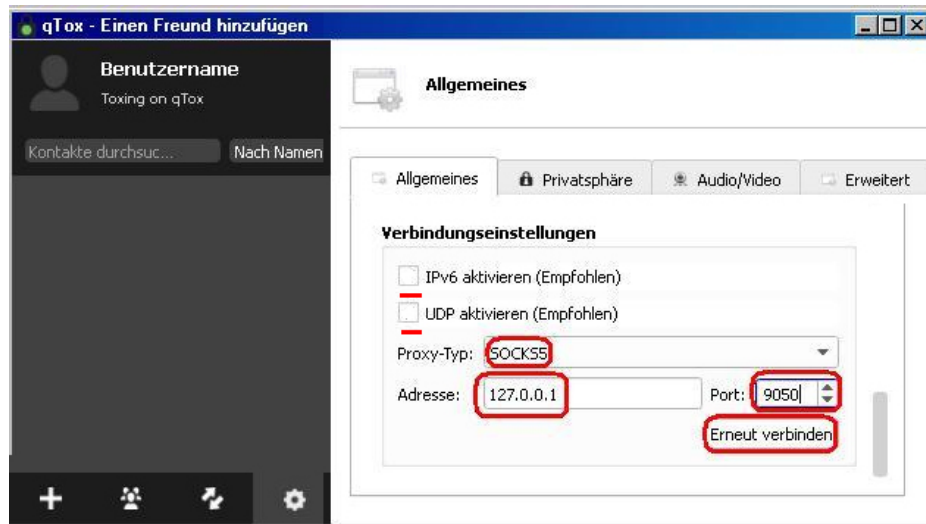


Abbildung 11.11: qTox Proxy Konfiguration für Tor Onion Router

Jabber/XMPP mit Tor zu verwenden, war vor einige 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 Gefahren durch bösartige Tor Exit Nodes. Angriffe von bösartigen Tor Exit Nodes auf Jabber/XMPP wurden bereits nachgewiesen.
3. Audio- und Video-Chats mit der *libjingle* dürfen nicht verfügbar bzw. müssen deaktivierbar sein. Audio- und Video-Chats sind nicht via Anonymisierungsdienst möglich. Bei Einladung zu einem Video-Chat versucht das integrierte *Interactive Connectivity Establishment* (ICE) der *libjingle* automatisch, eine Verbindung mit oder ohne Proxy herzustellen, das ist kein Bug sondern ein Feature der ICE Spezifikation. Nutzer können damit deanonymisiert werden.
4. Weitere XMPP Erweiterungen wie z.B. Jingle Dateitransfer können von einem Angreifer unter Umständen auch 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.

11.3.9 Gajim (Linux) und Tor Onion Router

Gajim ist unserer Meinung nach NICHT für die Kombination mit dem Tor Onion Router geeignet. Es ist eine Proxy Konfiguration für Tor vorbereitet, aber Gajim enthält Bugs, welche die Anonymität und Sicherheit bei der Verwendung von Tor gefährden.

Wir haben Gajim 0.16.5 unter Ubuntu 16.04 kurz getestet (Stand: Nov. 2016). Gajim für Windows verhält sich möglicherweise etwas anders. Evtl. ist die *libjingle* nicht enthalten? Vielleicht kann man sich ähnlich wie bei Pidgin einen Gajim für Linux selbst bauen?

DNS-Leaks: Gajim überlässt die Auflösung von Hostnamen in IP-Adressen nicht dem SOCKS5 Proxy, sondern macht es selbst und umgeht dabei die Proxy Einstellungen. Diese DNS-Leaks sind ein Security Bug und können die Anonymität gefährden. Im TorProject Wiki findet man folgende Empfehlung, das Problem zu umgehen:

To prevent this you have to take the hostname of your jabber-server you want to connect to and resolve its IP, e.g. with tor-resolve and paste the IP address into Account -> Connection -> Custom Hostname and Port. Now you're safe (probably)

Vor einigen Jahren war diese Empfehlung vielleicht ok, die IP-Adresse (oder die Tor Hidden Service Adressen) des XMPP Servers als Verbindungsserver einzutragen. Neumodisch aufgemotzte Jabber Server bieten aber mehrere Services unter unterschiedlichen Hostnamen. Wenn man mit dem Account verbunden ist, kann man sie unter *Aktionen - Dienste durchsuchen* abrufen. Der Jabber Server von conversations.im bietet z.B. die in Abbildung 11.12 zu sehenden Dienste.

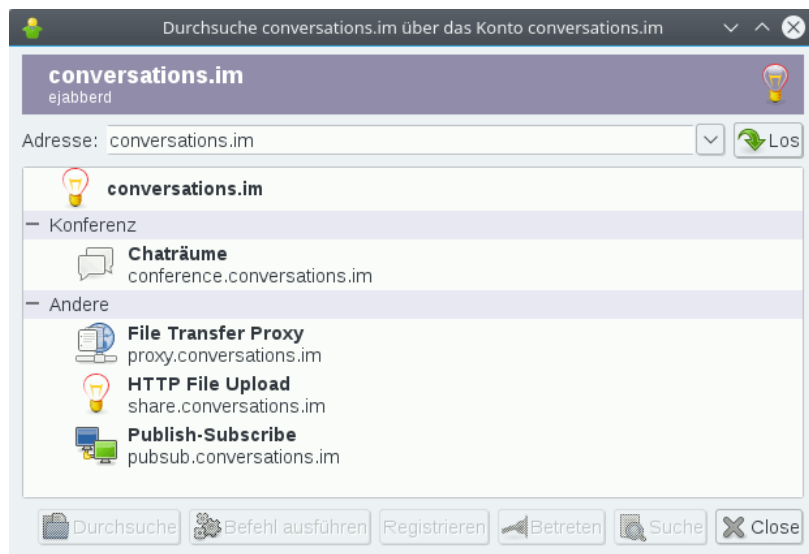


Abbildung 11.12: Services von conversations.im

Man müsste also auch die IP-Adressen der Services *conference.conversations.im*, *proxy.conversations.im* usw. ermitteln und lokal auf dem Rechner fest vorgeben, um DNS-Leaks für diese Hostnamen ebenfalls zu vermeiden (könnte man unter Linux in */etc/hosts* machen). Aber die Services können sich jederzeit ändern, der Admin könnte neue Services hinzugefügt und automatisch an die Clients verteilen... Man müsste es ständig beobachten und bei Bedarf anpassen. Unsicher.

Außerdem treten DNS-Leaks auf, wenn bei einem Dateitransfer ein Dateitransfer Proxy genutzt wird, der vom Kommunikationspartner angeboten wird. Die Nutzung von Dateitransfer Proxies könnte man in der Account Konfiguration deaktivieren.

ICE: Gajim für Linux enthält eine Implementierung der *libjingle* für Audio- und Videochats. Wenn ein Angreifer eine Einladung zu einem Audio Chat schickt, dann versucht das *Interactive Connectivity Establishment* (ICE) der *libjingle* auf unterschiedlichen Wegen, irgendwie eine Verbindung für einen Audio Channel herzustellen und umgeht dabei auch die Proxy Einstellungen. **Auch wenn man Tor als Proxy konfiguriert hat, versucht ICE mit oder ohne Tor irgendwie die Verbindung zum Angreifer herzustellen. Das kann den Nutzer deanonymisieren.** (Dieses Verhalten ist kein Bug sondern ein Feature, dass in der Spezifikation so vorgeschrieben ist).

Ein Beispiel: Unter anderem schickt Gajim eine SSDP Discovery Message ins LAN, um einen UPnP-fähigen Router zu finden, der die externe IP-Adresse liefern könnte:

```
M-SEARCH * HTTP/1.1
Host: 239.255.255.250:1900
Man: "ssdp:discover"
ST: urn:schemas-upnp-org:service:WANIPConnection:1
MX: 3
User-Agent: gajim GSSDP/0.14.14
```

Wenn der Angreifer innerhalb des gleichen lokalen Netz sitzt (innerhalb des Firmennetzwerk, bei Starbucks o.ä.), dann hat man damit verloren. Wenn der Angreifer diese SSDP Discovery Message unmittelbar als nach einer Einladung zu einem Audio Chat sieht, dann weiß er, an welchem Rechner das anonyme Gegenüber sitzt.

Wenn Gajim zufällig einen UPnP-fähigen Router findet, dann ist man auch gegenüber einem Angreifer aus dem Internet deanonymisiert. Bei vielen Heimroutern ist UPnP standardmäßig aktiviert, um die Usability zu verbessern.

Unser Test ist nicht gründlich und ist nicht abschließend. Wir haben ein bisschen rumgespielt und mit Wireshark den Datenverkehr beobachtet, das ist kein Security Audit! Insbesondere haben wir keine Zeit gehabt, wirklich im Code nachzuschauen. Wir haben genug Probleme gefunden, um vor der Kombination Gajim+Tor zu warnen.

11.3.10 Dateien anonym tauschen via Tor

*OnionShare*²⁴ 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 herunter zu laden. Den Link zum Download bekommen die Empfänger über einen anderen sicheren Kanal, z. B. via TorMessenger oder Ricochet.

Installation von OnionShare:

- Für Windows und MacOS stehen auf der Download Website Setup Dateien zur Installation bereit.
- In den Linux Distributionen Ubuntu 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.

²⁴<https://onionshare.org>

Nach dem Start von OnionShare kann man im Hauptfenster Dateien zur Liste der geharten Dateien hinzufügen und den Service starten. Der Tor Daemon des TorBrowser-Bundle wird genutzt, um den Hidden Service bereitzustellen, das TorBrowserBundle muss also gestartet werden, bevor man die Dateien zum Download freigeben kann.

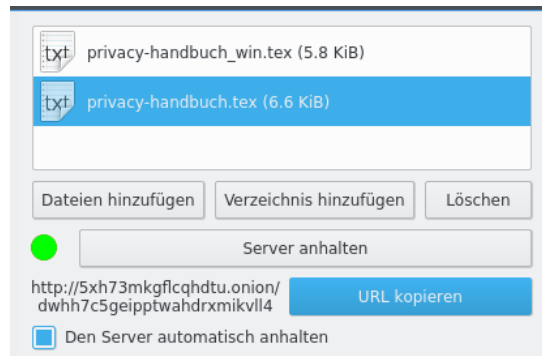


Abbildung 11.13: OnionShare Hauptfenster

Wenn die Option *Den Server automatisch anhalten* aktiviert, dann wird der Tor Hidden Service nach dem ersten erfolgreichen Download sofort wieder beendet. Das ist ein Sicherheitsfeature, da es im Tor Netz auch bössartige Nodes gibt, die neue Tor Hidden Services testen und teilweise auch angreifen.²⁵

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 den Download-Link verteilen.

- Auf diesen Hostern sind die Uploads nur eine begrenzte Zeit verfügbar (1-4 Wochen):
 - <https://1fichier.com> (Uploads werden nach 15 Tagen gelöscht)
 - <https://www.transferbigfiles.com> (bis zu 20GB für registrierte Nutzer)
 - <https://www.filefactory.com> (benötigt Javascript und eine E-Mail Addr.)
- Für Langzeit-Hosting kann man folgende Dienste verwenden:
 - <https://nofile.io> (Verschlüsselung möglich - BETA)
 - <https://www.mediafire.com> (Registrierung für Uploads nötig)

BitTorrent über einen Anonymisierungsdienst ???

Die naheliegende Variante ist es, 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 ist²⁶.

²⁵https://www.schneier.com/blog/archives/2016/07/researchers_dis.html

²⁶<https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea>

Anonyme Peer-2-Peer Netze

Einige Projekte für anonymes, unbeobachtetes Filesharing:

- **I2P Snark:** Das Invisible Internet Project bietet anonymes Filesharing innerhalb des Netzes. Eine kurze Einführung findet man im Kapitel zum Invisible Internet.
- **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 auf der Projektwebsite <https://gnunet.org>.

11.3.11 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:

Onion Services v2 sind veraltet und werden seit Okt. 2021 nicht mehr unterstützt. Diese Onion Service verwenden kryptografische Funktionen, die teilweise veraltet sind. Es wird SHA1 verwendet, DH-Schlüsseltausch und Public Key Kryptografie auf Basis 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 Jan. 2018). Die Onion Services V3 verwenden aktuelle kryptografischen Funktionen (SHA3, ECDHE mit ed25519 und Public Key Kryptografie auf 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, so dass 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.

Authorisierte 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 TorBrowser eingeben und dort dauerhaft speichern, wenn die Abfrage erscheint.

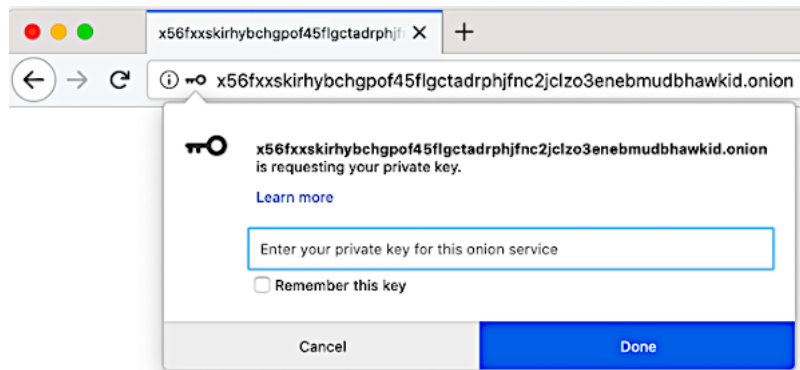


Abbildung 11.14: Abfrage des schlüssels für eine Stealth Onion Site im TorBrowser

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://2gzyxa5ihm7nsggfnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion>
Weitere Onion Sites findet man unter <https://onion.torproject.org> bzw. <http://xao2lxsmia2edq2n5zxg6uahx6xox2t7bfjw6b5vdzxi7ezmqob6qid.onion>
 - Die Onion Sites des Debian Projektes 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 aanbiedern will um sein Taschengeld ein bisschen aufzubessern, findet ihn hier: <http://ciadotgov4sjwlzihbbgxngq3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion>
 - Reddit.com ist als Tor Onion v3 Site erreichbar: <http://kphht2jcflojtqte4b4kyx7p2ahagv4debjj32nre67dxz7y57seqwyd.onion/>
 - u.v.a.m. ...

Wenn der Betreiber einer Webseite es wirklich ernst meint mit dem Onion Service, 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. 11.15).

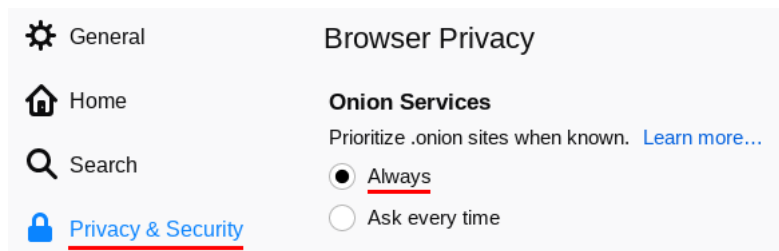


Abbildung 11.15: Einstellung im TorBrowser, um automatisch zum Onion Service zu wechseln, wenn ein Onion Service für die Webseite bekannt ist.

Tor Onion Services für E-Mail und XMPP

Die folgenden **E-Mail Provider** bieten POP3, IMAP und SMTP als Tor Onion Service:

- mailbox.org: xy5d2mmnh6zjnroce4yk7njlkya7tkrameybxu43rgsg5ywhnelmad.onion
- Riseup.net: 5gdvpfoh6kb2iqbizb37lzk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion
- ProtonMail ist unter <https://protonirockerxow.onion> als v2 Onion erreichbar.

Die folgenden **Jabber-Server** sind als Tor Onion Service erreichbar:

- Mailbox: xy5d2mmnh6zjnroce4yk7njlkya7tkrameybxu43rgsg5ywhnelmad.onion
- systemli: razpihro3mgydaiykvxwa44l57opvktqeqfrsg3vvwtmvr2srbkcihyd.onion
- Riseup: jukrlvyhgguedqswc5lehrag2fjunfktouuhi4wozxhb6heyzvshuyd.onion
- securejabber: sidignlwz2odjhgcfnbueinmr23v5bubq2x43dskcebh5sbd2qrxtkid.onion
- jabber.otr.im: ynnuxkbbiy5gicdydekpihmpbqd4fruax2mqhpc35xqjxp5ayvrjuqd.onion
- jabber.so36: yxkc2uu3rlwzzhxf2thtnzd7obsdd76vtv7n34zwald76g5ogbvjbbqd.onion
- Jabber.cat: 7drfpncjeom3svqkyjitif26ezb3xvmtgyhgplcvqa7wwbb4qdbsead.onion
- dismail: 4colmnrbjz3xtsjmqogehtpbt5upjzef57huilibbq3wfgpsylub7yd.onion

HKP-Keyserver für OpenPGP Schlüssel sind unter folgender Adresse erreichbar: <http://zkaan2xfbuxia2wpf7ofnkbz6r5zdbbvxbunvp5g2iebopbfc4iqmbad.onion>

Für unbeobachtete Kommunikation gibt es folgenden Dienste, die ausschließlich aus Tor Hidden Service genutzt werden können:

- *Mail2Tor* (kostenfrei, Gateway ins normale Web ist vorhanden)
<http://mail2torjgmngxentbrmhvgluavhj7ouul5yar6ylbvjkxwqf6ixkwyd.onion>
- *TorBox* (kostenfreier Hidden-only E-Mail Service)
<http://torbox36ijlcevuix7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.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 durchgehend sehr schlecht. Deshalb würde ich Tor Hidden Mail Provider nur für Kommunikation mit Onion-Adressen nutzen und für den Kontakt mit normalen E-Mail Adressen einen sicheren Provider aus dem normalen Netz.

Debian GNU/Linux Hidden Software Repository

Für Debian GNU/Linux gibt es einen Mirror der Repositories als Tor Hidden Service unter der Adresse *vwakviie2ienjx6t.onion*. Außerdem gibt es den Apt-Transport-Tor, der die Nutzung des Hidden Service mit den ganz normalen Tools zur Softwareverwaltung ermöglicht. Um die Software des Systems anonym und von Dritten unbeobachtet zu verwalten und zu aktualisieren ist ab Debian *jessie* nur das Paket *apt-transport-tor* zu installieren:

```
> sudo apt install apt-transport-tor
```

Anschließend editiert man die Datei */etc/apt/sources.list* und ersetzt die Server für Debian Paketquellen nach folgendem Muster:

```
deb tor+http://vwakviie2ienjx6t.onion/debian jessie
deb tor+http://vwakviie2ienjx6t.onion/debian jessie-updates main
deb tor+http://sgvtcaew4bxjd7ln.onion/debian-security jessie/updates main

# deb tor+http://vwakviie2ienjx6t.onion/debian jessie-backports main
```

Zukünftig nutzen alle Tools zur Softwareverwaltung (aptitude, Synaptic, KPackekit, ...) den Tor Hidden Service für die Installation und Aktualisierung der Software.

Neben Debian bietet natürlich auch TorProject.org das Repository für alle unterstützten Distributionen als Onion Site an. Um den tor Daemon regelmäßig zu aktualisieren, kann man folgendes Repository nutzen:

```
deb tor+http://sdscoq7snqtznauu.onion/torproject.org <DISTRIBUTION> main
```

<DISTRIBUTION> ist dabei durch den Codenamen der Distribution zu ersetzen, den man mit dem folgenden Kommando ermitteln kann:

```
> lsb_release -c
Codename: yakkety
```

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).²⁷
- 3x Angebote zum Thema *Rent a Killer*. Ein Auftragsmord kostet offenbar nur 20.000 Dollar (wenn diese Angebote echt sind).
- Ein Angebot für gefakete 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.²⁸

²⁷<http://heise.de/-2124930>

²⁸<http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085>

Fake Onion Sites

Für Tor Onion Sites gibt es kein Vertrauens- oder Reputationsmodell. Es ist unbekannt, wer einen Tor Hidden Services 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 2015²⁹ und Januar 2016³⁰ 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 Bild 11.16 zeigen. Die Fake Site sieht dem Original täuschend ähnlich, die Besucher werden mit den Suchergebnissen aber auf andere Fake Onion Sites gelenkt.

Teilweise sind die Adressen der Fake Sites den Originalen sehr ähnlich:

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 Ergebnislisten einer Suchmaschine für Onion Sites sind dabei nur begrenzt zuverlässig, da die Betreiber der Fake Onion Sites natürlich auch SEO-Techniken nutzen, um vor den Originalen platziert zu werden.

11.3.12 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, 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. 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 wurde 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.

²⁹<https://lists.torproject.org/pipermail/tor-talk/2015-June/038295.html>

³⁰<https://lists.torproject.org/pipermail/tor-talk/2016-January/040038.html>

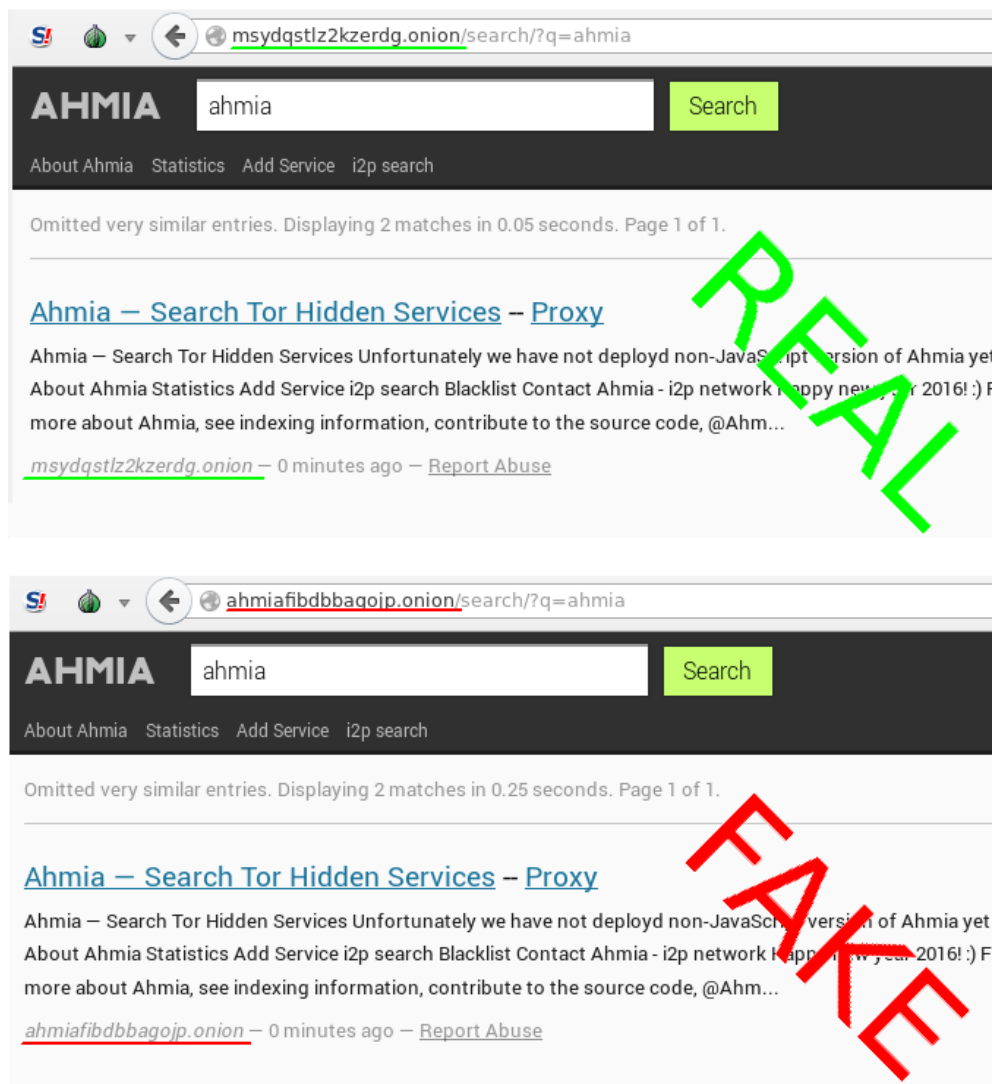


Abbildung 11.16: Original und Fake Onion Site der Suchmaschine Ahmia.fi

| | |
|------------------|---|
| apple | \$232986CD960556CD8053CBEC47C189082B34EF09 |
| CorryL | \$3163a22dc3849042f2416a785eaeefbfeea10cc48 |
| tortila | \$acc9d3a6f5ffcd67ff96efc579a001339422687 |
| whistlersmother | \$e413c4ed688de25a4b69edf9be743f88a2d083be |
| BlueMoon | \$d51cf2e4e65fd58f2381c53ce3df67795df86fca |
| TRHCourtney1..10 | \$F7D6E31D8AF52FA0E7BB330BB5BBA15F30BC8D48 |
| | \$AA254D3E276178DB8D955AD93602097AD802B986 |
| | \$F650611B117B575E0CF55B5EFBB065B170CBE0F1 |
| | \$ECA7112A29A0880392689A4A1B890E8692890E62 |
| | \$47AB3A1C3A262C3FE8D745BBF95E79D1C7C6DE77 |
| | \$0F07C4FFE25673EF6C94C1B11E88F138793FEA56 |
| | \$0FE669B59C602C37D874CF74AFE42E3AA8B62C6 |
| | \$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.³¹
- (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.³²
- (c) Im Sept. 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.³³

Beide Tor Nodes gingen kurz nach ihrer Entdeckung offline. Inzwischen können die Geheimdienste durch Zusammenarbeit mit kompromittierten Certification Authorities 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 ausgehebeln 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 |

³¹<http://www.teamfurry.com/wordpress/2007/11/20/tor-exit-node-doing-mitm-attacks/>

³²<http://archives.seul.org/or/talk/Mar-2008/msg00213.html>

³³<https://trac.torproject.org/projects/tor/ticket/8657>

```

                                IP: 219.90.126.61
ididedittheconfig 0450b15ffac9e310ab2a222adecfef35f4a65c23
                                IP: 94.185.81.130
UnFilTerD         ffd2075cc29852c322e1984555cddfbcb6fb1ee80
                                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 suchte.³⁴
5. Im April 2015 wurden 70 Bad Tor Nodes identifiziert, die den Hidden E-Mail Service angegriffen hatten. Die Betreiber von SIGAINT warnen, dass es den Angreifern gelungen ist, den Hidden Service mit einem man-in-the-middle Angriff zu kompromittieren und möglicherweise Daten inklusive Login Credentials mitzulesen.³⁵

I think we are being targeted by some agency here. That's a lot of exit nodes. SIGAINT Admin

Diese 70 Tor Nodes meldeten sich innerhalb eines Monats kurz vor dem Angriff als neue Tor Nodes im Netzwerk an. 31 weitere Nodes stehen noch in dem 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, hat Chloe im Juni 2015 einen Honigtopf aufgestellt und 11 passiv schnüffelnde Exit Nodes aufgespürt. Zwei der elf Nodes hatten Guard Status.³⁶
7. Im März 2016 haben 14 Bad Exit Nodes in einer konzertierten Aktion versucht, sich als man-in-the-middle in STARTTLS Verschlüsselung einiger Jabber/XMPP Server einzuschleichen.³⁷ 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. 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 Internet³⁸ of Iran eingefügt.

```

<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>

```

³⁴<http://heise.de/-2457271>

³⁵<https://lists.torproject.org/pipermail/tor-talk/2015-April/037549.html>

³⁶<https://chloe.re/2015/06/20/a-month-with-badonions/>

³⁷<https://tech.immerda.ch/2016/03/xmpp-man-in-the-middle-via-tor/>

³⁸<http://arxiv.org/abs/1209.6398>

9. Die Unterlagen des Whistleblowers E. Snowden haben bestätigt, 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.
10. 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.

11.3.13 Tor Good Exit Nodes

Im Abschnitt *Tor Bad Exits* sind einige Nodes genannt, denen man nicht trauen sollte. Diese Aufzählung kann natürlich nicht abschließend und vollständig sein.

Verschiedene Sicherheitsforscher haben nachgewiesen, dass es recht einfach möglich ist, mit schnüffelnden Exits Informationen über die Nutzer zu sammeln (D. Egerstad 2007, C. Castelluccia 2010...). Man kann davon ausgehen, dass es verschiedene Organisationen gibt, die mit unterschiedlichen Interessen im Tor Netz nach Informationen phishen. Auch SSL-verschlüsselte Verbindungen sind nicht 100% geschützt. C. Soghoian und S. Stamm haben in einer wiss. Arbeit gezeigt, dass Geheimdienste wahrscheinlich in der Lage sind, gültige SSL-Zertifikate zu faken.

Als Verteidigung könnte man in der Tor-Konfiguration Exit Nodes angeben, denen man vertraut und ausschließlich diese Nodes als Exit-Nodes nutzen. Welche Nodes vertrauenswürdige sind, muss jeder Nutzer selbst entscheiden. Die folgende kurze Liste von Tor Servern, die von der Community finanziert und betrieben werden, soll Anregungen zum Nachdenken liefern.

- Digitale Gesellschaft (CH) betreibt eine Tor Server Familie.
- AppliedPrivacy.org betreibt eine Tor Server Familie.
- DFRI.se betreibt eine Tor Server Familie.
- Nos-Oignons betreibt eine Tor Server Familie.
- Jens Kubiziel (qbi) betreibt zwei leistungsfähige Exit Nodes.
- Die Heinlein Support GmbH betreibt den Tor Node *mailboxorg* und empfiehlt die Konfiguration von MapAdresses in der *torrc*, so dass dieser Node als Exit Node für alle Mailbox.org Dienste genutzt wird.
- ... bitte selbst die Liste erweitern

Bei der Auswahl der Server sollte man nicht einfach nach dem Namen im TorStatus gehen. Jeder Admin kann seinem Server einen beliebigen Namen geben und den Anschein einer vertrauenswürdigen Organisation erwecken. Die Identität des Betreibers sollte verifiziert werden, beispielsweise durch Veröffentlichung auf einer Website.

Konfiguration in der torrc

In der Tor Konfigurationsdatei */etc/tor/torrc* (Whonix Gateway, stand-alone Tor) bzw. für das TorBrowserBundle in *<TorBrowserBundleVerzeichnis>/Browser/TorBrowser/Data/Tor/torrc* kann man die gewünschten Nodes mit folgenden Optionen konfigurieren. Das Beispiel enthält die Tor Exit Nodes der oben genannten europäischen Vereine (Stand: März 2022)

```
ExitNodes      $0111BA9B604669E636FFD5B503F382A4B7AD6E80,
                $AD86CD1A49573D52A7B6F4A35750F161AAD89C88,
                $B5CED6834BEE8E38D2C62F00CCB6715F0440DA21,
                $BF1B662D1DA4E55F700C130AC58574B47FB7EB8E,
                $08CE3DBFDAA27DB6C044A677AF68D7235C2AFC85,
```

\$0D2DE242ADA0ED77325E3AEE3A9D8C5CD07C2CF3,
\$8C25BA134D579B8AAF420E01215EB2CF06AAE907,
\$E006EA04C696BBD6E35407538131305FF3CB8C16,
\$BCF55F865EE6EF17E25EFEAF851BC429F190B85D,
\$9C61FC0A01401EDF71C4048665E53968E81351FC,
\$8A30B4BF2C86C7E65C2E52A95E882718E63FA74C,
\$763B7D67A6B2D19B3E9EA57D1FBDC48F3B85B559,
\$A4F0F516C83DE11B290384B9B4A4C928A78ED3A5,
\$1893041B86FCED1A2CE2F9E2C5987F534B7DC3E0,
\$B1045E12FA4EA0D457A74013866CB41DCOD290BF,
\$53B1C6E35706C9EC30B9468B61DFBB67F29BFC2F,
\$7EC4C310D1FB2A7C0943B810946EA354D64A2165,
\$BBE1DBF6009B6267AFB4DEF789F62FD9D8A940A4,
\$37C25C1E9CA9F4872D536D084EDDA57F66B43435,
\$AF1E88B00582CD82EAB68C50211DEA47429D5E8B,
\$FFA72BD683BC2FCF988356E6BEC1E490F313FB07,
\$32EE911D968BE3E016ECA572BB1ED0A9EE43FC2F,
\$DD8BD7307017407FCC36F8D04A688F74A0774C02,
\$CF1C1804C33CD69D8A75587FABC63D5D0E2980FA,
\$5933473A3563C0666C5BB833C1DB553C1F296B74,
\$BD6A829255CB08E66FBE7D3748363586E46B3810,
\$42E817BE07AB39CA3BD7A442AF08E007FF2E3F5B,
\$CD1FD2C1F330A3293DA6068E6A23866D063D6DCB,
\$C656B41AEFB40A141967EBF49D6E69603C9B4A11,
\$EFAE44728264982224445E96214C15F9075DEE1D,
\$578E007E5E4535FBFEF7758D8587B07B4C8C5D06,
\$90FD830C357A5109AB3C505287713F1AC811174C,
\$F47B13BFCE4EF48CDEF6C4D7C7A99208EBB972B5,
\$8E6EDA78D8E3ABA88D877C3E37D6D4F0938C7B9F,
\$B580111855B9C452EB224CA7932B626E28D3C2EA,
\$9BA84E8C90083676F86C7427C8D105925F13716C,
\$89B13D7F4D42B7952331893BD1484810600FB4A6,
\$9C1F42F539890E81D30D3F241962FC7625672EDD,
\$85D4088148B1A6954C9BFFFC010E85E0AA88FF0

11.4 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](#) oder [SafePlug](#) 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 privacy-freundliche Konfiguration im Internet surft, der kann sich die Nutzung von Tor sparen, 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 Webproxys, 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.

Mit Free Hide IP bleiben Sie beim Surfen im Internet anonym. So sind Sie vor Datensammeln 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 - beispielsweise 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 einen 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. 11.17).

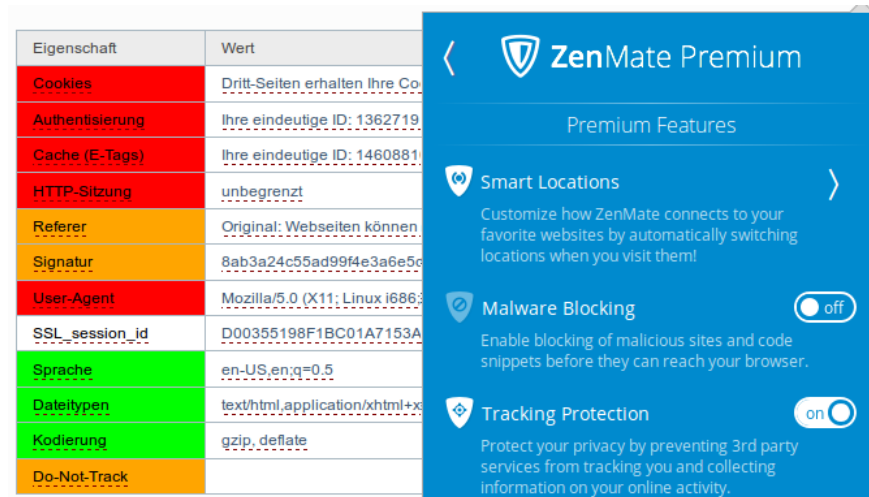


Abbildung 11.17: Tracking Protection in ZenMate funktioniert nicht

Schlussfolgerung: Das ist nu

Kapitel 12

Anonyme Peer-2-Peer Netzwerke

Anonyme Peer-2-Peer Netze nutzen die Infrastruktur des WWW, um in einer darüber liegenden, komplett verschlüsselten Transportschicht ein anonymes Kommunikationsnetz zu bilden. Der Datenverkehr wird mehrfach verschlüsselt über ständig wechselnde Teilnehmer des Netzes geleitet. Der eigene Rechner ist auch ständig an der Weiterleitung von Daten für andere Teilnehmer beteiligt. Das macht die Beobachtung durch Dritte nahezu unmöglich.

Es entsteht ein sogenanntes Darknet im Schatten des normalen Internet, das Google nicht kennt und in dem man sich weitgehend unbeobachtet bewegen kann, wie im Dunkel der Nacht.

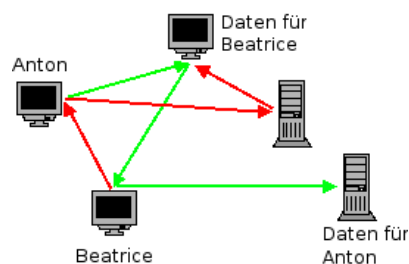


Abbildung 12.1: Prinzip von anonymen Peer-2-Peer Netzen

Hauptverwendungszweck für anonyme Peer-2-Peer Netze ist unbestritten das abmahn-sichere Tauschen von Dateien. Unbeobachtete Kommunikation zwischen den Teilnehmern (E-Mail, Chatten...) ist ebenfalls möglich. Außerdem kann man zensurresistent Webseiten publizieren. Da die Nutzung der Angebote mit technischen Hürden verbunden ist, werden sie deutlich weniger besucht als klassische Webseiten.

Invisible Internet Project (I2P)

I2P hat das Ziel, Anonymität sowohl für Konsumenten als auch für Anbieter von Angeboten zu bieten. Dieses Ziel lässt sich nur in einem geschlossenen Netz verwirklichen. Die innerhalb des Invisible Internet bereitgestellten Angebote sind nicht lokalisierbar. Wie im normalen Internet sind die meisten Angebote zentralisiert und Server-basiert.

- Webserver stellen die sogenannten *eepsites* bereit, die Webseiten mit der Toplevel Domain *.i2p*. Es gibt Suchmaschinen für die *eepsites*. Das Äquivalent für Google ist <http://eepsites.i2p>.
- Als E-Mail Dienst hat sich *SusiMail* etabliert, ein zentraler Mailserver für I2P mit Gateway ins normale Internet. Eine neue Alternative ist das serverlose Projekt *I2P-Bote*.

- Das Äquivalent zum Usenet ist *Syndie*. Es gibt öffentliche und private Diskussionsforen, die auf Syndicationservern gehostet werden.
- Es gibt zwei redundante Server für IRC.
- Für das Filesharing ist mit *I2Psnark* eine Adaption von BitTorrent vorhanden. Der Tracker von *Postman* ist das Äquivalent zur PirateBay im normalen Netz.

Freenet

Freenet bietet Schutz gegen das umfangreichste Angriffsmodell. Freie Kommunikation unter den Bedingungen totaler Überwachung ist das Ziel des Projektes. Es stellt die höchsten Anforderungen an die Nutzer und erzielt die langsamste Downloadgeschwindigkeit.

Im Unterschied zu I2P werden die Inhalte im Freenet redundant über alle Teilnehmer verteilt und verschlüsselt abgelegt. Es gibt keine Server für Webdienste, E-Mail usw. Der Zugriff auf die Inhalte erfolgt nicht über einfache URLs, sondern über komplexe Schlüssel, welche die Adressen der TOR Hidden Services als absolut harmlos erscheinen lassen. Einmal veröffentlichte Inhalte können im Freenet nicht mehr modifiziert werden, auch nicht vom Autor. Es ist jedoch möglich, aktualisierte Versionen zu veröffentlichen. Die Freenet Software stellt sicher, dass immer die aktuellste Version angezeigt wird.

Neben Webseiten gibt es *F-Mail* und mit *Frost* ein Äquivalent zum Usenet. Das Tauschen von Dateien erfolgt direkt im Browser mit einer Oberfläche, die die Freenet Software bereitstellt.

Unabhängig vom *Open Freenet* kann man mit vertrauenswürdigen Freunden ein eigenes Netz Friend-2-Friend Netzwerk konfigurieren, welches sich vollständig der Beobachtung durch unbefugte Dritte entzieht.

Retroschare

RetroShare ist ein Friend-2-Friend Netzwerk. Wie bei I2P und Freenet wird die Infrastruktur des Internet als Basis genutzt und ein voll verschlüsselter Layer darüber gelegt. Im Gegensatz zu I2P gibt es kein zentrales Netzwerk, mit dem man sich als Teilnehmer verbindet, sondern viele kleine Netze. Diese Mininetze müssen die Teilnehmer der Gruppe selbst aufbauen, indem sie kryptografische Schlüssel austauschen (z. B. per E-Mail) und diese Schlüssel im RetroShare Client importieren.

RetroShare ermöglicht die unbeobachtete Kommunikation in Gruppen, ohne zentrale Dienste im Internet zu nutzen. Die Kommunikation ist durch Dritte sehr schwer kompromittierbar, wenn jeder Teilnehmer die kryptografischen Schlüssel nur an vertrauenswürdige Freunde weitergibt. Wenn man allerdings diese Grundregel missachtet und die eigenen Schlüssel im Internet publiziert, um das private Netzwerk zu vergrößern, dann können sich auch unbefugte Dritte einschleichen.

12.1 Invisible Internet Project (I2P)

Das Invisible Internet Project (I2P) hat das Ziel, Anonymität sowohl für Konsumenten als auch für Anbieter von Angeboten zu bieten. Dieses Ziel lässt sich nur in einem geschlossenen Netz verwirklichen.

Das Projekt bietet einen Java-basierten Client. Dieser Client verschlüsselt den Datenverkehr für alle Internet-Anwendungen, die I2P nutzen. Außerdem stellt er sicher, dass ständig neue Verbindungen zu anderen Rechnern des Netzwerkes aufgebaut werden.

Neben der Möglichkeit, anonym zu surfen und Websites (sogenannte *eepsites*) anzubieten, sind weitere Anwendungen bereits fester Bestandteil von I2P. Es bietet anonyme E-Mail (Susimail, I2P-Bote), BitTorrent Downloads (I2Psnark), ein anonymes Usenet (Syndie) u.a.m.

12.1.1 Installation des I2P-Routers

Für die Nutzung des Invisible Internet Projects benötigt man den I2P-Router, der als Proxy für verschiedene Anwendungen (Webbrowser, E-Mail Client...) dient und die Weiterleitung der Daten vom und zum I2P-Netz übernimmt. Der I2P-Router ist eine Java-Applikation und steht unter <https://geti2p.net/de> zum Download bereit.

Windows: Als erstes ist ein Java-Runtime-Environment (JRE) zu installieren. Das Installationsprogramm für Java gibt auf der Webseite www.java.com¹. Der Installer möchte unbedingt die *Ask-Toolbar* für alle Browser installieren. Das sollte man deaktivieren, braucht man nicht.

Anschließend kann der I2P-Router installiert werden. Die Datei *i2pinstall-0.x.y.exe* von der I2P Downloadseite enthält einen kompletten Installer, der nach dem Start alles Nötige einrichtet. Einfach starten und dem Assistenten folgen. Nach der Installation findet man im Startmenü die neue Gruppe *I2P* (Bild 12.2).

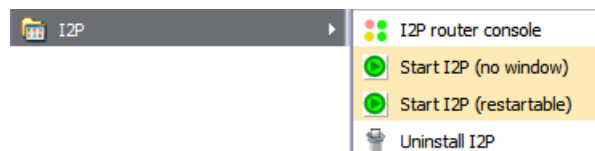


Abbildung 12.2: I2P im Startmenü von Windows

Die beiden Punkte zum Starten von I2P unterscheiden sich nur gering. Im ersten Fall hat man keine störende Konsole auf dem Desktop. *I2P router console* öffnet den Webbrowser, um den Router zu konfigurieren oder abzuschalten mit der Adresse <http://localhost:7657>.

Ubuntu: Die aktuellen Versionen von Ubuntu ab 18.04 enthalten den I2P-router in den Repositories. Mit dem bevorzugten Paketmanager kann man alles Nötige mit einem Kommando installieren:

```
> sudo apt install i2p
```

Für ältere Ubuntu kann man das PPA Repository der I2P Maintainer nutzen:

¹<https://www.java.com/de/>

```
> sudo apt-add-repository ppa:i2p-maintainers/i2p
> sudo apt update
> sudo apt install i2p
```

Debian: Für Debian *stretch* gibt es ein Repository, das man mit folgenden Zeilen in der Datei */etc/apt/sources.lst* einbindet:

```
deb http://deb.i2p2.no/ stable main
deb-src http://deb.i2p2.no/ stable main
```

Außerdem ist der Signaturschlüssel des Repository *i2p-debian-repo.key.asc* herunterzuladen und in den Apt-Keyring einzufügen mit:

```
> wget https://geti2p.net/_static/i2p-debian-repo.key.asc
> sudo apt-key add i2p-debian-repo.key.asc
```

Danach kann man I2P und auch das Paket *i2p-keyring* für spätere Updates des Signaturschlüssels installieren:

```
> sudo apt install i2p i2p-keyring
```

Debian *buster* enthält den I2P Router in den Repositories der Distribution, mit dem Paketmanager kann man alles notwendige installieren ohne extra Repositories einzufügen:

```
> sudo apt install i2p
```

Linux: Als erstes ist Java (Paket: *default-jre*) mit der Paketverwaltung der Distribution zu installieren. Danach kann der I2P-Router installiert werden. Den Installer *i2pinstall-0.x.y.jar* findet man auf der Downloadseite des Projektes. Nach dem Downlad startet man den Installer und wählt die Sprache sowie das Verzeichnis für die Installation:

```
> java -jar i2pinstall-*.jar
```

In dem neu angelegten Installationsverzeichnis findet man das Script zum Starten/Stoppen des I2P-Routers:

```
> ~/i2p/i2prouter start
```

Stoppen lässt sich der Router in der Router-Konsole im Webbrowser unter <http://localhost:7657> mit Klick auf den Link *shutdown* oder obiges Kommando mit der Option *stop*.

Linux (advanced): K. Raven hat eine umfassende Anleitung geschrieben, wie man den I2P-Router in einer chroot-Umgebung installiert und mit AppArmor zusätzlich absichert. Lesenswert für alle, die es richtig gut machen wollen. Link: <http://wiki.kairaven.de/open/anon/chrooti2p>

Nach dem ersten Start braucht der I2P-Router einige Zeit, um sich im Invisible Internet zu orientieren. Zum Warmlaufen sollte man ihm 30 min Zeit lassen. Wenn es danach noch immer nicht so richtig funktioniert, sind die Netzwerkeinstellungen zu prüfen. Die Startseite der Router-Console gibt einige Hinweise.

Den I2P-Router kann man nicht kurz einmal starten, wenn man ihn nutzen möchte. Er sollte möglichst immer laufen, wenn der Rechner online ist. Damit lernt er die verfügbaren Peers und eepsites besser kennen und ist besser in das Netz eingebunden.

12.1.2 Konfiguration des I2P-Router

Standardmäßig ist der I2P-Router funktionsfähig vorkonfiguriert. Ein paar kleine Anpassungen können die Arbeit etwas verbessern.

Bandbreite anpassen

Der I2P-Router arbeitet am besten, wenn man die Bandbreite an den eigenen Internetanschluss anpasst. Nach dem Start kann man auf der Seite <http://localhost:7657/config> der Router Konsole die Werte anpassen.

Netzwerkconfiguration

Auf der Seite <http://localhost:7657/confignet> der Router Konsole sind die Einstellungen für die Einbindung in das I2P-Netz zu konfigurieren. Dabei gibt es zwei Möglichkeiten:

1. Wenn der eigene Rechner nicht vom Internet erreichbar ist, dann sind folgende Optionen zu aktivieren, damit der I2P-Router korrekt arbeitet:
 - *Versteckter Modus* ist zu aktivieren.
 - Optional kann der *Laptop Modus* aktiviert werden. Dann ändert sich Router-Identifikation bei Änderung der IP-Adresse.
2. Wenn der eigene I2P-Router vom Internet für andere Teilnehmer erreichbar ist, verbessert sich die Performance und Anonymität. In der Netzwerk Konfiguration des I2P-Routers sind dann folgende Optionen zu konfigurieren:
 - UPnP ist aus Sicherheitsgründen auf dem DSL-Router zu deaktivieren. Damit ist klar, dass in der Netzwerkconfiguration des I2P-Routers das *UPnP Portforwarding* und die *UPnP IP-Adresserkennung* auch zu deaktivieren sind.
 - In den UDP-Einstellungen ist der Port anzugeben, für den die Weiterleitung auf dem DSL-Router konfiguriert wurde.
 - In den TCP-Einstellungen ist ebenfalls der Port zu konfigurieren und die Option *automatisch erkannte IP-Adresse benutzen* zu aktivieren.

Die Hinweise im Kapitel *Konfiguration des DSL-Routers* erläutern die notwendigen Einstellungen, damit Ihr Rechner vom Internet erreichbar ist. Auf dem DSL-Router ist ein Portforwarding zu Ihrem Rechner zu konfigurieren und die Firewall des Rechners ist anzupassen.

SusiDNS anpassen

Für die Zuordnung von Domainnamen mit der Toplevel Domain *.i2p* zu einem Service wird SusiDNS verwendet, ein dem DNS im Internet vergleichbares System. Wie in den Anfangszeiten des WWW erhält jeder I2P Router eine komplette Liste der bekannten eepsites: das *addressbook*.

Um neue eepsites oder Services in das *addressbook* einzufügen, verwendet I2P sogenannte *subscriptions*. Die eine standardmäßig vorhandene subscription wird relativ selten aktualisiert.

Um auf dem Laufenden zu bleiben, kann man weitere subscriptions zu abonnieren. Die Einstellungen für SusiDNS findet man in der Routerkonsole. Subscriptions kann man unter folgender Adresse einfügen: <http://localhost:7657/susidns/subscriptions.jsp> (Bild 12.3)

Folgende subscriptions bieten aktuelle Neuerscheinungen von eepsites:

```
http://stats.i2p/cgi-bin/newhosts.txt
http://i2host.i2p/cgi-bin/i2hostetag
http://tino.i2p/hosts.txt
```




Abbildung 12.3: subscriptions für SusiDNS

12.1.3 Anonym Surfen mit I2P

Der I2P-Router stellt einen HTTP- und HTTPS-Proxy für den Webbrowser bereit. Die Default-Adressen dieser Proxys sind:

```
Rechner: localhost
HTTP-Proxy Port: 4444
SSL-Proxy Port: 4445
FTP-Proxy Port: 4444
Gopher-Proxy Port: 4444
```

Der Proxy kann genutzt werden, um Webseiten im Invisible Internet aufzurufen (sogenannte *eepsites*, erkennbar an der Toplevel Domain **.i2p**).

JonDoFox nutzen

Das Firefox Profil *JonDoFox* ist für spurenarmes und sicheres Surfen optimiert. Es bietet neben *JonDo* und *Tor* eine *Benutzerdefinierte Proxy Konfiguration*, die man für I2P nutzen kann. Die Einstellungen zeigt Bild 12.4. Der JonDoFox verhindert zuverlässig eine Kompromittierung der Anonymität.

Firefox selbst konfigurieren

Ich würde empfehlen, für das Surfen im Invisible Internet ein separates Firefox-Profil zu erstellen. Dann ist es für spionierende Websites gänzlich unmöglich, im Cache oder in der Historie abgelegte Daten über das anonyme Surfen auszulesen. Den Profil-Manager von Firefox startet man mit folgendem Kommando:

```
> firefox -P
```

In dem sich öffnenden Dialog (Bild 12.5) kann man ein neues Profil anlegen und anschließend die Proxy-Einstellungen konfigurieren. In Zukunft wird Firefox bei jedem Start fragen, welches Profil genutzt werden soll.

Anschließend kann das Profil *I2P-Fox* gestartet werden und die Proxy-Einstellungen sind wie im Bild 12.6 gezeigt zu konfigurieren. Die allgemeinen Hinweise zu Cookies, JavaScript, Plug-ins, HTTPS-Security usw. im Abschnitt *Spurenarm Surfen* gelten auch für I2P. Das Profil *I2P-Fox* ist entsprechend zu konfigurieren.



Abbildung 12.4: Benutzerdefinierte Proxy Konfiguration im JonDoFox



Abbildung 12.5: Firefox Profil-Manager

Wichtige Sicherheitseinstellungen für Firefox

Flash und Java Plug-ins sind unbedingt zu deaktivieren, da diese Plug-ins die Proxy Einstellungen umgehen könnten. Um eine Deanonymisierung zu vermeiden, sind für einen aktuellen Firefox außerdem folgende Features unter der Adresse *about:config* zu deaktivieren:

- WebRTC kann durch UDP-Tunnel die reale IP-Adresse aufdecken (nur Firefox 18 und neuer):

```
media.peerconnection.enabled = false
```

- Geolocation-API kann den realen Standort ermitteln:

```
geo.enabled = false
```

- Phishing- und Malware Protection funktioniert für eepsites nicht, da die Webseiten des Darknet nicht in der Google Datenbank enthalten sind:

```
browser.safebrowsing.enabled = false
```



Abbildung 12.6: Firefox Proxy-Einstellungen für I2P

Suchmaschinen für I2P

Um sich in einem Netzwerk zu orientieren, braucht man eine Suchmaschine. Die Webseite plugins.i2p bietet viele *Firefox Search Plugins für I2P*. Wenn man die Webseite <http://plugins.i2p/firefox> aufgerufen hat, kann man die Suchmaschinen einfach durch Aufklappen der Liste der Suchmaschinen oben rechts im Firefox hinzufügen. Unter dem Trennstrich findet man die neuen Suchmaschinen, die diese Webseite zur Installation anbietet.

Das Äquivalent zu Google im normalen Internet ist im I2P-Netz die Suchmaschine <http://eepsites.i2p>. Die anderen Dienste in der Liste durchsuchen einzelne eepsites.

12.1.4 I2P Mail 1 (Susimail)

Die Anwendung Susimail ist integraler Bestandteil von I2P und ermöglicht den unbeobachteten Austausch von E-Mails. Das Anlegen und Verwalten eines Susimail-Accounts erfolgt auf der eepsite <http://hq.postman.i2p>.

Es ist möglich, E-Mails in das normale Web zu versenden und auch von dort unter der Adresse `<username>@i2pmail.org` zu empfangen. die Weiterleitung ins normale Internet kann bis zu 24h dauern und ist von den gewählten Einstellungen auf HQ Postmaster abhängig. Um für Spammer unattraktiv zu sein, haben die Entwickler von I2P die Anzahl der ins normale Web versendbaren Mails begrenzt. Es ist möglich, innerhalb von 24h bis zu 20 Empfängern beliebig viele E-Mail zu senden. Wer unbedingt mehr Leute per E-Mail kontaktieren will, kann mit einem Hashcash ein Kontingent von weiteren 20, 40 oder 80 Empfängern freischalten.

Routerkonsole nutzen

Ein einfaches Webinterface für Susimail ist in der I2P Routerkonsole erreichbar unter der Adresse <http://localhost:7657/susimail/susimail>.

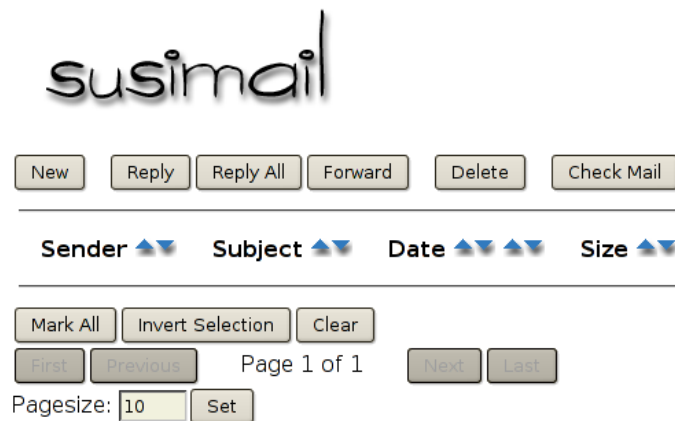


Abbildung 12.7: Webinterface von Susimail

Es bietet eine simple Möglichkeit, Mails abzurufen und zu versenden. Komfortabler ist die Nutzung des bevorzugten E-Mail Clients, vor allem wenn man die Möglichkeiten zur Verschlüsselung der Nachrichten nutzen möchte.

Thunderbird konfigurieren

Der Susimail-Account kann mit jedem E-Mail Client genutzt werden.

```
SMTP-Server: localhost      Port: 7659
POP3-Server: localhost      Port: 7660
Login-Name:  <username>
```

In Thunderbird ist als erstes ein neuer SMTP-Server anzulegen (Konten -> Postausgangs-Server (SMTP) -> Hinzufügen). Der Server erfordert eine Authentifizierung mit den Daten des Susimail Accounts.

Danach kann ein neues POP3-Konto angelegt werden, welches diesen SMTP-Server für die Versendung nutzt. SSL- und TLS-Verschlüsselung sind zu deaktivieren. Der I2P-Router übernimmt die abhörsichere Übertragung.

In den Server-Einstellungen des Kontos sollte die Option *“Alle x Minuten auf neue Nachrichten prüfen”* deaktiviert werden! Die Admins von Susimail bitten darum, den Service nicht unnötig zu belasten.

Susimail mit Tor nutzen

An Stelle des I2P-Routers kann auch Tor für den Abruf und das Versenden von Nachrichten via I2P Mail genutzt werden. Folgende Hidden Services bieten ein SMTP-Gateway (Port: 7659) und POP3-Gateway (Port: 7660):

```
v6ni63jd2tt2keb5.onion
5rw56roal3f2riwj.onion
```

Die Hidden Service Adresse ist als SMTP- und POP3-Server im E-Mail Client für das I2P-Mail-Konto an Stelle von *localhost* einzutragen. Außerdem ist der E-Mail Client so zu konfigurieren, dass er Tor als Proxy nutzt. Sollte der E-Mail Client ständig den Fehler *TIMEOUT* liefern, hilft es, den Hidden Service erst einmal im Webbrowser aufzurufen.

Hinweise zur Nutzung von Susimail

Der Service wird von *postman* und *mastijaner* in der Freizeit aufgebaut und gepflegt. Sie bitten darum, folgende Hinweise zu beachten:

1. Bitte nicht den POP3-Service in kurzen Intervallen automatisiert abfragen. Einige Nutzer fragen den POP3-Dienst immer wieder innerhalb weniger Minuten ab und belasten den Service stark. Zweimal pro Tag sollte reichen.
2. Um anonym zu bleiben, sollte man keine Mails an die eigene Mail Adresse im Web schreiben oder an Bekannte, mit denen man via E-Mail im normalen Web Kontakt hält.
3. Bitte Susimail nicht für Mailinglisten nutzen, die man nicht mitliest. Das Abmelden auf Mailinglisten bei Desinteresse nicht vergessen.
4. Wer nicht mehr im Invisible Internet aktiv ist, sollte auch an das Löschen des Susimail Account denken. Scheinbar gibt es auf dem Server viele tote Mail-Accounts, wo noch immer Mails eingehen (Spam und Mailinglisten) und viel Speicherplatz verbrauchen.
5. Bitte verwendet den Dienst nicht, um anonyme Beleidigungen oder Drohungen zu schreiben. Das bringt den Betreibern Ärger und gefährdet den reibungslosen Betrieb.

Englischer Originaltext bei HQ Postman: <http://hq.postman.i2p/?p=63>

12.1.5 I2P Mail 2 (Bote)

I2P Bote bietet serverlose und verschlüsselte E-Mail Kommunikation. Die Daten werden redundant und verschlüsselt in einer DHT gespeichert, über alle Teilnehmer verteilt. Es gibt keinen zentralen Server, der Kommunikationsprofile erstellen oder eine Vorratsdatenspeicherung umsetzen könnte. Starke Kryptografie stellt sicher, dass nur der Empfänger die Nachricht lesen kann.

I2P Bote ist keine Weiterentwicklung von Susimail und es soll es auch nicht ersetzen. Langfristig werden beide Projekte parallel existieren und kooperieren. Das Projekt bietet folgende Features:

- Bedienung im Webinterface der I2P-Routerkonsole.
- Erzeugen von Identitäten, Senden/Empfangen von E-Mails.
- SMTP- und IMAP-Gateway für die Integration in Thunderbird u.a.
- Anonyme Absender und Versenden über Zwischenstationen mit zeitlicher Verzögerung (Remailer-Konzept).
- Dateianhänge bis 500 kB werden unterstützt. Die Begrenzung der Größe der Dateianhänge ist aufgrund der redundanten Speicherung nötig. Die Nachrichten werden mit 20x Redundanz gespeichert und eine 1 MB große Mail würde 20 MB Speicherplatz in der DHT belegen.

Installation von I2P Bote

Um I2P Bote zu nutzen, ist die Installation von 3 Plug-ins für den I2P Router nötig. Auf der Seite I2P Dienste der Routerkonsole (unter <http://localhost:7657/configclients.jsp>) findet man ganz unten den Abschnitt für die Installation zusätzlicher Plug-Ins (Bild 12.8).

Folgende Plug-Ins sind in dieser Reihenfolge zu installieren:

1. http://sponge.i2p/files/seedless/01_neodatis.xpi2p
2. http://sponge.i2p/files/seedless/02_seedless.xpi2p

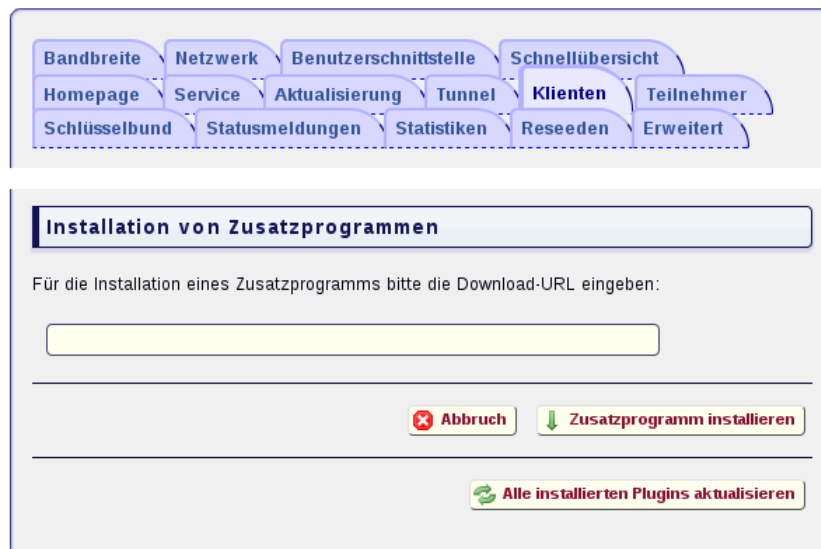


Abbildung 12.8: Installation des Plug-in I2P Bote

3. <http://i2pbote.i2p/i2pbote.xpi2p>

Nach erfolgreicher Installation findet man auf der Startseite in der Liste der *Lokalen Dienste* oder rechts im Menü der Routerkonsole einen neuen I2P Dienst *SecureMail*. Ein Klick öffnet die Web-Oberfläche in einem neuen Browser-Tab.

Eigene Identität erzeugen

Der erste Schritt nach der Installation ist in der Regel die Erstellung einer eigenen Adresse. In der Navigationsleiste rechts wählt man "Identitäten" und den Button "Neue Identität".

Als Pflichtfeld ist nur ein Name anzugeben. Die Verschlüsselung belässt man am besten bei 256Bit-ECC. Diese Verschlüsselung liefert relativ kurze und starke Schlüssel. Die Mailadresse wird zur Zeit noch nicht genutzt.

Die kryptische Bote-Adresse ist an alle Partner zu verteilen oder zu veröffentlichen. In der Übersicht ist die Adresse nicht voll sichtbar. Wenn man auf die Identität klickt, erhält man eine vollständige Ansicht. Die gesammelten Adressen der Partner können in einem rudimentären Adressbuch verwaltet werden.



Abbildung 12.9: Neue Identität für I2P-Bote anlegen

Konfiguration

Bevor man loslegt, sollte man einen Blick in die Konfiguration werfen und diese anpassen.

- Abrufen der Nachrichten: Es ist konfigurierbar, ob und in welchem Intervall neue Nachrichten aus der DHT automatisch abgerufen werden sollen. Um die Belastung des Bote-Netzes gering zu halten sollte man Intervalle von 2-3h nutzen. Bei Bedarf kann man das Abrufen neuer Nachrichten auch selbst anstoßen.
- Über Zwischenstationen senden: Wird diese Option deaktiviert ("AUS"), gehen versendete Nachrichten direkt in die DHT. Die Anonymität entspricht der normalen Anonymität bei der Nutzung von I2P.

Eine höhere Anonymität erreicht man, wenn die Nachricht vor dem Speichern in der DHT über 1...n Teilnehmer des I2P-Bote Netzes geleitet und dort jeweils um eine zufällige Zeitspanne verzögert wird. Die min. und max. Werte für die Verzögerung können konfiguriert werden. Ähnlich wie bei Remailern sinkt damit natürlich die Performance der Kommunikation.

- Durchleitung an Nicht-I2P-Adressen: Es ist möglich, Mails an Nicht-I2P-Bote Teilnehmer zu versenden. Die Nachrichten werden an die Bote-Adresse eines Durchleitungsdienstes versendet, der sich dann um die weitere Zustellung kümmert. Derzeit arbeitet HQ Postman an der Entwicklung dieses Services, der aber noch nicht arbeitsfähig ist.
- Absendezeit: Die Absendezeit sollte man nicht mit versenden, wenn die Nachricht über Zwischenstationen gesendet wird. Anderenfalls ist es ein Feature, dass die Anonymität nur geringfügig erhöhen kann, wenn diese Option deaktiviert wird. Mir hilft es, den Überblick in der Inbox zu behalten, wenn ein Zeitstempel vorhanden ist.

Mails schreiben und empfangen

Das im Bild 12.10 gezeigte Formular für eine neue Mail öffnet sich mit Klick auf den Button "Neu".

The screenshot shows a web form for composing a new email in the I2P Bote interface. The form is titled 'Neue Mail' and has a light blue background. It includes the following elements:

- Von:** A dropdown menu set to 'Anonym'.
- An:** A dropdown menu and a text input field containing the I2P address '51uKKLjWm573IX48QyS3J8rqql'. There is a button with a right-pointing arrow and a file icon next to the address field.
- Betreff:** A text input field containing 'Test Mail'.
- Anhänge:** A file icon and a button labeled 'Anhängen'.
- Nachricht:** A large text area containing the text 'Diese Mail ist nur ein Test! Gruß'.
- Buttons:** 'Senden' and 'Speichern' at the bottom.

Below the 'Anhänge' section, there is a note: 'Es wird empfohlen, Anhänge kleiner als 500 kB zu halten.'

Abbildung 12.10: Neue E-Mail in I2P Bote schreiben

Als Absender kann man *Anonym* wählen, oder eine der zuvor angelegten Identitäten. Wer *Anonym* wählt, sollte sich nicht wundern, dass er vom Empfänger als anonymer Unbekannter behandelt wird. Für vertrauliche Konversation muss man seinen Gegenüber verifizieren können.

In die Felder *An*, *Kopie* oder *Blindkopie* sind die kryptischen Bote-Adressen der Empfänger einzutragen, der Rest sollte sich selbst erklären. Eingehende Mails findet man im Ordner *Posteingang*.

Adressbuch

Das Web-Interface bietet ein einfaches Adressbuch. Man kann die Bote-Adressen und Namen von Partnern sammeln und beim Schreiben einer Mail mit zwei Klicks übernehmen.

Außerdem hilft das Adressbuch bei der Verifikation der Absender empfangener Nachrichten. Ein Absender ist eindeutig nur durch seine Bote-Adresse bestimmt. Der Name kann frei gewählt werden und kann auch mehrfach genutzt werden. Es könnte also jemand den Namen HungryHobo nutzen, um sich als Hauptentwickler von I2P-Bote auszugeben.

Ein Vergleich der Bote-Adressen ist nicht intuitiv. Das Adressbuch kann diese Aufgabe übernehmen. Ist der Absender einer Nachricht im Adressbuch enthalten und stimmt die Bote-Adresse überein, dann zeigt die Liste der Inbox ein Häkchen in der Spalte **Bek.**


| Von | Bek. | Sig | An | Betreff | Absendezeit ▾ |
|----------------|------|-----|-----------|------------------|--|
| HungryHobo <hc | ✓ | ✓ | awxcnx<1~ | AW: A small test | 26.08.2010 05:07  |

Abbildung 12.11: Inbox mit verifiziertem Absender

12.1.6 I2P IRC

IRC ist ein öffentlicher Chat Service. Auf den IRC-Servern gibt es verschiedene Chat-Räume, sogenannte Channels, in denen man sich zu einem bestimmten Thema austauschen kann. Die Unterhaltung ist in der Regel öffentlich, aber auch private Nachrichten können zwischen Nutzern ausgetauscht werden.

Das I2P-Netz bietet zwei anonyme Chat-Server, die direkt über den I2P-Router erreichbar sind. Die Konfiguration der verschiedenen Clients wie XChat (Linux/UNIX), Kopete (KDE), Colloquy (MacOS) oder Mirc (Windows) ist einfach. Man nutzt als Chat-Server folgende Adresse und ist anonym:

```
Host: localhost
Port: 6668
```

Die wichtigsten Chat-Kommandos

Der Chat wird in der Regeln komplett durch Kommandos gesteuert. Alle Kommandos beginnen mit einem Slash. Eine kurze Liste der wichtigsten Kommandos:

/list Listet alle Diskussions-Channels auf, die auf dem Server verfügbar sind.

/join #channel Den Raum #channel betreten und mitdiskutieren.

/quit Den aktiven Raum verlassen oder vom Server abmelden.

/msg nick <text> Sendet eine Nachricht an den User *nick*.

/ignore nick Einen Troll ignorieren.

/help Beantwortet alle weiteren Fragen.

Im IRC ist man mit einem Nicknamen unterwegs. Die Nicknamen werden registriert und mit einem Passwort geschützt, damit kein Dritter einen bekannten Nicknamen nutzen kann, um sich eine Identität zu erschleichen.

Die Registrierung erfolgt mit folgendem Kommando:

```
/msg nickserv register <Password> fake-email-addr
```

Um einen registrierten Nicknamen zu nutzen, muss man sich identifizieren:

```
/msg nickserv identify <Password>
```

#anonops

Die Channels von *Anonymous* stehen auch auf den I2P-IRC Servern zur Verfügung. Für die Diskussionen in diesen Channels sollten sie die Regeln von *Anonymous* beherzigen:

Basics: Tauchen Sie in der Masse unter ohne ein besonders smarter Typ sein zu wollen. Es gibt keine Helden, die alt geworden sind, es gibt nur junge Helden und "tote" Helden.

Geben Sie keine persönlichen Informationen im public IRC preis.

- keine Anhaltspunkte im Nicknamen und Realnamen veröffentlichen
- keine persönlichen Informationen im Chat diskutieren
- keine Informationen über die Herkunft diskutieren (Land, Stadt usw.)
- keine Beschreibung von Tattoos, Piercings oder anderer Merkmale
- keine Informationen über Beruf und Hobbys
- keine Sonderzeichen wie äöü verwenden, die nur in Ihrer Sprache verfügbar sind
- veröffentlichen Sie nichts im normalen Netz, während Sie in einem anonymen Chat sind - es kann einfach korreliert werden
- posten Sie keine Bilder von Facebook im Chat, diese Bilder enthalten die persönliche ID
- verbinden Sie sich nicht Tag für Tag zur gleichen Zeit mit dem Chat

12.1.7 I2P BitTorrent

Der I2P-Router bietet auch eine angepasste Implementierung des BitTorrent Protokolls für anonymes Peer-2-Peer Filesharing. Im Gegensatz zur Nutzung von normalem BitTorrent über Tor ist die Implementierung des Invisible Internet Project anonym und die Nutzung ausdrücklich erwünscht. Der Dienst bietet Optimierungen mit speziellen Clients.

Die I2P-Router-Konsole bietet einen einfachen BitTorrent Client als Webinterface unter *Torrents* (<http://localhost:7657/i2psnark>).

Die zum Tausch bereitgestellten oder heruntergeladenen Dateien findet man im Unterverzeichnis *i2psnark* der I2P-Installation. Dieses Verzeichnis sollte Lese- und Schreibrechte für alle lokalen User haben, die I2PSnark nutzen dürfen. Torrents findet man z.B. auf den eepsites <http://tracker2.postman.i2p>, <http://crstrack.i2p/tracker> oder <http://tracker.welterde.i2p>. Das Webinterface bietet direkte Links zu diesen eepsites.

Hinweis zur Nutzung: Es gehört beim Filesharing zum guten Ton, Dateien nicht nur zu saugen. Man stellt die heruntergeladenen Dateien auch anderen Teilnehmern zur Verfügung. Bei BitTorrent im normalen Netz gilt es als freundlich, wenn man heruntergeladene Dateien mindestens für 2 Tage zum Upload anbietet oder bis die Datenmenge des

Upload das 2,5fache des Downloads beträgt. Da die Geschwindigkeit im I2P-Netz wesentlich geringer ist, sollte man heruntergeladene Dateien mindestens für 1 Woche zum Upload anbieten.

12.2 DSL-Router und Computer vorbereiten

Um als vollwertiger Teilnehmer an einem anonymen Peer-2-Peer Netz teilzunehmen, muss der eigene Rechner vom Internet aus erreichbar sein. Nur dann können andere Teilnehmer des Netzes den eigenen Knoten kontaktieren. Als typischer Heimnutzer mit DSL-Anschluss sind einige Anpassungen nötig, damit der eigene Rechner aus dem Internet erreichbar ist.

1. Der DSL-Router muss den ankommenden Datenverkehr der anderen Peer-2-Peer Teilnehmer an den eigenen Rechner weiterleiten. Einige Programme können den Router mit UPnP konfigurieren. Aufgrund der Sicherheitsprobleme bei UPnP² sollte man dieses Feature auf dem Router deaktivieren und die Weiterleitung per Hand konfigurieren.

Der Screenshot 12.12 zeigt die Konfiguration für einen Linksys Router. Für I2P wurde im Beispiel der Port 8888 gewählt, für GnuNet muss man die Ports 1080 und 2086 weiterleiten.

| Port Range | | | | | |
|-------------|-------|---------|----------|--------------|-------------------------------------|
| Application | Start | End | Protocol | IP Address | Enable |
| i2p | 8888 | to 8888 | Both ↕ | 192.168.1.18 | <input checked="" type="checkbox"/> |
| gnunet1 | 1080 | to 1080 | Both ↕ | 192.168.1.18 | <input checked="" type="checkbox"/> |
| gnunet2 | 2086 | to 2086 | Both ↕ | 192.168.1.18 | <input checked="" type="checkbox"/> |

Abbildung 12.12: Portforwarding auf dem Router

2. Die Konfiguration der Weiterleitung auf dem DSL-Router ist einfacher, wenn der eigene Rechner innerhalb des privaten lokalen Netzwerkes eine feste IP-Adresse hat. Dafür ändert man die Konfiguration der Netzwerkschnittstelle von *DHCP* auf *feste IP-Adresse*.
3. Außerdem muss die Firewall auf dem lokalen Rechner den ankommenden Datenverkehr der anderen Peer-2-Peer Teilnehmer auf den Ports durchlassen, für die eine Weiterleitung im Router konfiguriert wurde.

²<http://heise.de/-1793625>

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 Warrior) 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 verwendet, um die Verfolgung der Reisetätigkeit durch Geo-Lokalisierung der IP-Adresse zu verhindern und in nicht vertrauenswürdigen Wi-Fi Netzwerken (Hotel, Flughafen, U-Bahn o.ä.) die Verbindung zu einem vertrauenswürdigen Zugangsprovider herzustellen und damit Angriffe durch bössartige Nutzer des Hotspots zu verhindern.

Ähnlich wie im Beruf ermöglicht ein VPN Zugriff auf das Heimnetz von unterwegs.

Außerdem kann man mit einem VPN die Geo-IP Sperren von einigen Medien umgehen. Wenn man einen VPN Server mit deutscher IP-Adresse verwendet, kann man beispw. auf Mallorca ein bisschen in der ZDF Mediathek stöbern o.ä.

(Das funktioniert aber nicht immer. Die Geo-IP Sperre von BBC lässt sich beispw. 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 unzensurierte 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 Peer 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 bereitstellt 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 hochsichere, zertifizierte VPN Lösungen. Beispiele dafür sind die Produktlinien genucrypt (von Genua.de) oder SINA (von Secu-net.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 Instektion (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 verwendet. 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.

- as SSH-Protokoll verwendet nur nackte Keys und arbeitet nicht mit signierten Zertifikaten wie TLS. Es bietet weniger Merkmale für die Trafficanalyse via DPI. Man kann auch mit SSH einen verschlüsselten Tunnel zu einem Server aufbauen und durch diesen verschlüsselten Tunnel 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 auf für VPN Traffic nutzen. Einige VPN Provider wie IVPN haben 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 Warrior 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 werden 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 die Verwendung von Smartcards oder Hardware Security Modulen (z.B. Nitrokey HSM) für Server Zertifikate in größeren, kommerziellen Umgebungen sinnvoll. Wenn die Serverzertifikate kompromittiert werden und hundert oder mehr Road Warrior die Serverzertifikate 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.

Sicherheitsempfehlung 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 empfohlen mit aktuellen Ciphern.
- 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 Angeboten von VPN-Anbietern mit dieser Liste vergleicht, dann löst sich das PR-Gebulber 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. Es wird das falsche Tool für eine Aufgabe genutzt, dass 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 mit 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 Anonymisierers zu 95% durch Beobachtung des Traffics des VPN-Servers bzw. -Nutzers 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 wären dann

¹<https://epub.uni-regensburg.de/11919>

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

- 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 die Nutzer verwenden. Damit kann Facebook frühzeitig Konkurrenten erkennen und Maßnahmen zur Sicherung der Marktes ergreifen.³
 - 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

Statt einem Gewinn an Privatsphäre 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 fordern oder Zugriff auf den Datenverkehr für Geheimdienste.

Der britische VPN-Dienst HideMyAss (Testsieger beim VPN Magazine⁵) 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 oder Vodafone oder...

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 und die VPN-Verschlüsselung muss ebenfalls außerhalb der Arbeitsumgebung erfolgen. Diese Anforderungen erfüllt kein bekannter VPN-Provider.)

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.

²<https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru>

³<https://netzpolitik.org/2017/facebook-spioniert-nutzer-seines-vpn-dienstes-aus>

⁴<https://heise.de/-3795523>

⁵<https://www.vpnmagazin.de/hidemyass-test>

⁶<http://t3n.de/news/lulzsec-hacker-anonymizer-hidemyass-straftverfolgung-332537>

⁷<https://mullvad.net/de>

- Die Smartphone Apps von Mullvad VPN enthalten keine Tracker und fordert nur die minimal nötigen Berechtigungen.
- Man kann auf PCs die Standardsoftware für OpenVPN oder Wireguard nutzen.

ProtonVPN hebt sich durch einige Sicherheitsfeatures von anderen Anbietern ab.⁸

- ProtonVPN bietet Server für OpenVPN und IPsec/IKEv2 mit starker Krypto.
- Es gibt ein kostenloses Angebot und Premiumangebote für 4,- Euro (zwei Geräte, kein Streaming) 8,- Euro (inklusive Video Streaming) bis 24,- Euro monatlich.
- Es ist empfehlenswert, auf Smartphones die Apps von ProtonVPN zu nutzen. Es sind nur notwendige Freigaben erforderlich und keine Tracker enthalten aber dafür zusätzliche Sicherheitsfeatures wie den *Netzwerk Kill Switch* für Android oder *Always-on-VPN* für iPhones.
- Windows 10, MacOS (El Capitan) und Linux unterstützen IPsec/IKEv2 oder OpenVPN standardmäßig.

IVPN.net ist auf Gibralta registriert. Der Hauptteil des Teams sitzt in Berlin.

- IVPN.net bietet Wireguard, OpenVPN und IPsec/IKEv2 Server in 32 Ländern, 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 und zus. 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, Telefonnummer oder E-Mail Addr. 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.

Der **erste VPN Provider**, dem man vertrauen kann, ist man selbst mit eigener Technik.

- Wenn man einen kleinen Server im eigenen Firmen- oder Heimnetz betreibt, kann man ihn zu einem VPN Server mit IPsec, OpenVPN oder Wireguard aufrüsten.
- Fritz!Boxen könnten out-of-the Box als VPN Server eingesetzt werden, wenn keine hohen Ansprüche an die Sicherheit der VPN-Verbindung gestellt werden. Für Smartphones ist Fritz!VPN nicht geeignet. Außerdem ist Fritz!VPN NICHT geeignet, um eine sichere Verbindung ins Firmennetz oder zwischen Standorten aufzubauen.
- Telekom Router der Baureihe Speedport Smart 3 enthalten eine rudimentäre Wireguard Implementierung, die hinsichtlich einfachster Bedienung optimiert wurde. Mit wenigen Klicks wird eine Wireguard Konfiguration für einen einzelnen Nutzer erstellt, die man via QR-Code oder Konfigurationsdatei auf einem Client importiert.

⁸<https://protonvpn.com/de>

13.3 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, um die VPN-Verbindung auszuwählen.
 - 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 CA⁹ 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).

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
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
```

⁹https://protonvpn.com/download/ProtonVPN_ike_root.der

- 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.

13.4 Verschiedene VPN Lösungen für Linux

- 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.

- 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-Verbindung mit Boardmitteln konfiguriert. Dabei handelt es sich nicht um Bugs (im Sinne einer Fehlfunktion des VPN) sondern um Features im Routing, die man durch geeignete Konfiguration vermeiden kann (s.u.)

13.4.1 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 resolvconf
Fedora: > sudo dnf install openvpn NetworkManager-openvpn-gnome resolvconf
```

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 37.120.217.163
remote 91.207.172.187
remote 93.177.73.35
remote 37.120.217.83
remote 194.126.177.11
remote 194.126.177.12

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-----
MIIFozCCA4ugAwIBAgIBATANBgkqhkiG9w0BAQOFADBAMQswCQYDVQQGEwJDSDEV
MBMGA1UEChMMUHJvdG9uV1BOIEFHMR0wGAYDVQQDEExFQcm90b25WUE4gUm9vdCBD
...
-----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

Abbildung 13.1: NetworkManager OpenVPN Import: Login Credentials eingeben

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 13.1).

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.
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 13.2).

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
```

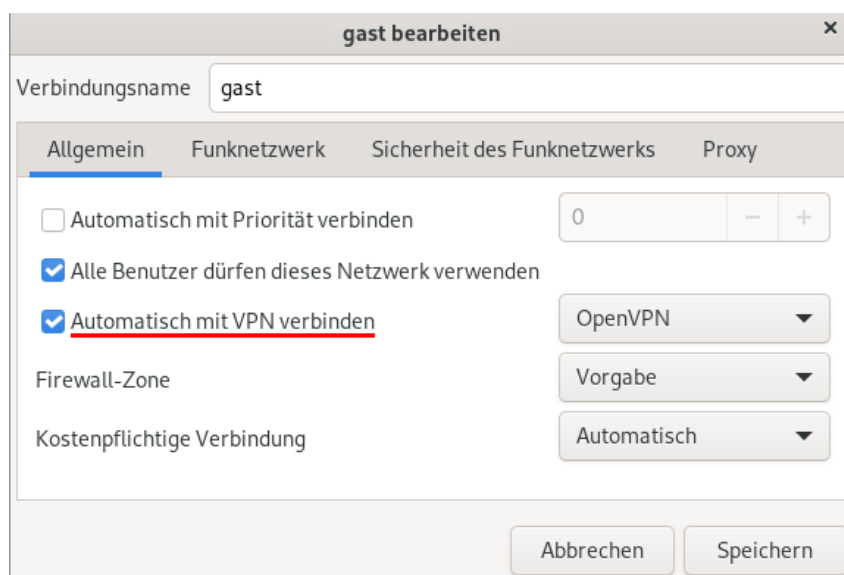



Abbildung 13.2: VPN mit einer Netzwerkverbindung automatisch starten

13.4.2 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.
- 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 sondern muss Konfigurationsdateien verwenden. Konfigurationsdateien ohne PostUp- und PostDown-Scripte kann man im NetworkManager importieren.

Vorbereitung des eigenen Rechners

1. Als erstes ist die Wireguard Software zu installieren:

```

Ubuntu: > sudo apt install wireguard resolvconf
Fedora: > sudo dnf install wireguard-tools resolvconf

```

2. Dann muss man seinen eigenen privaten und öffentlichen Schlüssel erzeugen:

```

> sudo su
# cd /etc/wireguard
# umask 077
# wg genkey | tee privatekey | wg pubkey | tee publickey
bjqCt8IJ20zbf3kLxvJ3mYGjTF+oe7Dg5vgyKqG4gU=

```

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.

Wenn der VPN-Provider die öffentlichen Schlüssel der Wireguard Server zum Download anbietet, auf der Webseite einen Upload der öffentlichen Schlüssel der Nutzer erlaubt, eine IP-Adresse für das Wireguard Interface zuteilt und wenn man keine Angst vor einem Full-Text Adventure hat, könnte man auch Wireguard unter Linux direkt nutzen.

Dann kann man eine Konfigurationsdatei `/etc/wireguard/wg0.conf` für die Verbindung zum ersten Wireguard Server erstellen. Wenn man zwischen mehreren Servern wechseln möchte, muss man für jeden Wireguard Server eine Konfigurationsdatei `wgX` erstellen.

Da die Konfigurationsdatei den privaten Schlüssel enthält, darf sie ausschließlich für `root` lesbar sein und es sollten keine Kopien irgendwo in `$HOME` Verzeichnissen rumliegen. (Der Schutz der Schlüssel ist wichtig in der Kryptografie und wird oft unterschätzt.)

```

[Interface]
PrivateKey = <privater Schlüssel>
Address = <IP für den eigenen Peer>/32
DNS = <IP vom DNS Server>
PostUp = /etc/wireguard/wg0-postup.sh
PostDown = /etc/wireguard/wg-all-postdown.sh
[Peer]
PublicKey = <öffentlicher Schlüssel des Servers>
Endpoint = <Server-Adresse>:<Port>
AllowedIPs = 0.0.0.0/0

```

- Die IP-Adresse für den eigenen Peer findet man auf der Webseite des VPN-Providers nach dem Login. Man muss seinen public Key hochladen und dann wird eine IP-Adresse zugewiesen. An die IP-Adresse ist `/32` für den Netzbereich anzuhängen.
- Den empfohlenen DNS-Server findet man in der Doku oder FAQ des VPN-Providers. In der Regel bieten guten VPN Provider DNS Server IPs mit und ohne Werbefilter. Man könnte auch andere DNS-Server nutzen, die vom VPN-Server erreichbar sind.
- Den öffentlichen Schlüssel des Servers sowie den DNS-Namen bzw. IP-Adresse findet man in der Serverliste des VPN-Providers. Der Port muss ebenfalls angegeben werden. Oft wird Port 51820 verwendet, den man ausprobieren kann, wenn in den FAQ nichts erwähnt wird. Aber einige Provider verwenden andere Ports. IVPN.net bietet die Ports 53, 2049, 2050, 30587, 41893, 48574 oder 58237 an. Man sollte also in den FAQ nachschauen.
- Die letzte Zeile bedeutet, dass die Gegenstelle (also der VPN-Server) das gesamte Internet zur Verfügung stellt (0.0.0.0/0: alle IPv4 Adressen).

- Mit den PostUp und PostDown Skripten kann man IPv6 deaktivieren und die Firewall für VPN-Nutzung umkonfigurieren. Ein Beispiel für UFW:

```
#!/bin/sh
# IPv6 deaktivieren
echo 1 > /proc/sys/net/ipv6/conf/all/disable_ipv6
# UFW Firewall Konfiguration für Wireguard Interface "wg0"
ufw reset
ufw default reject outgoing
ufw default deny incoming
ufw allow out on wg0 from any to any
ufw allow out from any to <VPN Server Adresse>
```

Das PostDown Skript stellt den ursprünglichen Zustand wieder her:

```
#!/bin/sh
# IPv6 aktivieren
echo 0 > /proc/sys/net/ipv6/conf/all/disable_ipv6
# UFW Firewall (normale Konfiguration)
ufw reset
ufw default allow outgoing
ufw default deny incoming
```

Beide Skripte müssen ausführbar gemacht werden:

```
> sudo chmod +x /etc/wireguard/wg0-postup.sh
> sudo chmod +x /etc/wireguard/wg-all-postdown.sh
```

Wireguard VPN starten

Die Verbindung zum Wireguard VPN-Server startet man mit folgendem Kommando:

```
> sudo wg-quick up wg0
```

Mit folgendem Kommando beendet man die Verbindung zu diesem VPN-Server:

```
> sudo wg-quick down wg0
```

Systemd kann das Wireguard-VPN auch 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 systemctl reset-failed
```

Mit Wireguard ins Firmennetz oder private Heimnetz (mit DNS-Server)

Wenn man normal im Internet surfen will aber als Road Warrior bzw. im Home Office zusätzlich Zugriff auf interne Ressourcen in der Firma benötigt oder aus dem Hotel auf das private Heimnetz zugreifen will, könnte man folgende Konfiguration für *wg1.conf* als Inspiration verwenden:

```
[Interface]
PrivateKey = <privater Schlüssel>
Address = 172.22.22.211/32
DNS = 172.22.22.3
PostUp = /usr/bin/resolvectl domain wg1 grotta.del.cane
[Peer]
PublicKey = <öffentlicher Schlüssel des Servers>
Endpoint = caneHome.dedyn.io:51820
AllowedIPs = 172.22.22.0/24
```

- Der VPN-Server für das Hausnetz ist über eine Dyn-DNS Adresse erreichbar. Genauer betrachtet erreicht man über diese Dyn-DNS Adresse einen Router, auf dem für Port 51820 (UDP) ein Portforwarding zum VPN-Server konfiguriert wurde.
- Der VPN-Server bietet Zugang zu dem privaten Netz 172.22.22.0/24 (als Beispiel).
- In diesem privaten Netz steht ein DNS-Server mit der IP-Addr. 172.22.22.3.
- Da Wireguard keine Split-DNS Konfiguration für systemd-resolved out-of-the-box unterstützt, wird mit dem PostUp Befehl festgelegt, dass dieser DNS-Server nur für Auflösung von internen Adressen mit dem DNS Suffix grotta.del.cane (als Beispiel) verwendet werden soll.

Wenn man sich mit dem eigenen DNS-Server viel Mühe gegeben hat und Tracking Adressen blockiert, DNSsec aktiviert hat usw. dann möchte man vielleicht diesen DNS-Server für alle Anfragen verwenden, sobald das VPN verfügbar ist. Dann muss man diesen Server als +DefaultRoute in der DNS Konfiguration setzen.

Der PostUp Befehl wäre dann:

```
PostUp = /usr/bin/resolvectl default-route wg1 true
```

Mit Wireguard ins Firmennetz oder ins private Heimnetz (ohne DNS-Server)

Wenn man nur wenige Ressourcen aus dem privaten Firmen- oder Hausnetz nutzen möchte (NextCloud Server, Datenspeicher, Drucker), könnte man sich den privaten DNS-Server auch sparen. Man schreibt diese IP-Adressen mit DNS-Namen in die Datei `/etc/hosts`:

```
172.22.22.5 nextcloud.grotta.del.cane nextcloud
172.22.22.6 speicher.grotta.del.cane speicher
172.22.22.7 drucker.grotta.del.cane drucker
```

Die Wireguard Konfiguration vereinfacht sich damit.

```
[Interface]
PrivateKey = <privater Schlüssel>
Address = 172.22.22.211/32
[Peer]
PublicKey = <öffentlicher Schlüssel des Servers>
Endpoint = caneHome.dedyn.io:51820
AllowedIPs = 172.22.22.0/24
```

Diese einfache Konfiguration könnte man im NetworkManager importieren, um sie später mit zwei Klicks zu starten und jederzeit parallel mit anderen VPNs zu verwenden.

```
> sudo nmcli con import type wireguard file /etc/wireguard/wg1.conf
```

Wireguard Server Konfiguration

Zur Vollständigkeit noch die Wireguard Server Konfiguration für ein privates Setup:

```
[Interface]
PrivateKey = <privater Schlüssel des Servers>
Address = 172.22.22.1/24
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 ufw proto udp allow 51820
Fedora: > sudo firewall-cmd --add-port=51820/udp --permanent --zone=public
```

13.4.3 Firewall Kill-Switch-Konfiguration für VPNs mit UFW

Wenn man eine VPN-Verbindung zu einem VPN Provider aktiviert, dann möchte man in der Regel 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 Uncomplicated Firewall (UFW) kann man das erzwingen und verhindert damit WebRTC Leaks und DNS Leaks oder dass Daten direkt 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 benötigt 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 konfigurieren 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 beispieldscript.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
```

13.5 Das VPN Exploitation Team der NSA

Aus den Dokumenten, die Edward Snowden bei der NSA rausgetragen hat, ist bekannt, dass die in 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 Attack¹⁰ 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 Informationsvorsprung 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-Server so, als ob er der Client wäre. Während der Kommunikation sitzt der Angreifer janusköpfig zwischen beiden und kann alles mitlesen.
- 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. (Nov. 2013)¹¹

(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 Attack¹² 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 geeignet sein könnten. Diese Schlüssel werden gesammelt und automatisiert genutzt. (Es gibt immer Admins, die diese Schlüssel per E-Mail verteilen.)

¹⁰<https://weakdh.org>

¹¹<https://twitter.com/ioerror/status/398059565947699200>

¹²<https://www.rc4nomore.com>

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.

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*¹³).

¹³<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 Webserver, der die gewünschte Webseite liefern könnte. Üblicherweise wird der DNS-Server des Zugangsproviders gefragt, also z. B. Telekom, Vodafone...
3. Der angefragte DNS-Server erkundigt sich daraufhin bei den Servern der Root-Zone nach dem DNS-Server, der für die Toplevel Domain .de zuständig ist. Dann fragt er dieses Server nach dem DNS-Server, der für die Domain privacy-handbuch.de zuständig ist und diesen DNS-Server nach der IP-Adresse des Webserver für www.privacy-handbuch.de.
4. Wenn ein passender Webserver gefunden wurde, dann wird die IP-Adresse an den Browser zurück 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 alle Webserver, die man kontaktiert. Außerdem kann der DNS-Server durch Manipulation der Antworten entscheiden, welche Webseiten der Surfer sehen kann und welche Dienste man nutzen kann.

Möglichkeit zur Zensur

Die Möglichkeit der DNS-Manipulation zur Zensur des Internetzugangs sollte 2009 mit dem Zugangerschwerungsgesetz (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 die Provider die Nutzung alternativer, unzensurierter DNS-Server verhindern.

Neben dem damaligen Innenminister Schäuble haben sich besonders Hr. v. Guttenberg und die damalige Familienministerin Ursula von der Leyen für das Gesetz engagiert. Frau v.d.Leyen wurde dafür mit dem Big Brother geehrt. Aufgrund des Widerstandes der Zivilgesellschaft wurde das ZugErschwG wieder aufgehoben.

Aktuell wird die Sperrung von Webseiten in Iran, Türkei, Ukraine, Süd Korea oder Vietnam beispielsweise nach diesem Muster umgesetzt und 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 zur Umgehung der Zensur blockiert wird und DNS Anfragen auf Port 53 immer an die kompromittierten Server umgeleitet wird. Nur verschlüsseltes DNS ermöglicht eine Umgehung der 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 Zertifikaten 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 eigene 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/* anzulegen mit folgendem Inhalt:

```
[Resolve]
DNSSEC=true
```

14.2 Verschlüsselung des DNS Datenverkehr

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 umgesetzt.

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 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. DNSCrypt 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 Betriebssystem 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 Umgehung von Zensur auf Basis von DNS Manipulationen und ist aufgrund des HTTP Overhead einig Millisekunden langsamer als normales DNS.

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 der/die DNS-Server die eigene IP-Adresse protokollieren kann.

Man erreicht das gleiche Ziel aber auch ohne Performance Einbußen, indem man einen vertrauenswürdigen DNS-Server mit No-Logging-Policy verwendet.

Abgesehen von einigen Szenarien mit höchsten Sicherheitsanforderungen, für die es schwer fällt, ein plausibles Beispiel zu konstruieren, ist DoHoT meist Overkill.

Oblivious DNS-over-HTTPS wurde von Cloudflare im Dez. 2020 initiiert, weil es Vorbehalte in Europa gegen die Nutzung von Cloudflare als Default Trust-Recursive-Resolver (DoH) in Firefox gab. Derzeit läuft der Standardisierungsprozess.

Cloudflare ist nicht daran interessiert, welche Webseiten Lieschen Müller oder Pitschie Hufnagel aufrufen. Sie interessieren sich für eine globale Sicht, welche neuen Ideen gewinnen an Popularität, was ist der neue *heiße Shit* und was ist andererseits auf dem absteigenden Ast. Diese Informationen frühzeitig zu haben ist wertvoll, wie es Google mit seiner Suchmaschine demonstriert. Für Cloudflare 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-Bahn 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 Zugangs-Provider 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 auch 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 (USA, GB) aber in Deutschland nicht. Zensur durch DNS-Server spielt nach der Abwehr des ZugErschwG in Deutschland auch nur eine geringe Rolle, könnte in seltenen Fällen aber auch mal ein Grund sein.

Hinweis: Ein Trackingdienst könnte ermitteln, welcher DNS-Server vom Browser verwendet wird, und diese Information als Parameter für das Fingerprinting des Browser 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, 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 Schutz¹ kann man als Alternative zu den Default DNS-Servern der Provider empfehlen:

- Freifunk München² (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!)

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/>

- 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 Denmark⁴ (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:

- dismail.de⁵ (mit DNS-over-TLS)
 - IPv4: 80.241.218.68 / IPv6: 2a02:c205:3001:4558::1 / fdns1.dismail.de
 - IPv4: 159.69.114.157 / IPv6: 2a01:4f8:c17:739a::2 / fdns2.dismail.de
- dnsforge.de⁶ (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.com⁷ (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: 95.216.212.177 / 2a01:4f9:c010:43ce::1 / dot-fi.blahdns.com

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.com
 - IPv4: 94.140.15.15 / IPv6: 2a10:50c0::ad2:ff / dns.adguard.com
- AdGuard DNS-Server OHNE Werbe- und Trackingfilter:
 - IPv4: 94.140.14.140 / IPv6: 2a10:50c0::1:ff / dns-unfiltered.adguard.com
 - IPv4: 94.140.14.141 / IPv6: 2a10:50c0::2:ff / dns-unfiltered.adguard.com

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, Schweiz, Schweden, Großbritannien, Singapur, Australien sowie USA und sind unter einer einheitlichen IP-Adresse erreichbar.⁹

- Mullvad DoT- und DoH-Server MIT Werbe- und Trackingfilter:
 - IPv4: 194.242.2.3, 193.19.108.3 / IPv6: 2a07:e340::3 / adblock.doh.mullvad.net
- Mullvad DoT und DoH-Server OHNE Werbe- und Trackingfilter:
 - IPv4: 194.242.2.2, 193.19.108.2 / IPv6: 2a07:e340::2 / doh.mullvad.net

⁴<http://blog.uncensoreddns.org>

⁵<https://dismail.de/info.html>

⁶<https://dnsforge.de/>

⁷<https://blahdns.com>

⁸<https://adguard.com>

⁹<https://mullvad.net/de/help/dns-over-https-and-dns-over-tls>

Einige DNS Server filtern Tracking und Malware Domains. Die Grenze zur Zensur ist dabei schmal und es 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. Dazu zählen die russischen Nachrichtenseite *RT International*, die franz. *VoltaireNet.org* und viele US Webseiten.

Unabhängig von den Diskussionen um Fake News, die wesentlich vom politischen Weltbild des Betrachters abhängt, ist die Sperrung von Informationsangeboten Zensur. Und ein unzensurierter 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 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 Zugangsprovider, wie es 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 Datenschutz(m)utz Policy¹⁰ von Google. Ziel ist, 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 es 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
```

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 Thread Intelligence Providern zusammen. Deren Erkenntnisse über Cyber-Angriffe werden gesammelt, um die Abwehr von kriminellen Angriffen und Wirtschaftsspionage auf DNS-Ebene zu konsolidieren. Im Gegenzug erhalten die Thread Intelligence Provider Zugriff auf den (anonymisierten) DNS-Traffic bei einem Angriff, 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 und 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 weltweite sehr schnelle DNS-Server bereit, die hinsichtlich Geschwindigkeit Google DNS und Quad9 übertreffen.¹¹

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

¹⁰<https://policies.google.com/privacy?hl=de&gl=de>

¹¹<https://1.1.1.1/de/>

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 ist. Im Blog Artikel wird darauf hingewiesen, dass man mit den DNS-Servern via DoT oder DoH die länder-spezifischen Sperren wie z. B in der Türkei umgehen kann, aber man kann davon ausgehen, dass Cloudflare die Anforderungen der US-Administration umsetzen wird.

DNSSEC ist aktiv, außerdem ist DNS-over-TLS und DNS-over-HTTPS nutzbar.

14.5 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 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 Portalseite aufrufen zu können.

In dem Applet in der Taskleiste des Desktop wählt man den Menüpunkt *Verbindungen bearbeiten*. In dem sich öffnenden Fenster kann man für jede Internet-Verbindung (LAN, WLAN...) die DNS-Server konfigurieren. Der NetworkManager kümmert sich dann darum, dass die gewünschten Einstellungen beim Herstellen der Internetverbindung aktiviert werden. (Ist ein 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](#))

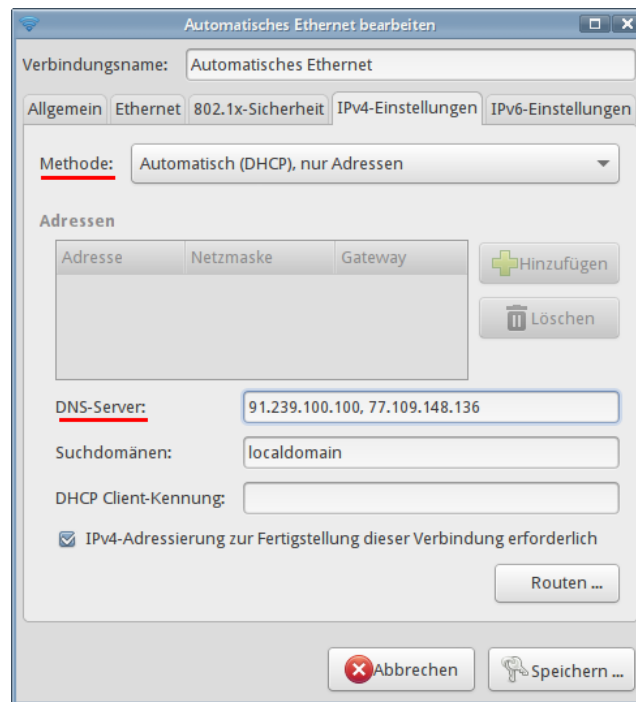


Abbildung 14.1: Konfiguration der DNS-Server im NetworkManager (Linux)

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 *Simple DNSCrypt Daemon* verwenden.¹²

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 verwendet.

Linux Distributionen verwenden überwiegend *systemd-resolve* für die DNS Namensauflösung. *systemd* Version > 245.2-1 (Ubuntu 20.04+, Fedora 32+) beherrscht DNS-over-TLS und man kann es 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 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:

¹²<https://simplifiednscrypt.org>

```
[main]
dns=none
systemd-resolved=false
```

Hinweis: diese Konfiguration ist nicht für Road Warrior geeignet, die unterwegs WiFi Hotspots mit Login Webseite 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).

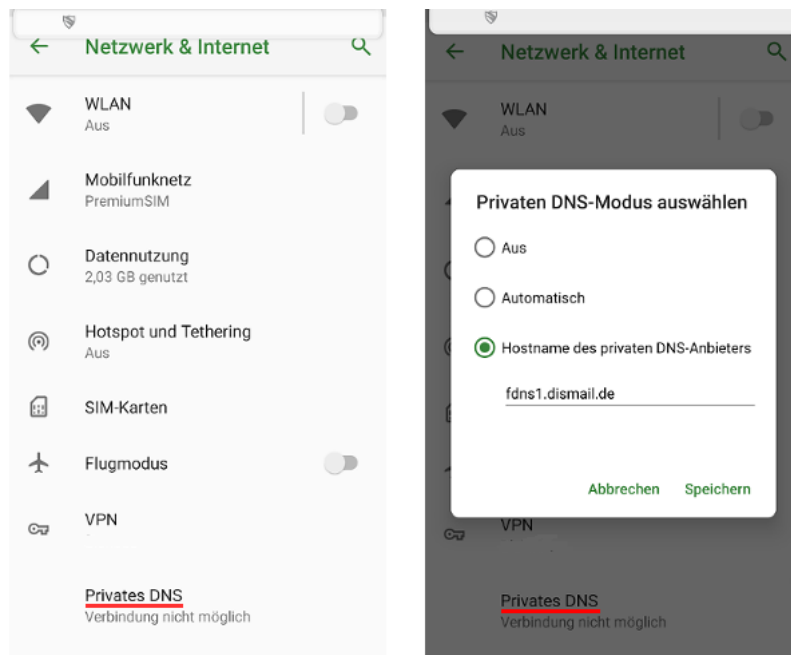


Abbildung 14.2: Android: DNS-over-TLS aktivieren

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.

Man muss sich ein Konfigurationsprofil für den DNS Server herunterladen. Es gibt mehrere Webseiten (z. B. encrypted-dns.party), die Profile für einige DNS Server bereitstellen. Es ist aber empfehlenswert, ein signiertes Profil direkt vom Anbieter herunter zu laden, 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 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.

Investigative Journalisten, Rechtsanwälte und auch Priester haben das Recht und die Pflicht, 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 kurzen Beispiele zeigen, dass unterschiedliche Anforderungen an eine Verschlüsselung bestehen können. Bevor man wild anfängt, alles irgendwie zu verschlüsseln, sollte man sich 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 ebenfalls 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 Verzeichnis-basierte Ansätze wie *Boxcryptor* oder *Cryptomator* (beide für Windows, MacOS, Linux und Smartphones verfügbar).
5. Wer eine **Manipulation der Systemdaten** befürchtet, kann seinen Rechner komplett verschlüsseln (z. B. mit dm-crypt für Linux).

15.1 Konzepte der vorgestellten Tools

Um die vorgestellten Tools sinnvoll einzusetzen, ist es nötig, die unterschiedlichen Konzepte zu verstehen.

GnuPG arbeitet Datei-orientiert. Einzelne Dateien können verschlüsselt werden. Die unverschlüsselten Originaldateien sind danach sicher(!) zu löschen, damit keine Spuren auf der Festplatte bleiben.

Cryptomator, Boxcryptor arbeiten Verzeichnis-basiert. Es gibt zwei Verzeichnisse:

1. Das Verzeichnis A mit den verschlüsselten Daten wird auf den Datenträger geschrieben bzw. in die Cloud synchronisiert.
2. Ein zweites Verzeichnis B oder ein virtuelles Laufwerk bietet den transparenten Zugriff auf die entschlüsselten Daten.

Für alle Schreib- und Leseoperationen wird das Verzeichnis B verwendet, wo man die Daten unverschlüsselt sieht, sobald Cryptomator oder Boxcryptor gestartet wurden.

Veracrypt, dm-crypt 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 eingefügt) 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 bzw. gelöscht werden. Die Verschlüsselung erfolgt transparent ohne weiteres Zutun des Nutzers.

Veracrypt - mit doppeltem Boden

Veracrypt¹ ist ein Nachfolger des legendären Truecrypt. Es beseitigt einige Schwächen, die bei einem Audit von Truecrypt² aufgedeckt wurden und wird als Open Source weiterentwickelt. Mit zuluCrypt gibt es eine 100% kompatible Linux Software.

Ein besonderes Feature von Veracrypt ist das Konzept des *versteckten Volumes*, eine Art doppelter Boden für den verschlüsselten Container. Der Zugriff auf diesen Bereich ist mit einem zweiten Schlüssel geschützt, einer weiteren Passphrase und/oder Schlüsseldatei(en). 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 versteckten 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.

¹<https://www.veracrypt.fr/en/Home.html>

²https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf

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, Google Desktop Search...) liefern möglicherweise Hinweise auf den versteckten Container.

Veracrypt - CIPHERauswahl

Veracrypt bietet verschiedene Verschlüsselungsalgorithmen (Cipher) und -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 vollen Schutz von 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 alle Cipher testen. Welchen Cipher man wählt, ist dabei egal, Hauptsache nicht AES.

15.2 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 zufälligen Zufallszahlen generiert, die als Schlüssel für die symmetrische Verschlüsselung mit AES256-XTS o.ä. dient.
2. Dieser Schlüssel aus zufälligen 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 oder... 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 damit 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 somit der entscheidende Faktor für die Sicherheit der Datenverschlüsselung und gleichzeitig auch oft das schwächste Glied in der Kette. Eine Passphrase, welche die gleiche Stärke gegen Brute-Force Angriffe wie AES128 hätte, müsste beispw. 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 schwächsten 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 mind. 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 (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 von einem leicht merkbaren Satz ableiten und den variablen Anteil aus der Verwendung:

- 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 verwendet statt zufälliger Zeichenkombinationen. Wortkombinationen kann man sich leichter merken als sinnlose Zeichenkombinationen.

Für den klassischen Weg zur Erstellung einer Diceware Passphrase benötigt man eine Wortliste (beispw. die *DeReKo Liste*³ mit den häufigsten deutschen Wörtern laut Leibnitz Institut) und einen Würfel. Für jedes Wort würfelt man 5x und erhält damit einen Zahlenkombination. Diese Zahlenkombination 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.⁴

- Beim **Challenge-Response** Verfahren mit Yubikeys wird ein simples, 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:

³<https://www.privacy-handbuch.de/download/diceware-dereko.txt>

⁴<https://online-wuerfel.de/5-wuerfel>

- KeePassXC Datenbanken für Passwörter können damit geschützt werden.
- dmccrypt/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 Repositories:

```
> sudo apt install yubikey-personalisation
```

Dann wird der zweite PW-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 Regelungen:

- 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. Man kann oder glaubhaft(!) versichert, 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 2 Jahre Gefängnis oder Geldstrafen. Dass die Anwendung des Gesetzes nicht auf böse Terroristen beschränkt ist, kann man bei Heise.de nachlesen. Es wurde als erstes gegen eine Gruppe von Tierschützern angewendet.⁵

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.⁶

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 eingeschalteten 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.⁷

⁵<http://www.heise.de/newsticker/meldung/99313>

⁶<https://www.eff.org/wp/digital-privacy-us-border-2017>

⁷<http://motherboard.vice.com/de/read/bis-das-sek-kommt>

15.3 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 sinnvoll wie Steuererklärungen, Mitgliederlisten für politisch aktive Vereine... usw.

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. 15.1).

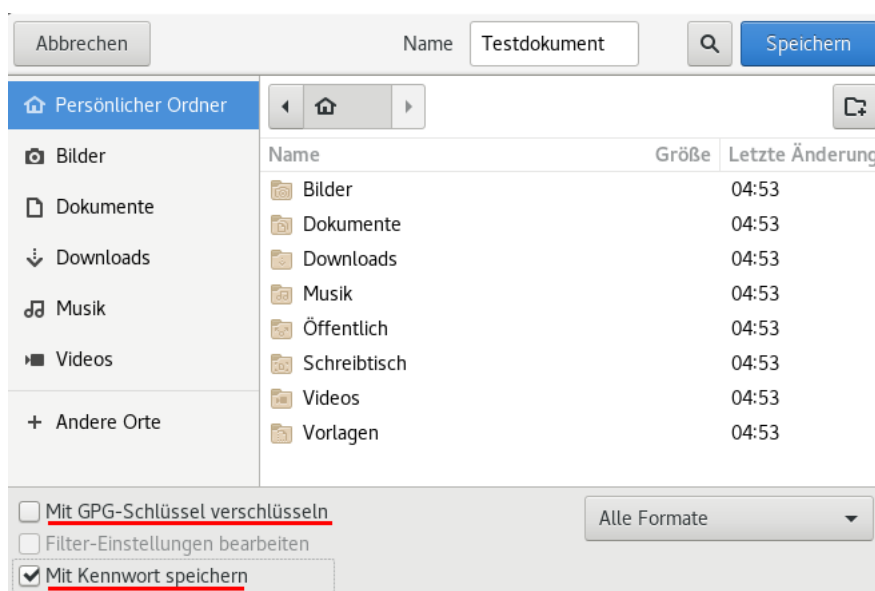


Abbildung 15.1: Verschlüsselte Speicherung in LibreOffice aktivieren

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, so dass ihm beim Öffnen des Dokumentes der vertrauliche Inhalt via Internet zugesendet wird.⁸

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.

⁸<https://www.pdf-insecurity.org/>

15.4 Quick and Dirty mit GnuPG

Eine Möglichkeit ist die Verschlüsselung einzelner Dateien oder Verzeichnisse mit GnuPG. Die grafischen Tools *GPA* (GNU Privacy Assistant) oder *Kleopatra* bieten dafür im Menü den Punkt *Datei - Datei verschlüsseln/signieren* und *Datei - Datei entschlüsseln/prüfen*.

Noch einfach geht es, wenn man im bevorzugten Dateimanager mit der rechten Maustaste auf eine Datei klickt und in dem Kontextmenü den Punkt *Datei verschlüsseln* wählt. Es startet ein Assistent, der durch die Auswahl der Schlüssel usw. führt.

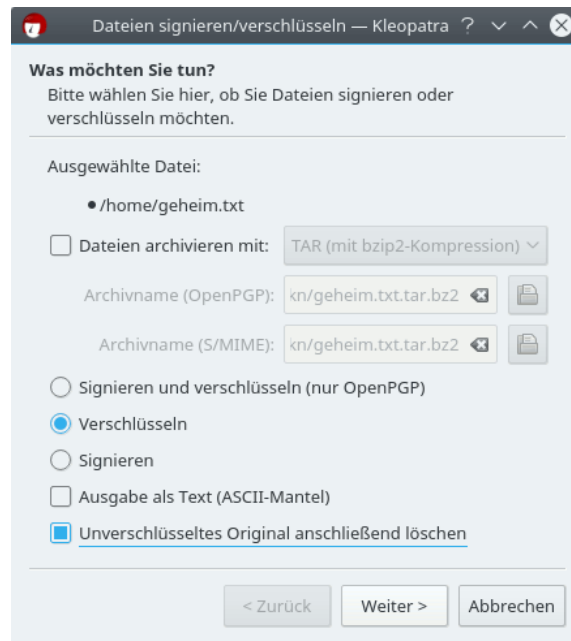


Abbildung 15.2: Kleopatra GnuPG GUI: Assistent zur Verschlüsselung von Dateien

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**⁹ zu installieren.

⁹<https://www.gpg4win.org>

15.5 dm-crypt/LUKS für Linux

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 und nicht mit Passwörtern).

dm-crypt/LUKS verschlüsselt Blockdevices (Festplattenpartitionen, USB-Sticks oder Imagedateien) und arbeitet vollständig transparent. Es können bis zu 8 unterschiedliche Passphrasen + 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.

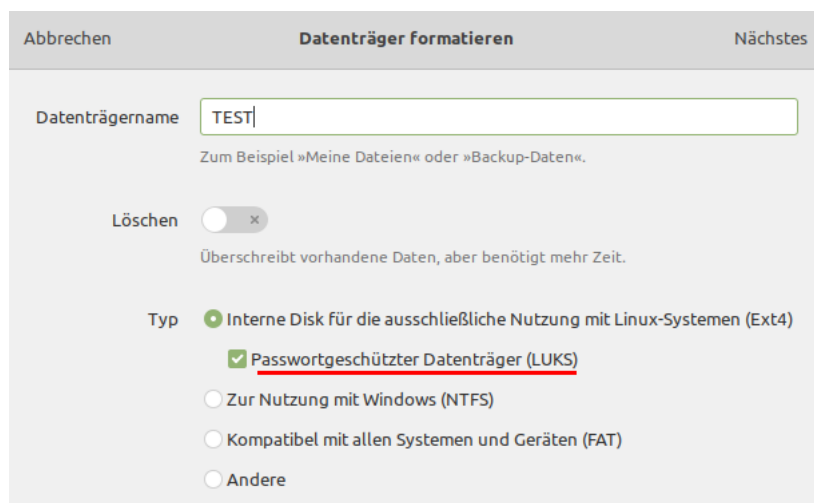


Abbildung 15.3: Datenträger verschlüsseln unter Linux

Im nächsten Schritt wird man nach der Passphrase gefragt, die man wie üblich 2x 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.

15.5.1 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 System mit dm-crypt/LUKS ist dann nur ein kleines Häkchen zu setzen.

Beim Linux Mint Installer findet man die Option in den *Erweiterten Funktionen*.... Bei anderen Linux Distributionen sieht es irgendwie ähnlich aus.

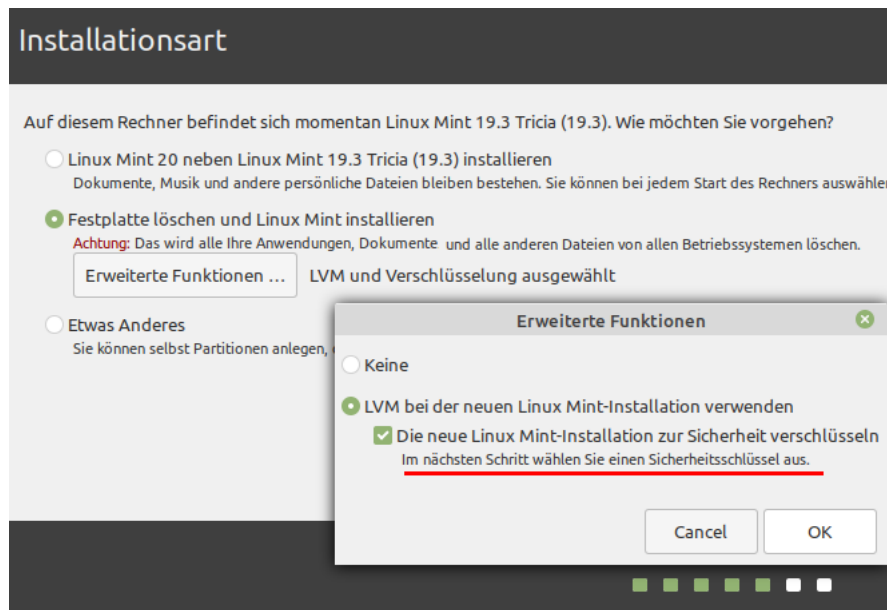


Abbildung 15.4: Linux Mint bei der Installation komplett verschlüsseln

15.5.2 Für Genießer in der Konsole mit cryptsetup

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 3x 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. 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.ext3 /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 zu 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
```

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 Container 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 *geheim.img* zu verwalten, ist die Imagedatei 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...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, eine Zahl von 0...7. Es ist also 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>
...
Key Slot 0: DISABLED
Key Slot 1: ENABLED
```



```

Iterations:
Salt:

Key material offset:
AF stripes:
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED

```

Komfortabel beim Login

Mit Hilfe des Modules pam-mount ist es möglich, das Anmeldepasswort zu nutzen, um standardmäßig beim Login einen oder mehrere Container zu öffnen. Insbesondere für verschlüsselte /home Partitionen ist dies sinnvoll und komfortabel.

Folgende Konfigurationen sind für einen Crypto-Login anzupassen:

1. **PAM-Konfiguration:** Dem PAM-Dämon ist mitzuteilen, dass er das Modul *mount* zu verwenden hat und das Login-Passwort zu übergeben ist. Gut vorbereitete Distributionen wie Debian und aktuelle Ubuntu(s) benötigen nur einen Eintrag in den Dateien */etc/pam.d/login*, */etc/pam.d/kdm* und */etc/pam.d/gdm*:

```
@include common-pammount
```

2. **pam-mount Modul:** Das Modul wird konfiguriert in der XML-Datei */etc/security/pam_mount.conf.xml*. Am Anfang der Datei findet man eine Section für Volumes, die beim Login geöffnet werden sollen. Im ersten Beispiel wird bei allen Logins die verschlüsselte Partition */dev/hda4* als */home* eingebunden:

```
<volume fstype="crypt" path="/dev/hda4" mountpoint="/home" />
```

Das zweite Beispiel zeigt die Einbindung einer verschlüsselten Containerdatei */geheim.luks* als HOME für den User Pitschie. Die Containerdatei wird nur geöffnet, wenn Pitschie sich anmeldet.

```
<volume user="pitschie" fstype="crypt" path="/geheim.luks"
      mountpoint="/home/pitschie" options="loop" />
```

3. **fstab:** Da beim Booten keine Partition nach */home* gemountet werden soll, ist evtl. der entsprechende Eintrag in der Datei */etc/fstab* zu löschen.

SWAP und /tmp verschlüsseln

Das */tmp*-Verzeichnis und der SWAP Bereich können unter Umständen persönliche Informationen enthalten, die im Verlauf der Arbeit ausgelagert wurden. Wenn eine komplette Verschlüsselung des Systems nicht möglich ist, sollte man verhindern, dass lesbare Datenrückstände in diesen Bereichen verbleiben.

Das Verzeichnis */tmp* kann man im RAM des Rechners ablegen, wenn dieser hinreichend groß dimensioniert ist. Mit dem Ausschalten des Rechners sind alle Daten verloren. Um diese Variante zu realisieren bootet man den Rechner im abgesicherten Mode, beendet die grafische Oberfläche (X-Server) und löscht alle Dateien in */tmp*. In der Datei */etc/fstab* wird folgender Eintrag ergänzt:

```
tmpfs /tmp tmpfs nosuid,noexec 0 0
```

Die Bereiche SWAP und */tmp* können im Bootprozess als verschlüsselte Partitionen mit einem zufälligen Passwort initialisiert und eingebunden werden. Mit dem Ausschalten des Rechners ist das Passwort verloren und ein Zugriff auf diese Daten nicht mehr möglich.

Achtung: Suspend-to-RAM und Suspend-to-Disk funktionieren mit einer verschlüsselten SWAP-Partition noch nicht.

Debian GNU/Linux

Debian und Ubuntu enthalten ein Init-Script, welches eine einfache Verschlüsselung von SWAP und */tmp* ermöglicht, wenn diese auf einer eigenen Partition liegen.

In der Datei */etc/crypttab* sind die folgenden Zeilen einzufügen, wobei */dev/hda5* und */dev/hda8* durch die jeweils genutzten Partitionen zu ersetzen sind:

```
cryptswp    /dev/hda5    /dev/urandom    swap
crypttmp    /dev/hda8    /dev/urandom    tmp
```

In der Datei */etc/fstab* sind die Einträge für swap und */tmp* anzupassen:

```
/dev/mapper/cryptswp    none    swap    sw    0 0
/dev/mapper/crypttmp    /tmp    ext2    defaults    0 0
```

Anschließend ist der Rechner neu zu booten und beide Partitionen sind verschlüsselt.

Achtung: Die Partition für */tmp* darf kein Dateisystem enthalten! Soll eine bereits verwendete */tmp*-Partition verschlüsselt werden, ist diese erst einmal nach dem Beenden des X-Servers(!) zu dismounten und zu überschreiben:

```
# umount /tmp
# dd if=/dev/zero of=/dev/hda8
```

15.5.3 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, Containerdatei). Dabei wird eine echt knackige, komplexe Passphrase verwendet, die einem Brute-Force Angriff hochpotenter Angreifer mehrere Jahre standhält.

Diese Passphrase benötigt man im nächsten Schritt zum Hinzufügen von Hardware Token und sie dient als Backup zum Öffnen des Containers, wenn das HW Token verloren geht. Sie wird *off site* in einem Tresor hinterlegt (digital oder auf Papier).

2. Ein oder mehrere Keyslots von LUKS werden mit Hardware Token vorbereitet und in der täglichen Arbeit genutzt. Zur Unterstützung sind ein paar kleine Scripte hilfreich.
3. Wenn man zwei oder mehr HW Token zum Öffnen des Container definiert hat (mind. ein Backup Token!), könnte man die initiale Passphrase im Keyslot 0 auch löschen:

```
> cryptsetup luksKillSlot <device> 0
```

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, die die Token die HMAC-Secret Erweiterung unterstützen (z.B. Nitrokey FIDO2, Yubikey ab Version 5).

Um zu prüfen, ob systemd hinreichend aktuell ist und die Option *fido2-device* unterstützt wird, ruft man am einfachsten das Kommando *sudo systemd-cryptenroll --help* auf.

1. 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
```

2. Danach wird der Container einmal mit der knackigen Passphrase geöffnet:

```
> sudo cryptsetup open --type luks <device> <name>
```

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 --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 --fido2-device=list <device>
```

4. Wenn das Linux System bei der Installation vollständig verschlüsselt wurde und man die verschlüsselte Systempartition mit einem FIDO2 Security Token öffnen möchte, entfallen 1+2. Statt dessen muss man in der Datei */etc/crypttab* für das Boot Device in der vierten Spalte die Option *fido2-device=auto* einzufügen:

```
<Name> <Gerät> - luks,fido2-device=auto...
```

Die bereits vorhandenen Parameter variieren bei den unterschiedlichen Linux Distributionen. Danach ist noch das Bootimage neu zu bauen mit:

```
> 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.

5. 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:

```
> 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...)
2. Im nächsten Schritt erstellt man den LUKS2(!) Container (USB-Stick, verschlüsselte Partition oder Containerdatei) und schützt ihn mit einer knackigen Passphrase.
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 nacheinander mehrere Token hinzugefügt werden oder gleichzeitig mit:

```
> sudo systemd-cryptenroll --pkcs11-token-uri=list <device>
```

5. Wenn das Linux System bei der Installation vollständig verschlüsselt wurde und man die verschlüsselte Systempartition mit einem PKCS#11 Token öffnen möchte, dann entfällt 2+3. Statt dessen muss man in der Datei */etc/crypttab* für das Boot Device in der vierten Spalte die Option *pkcs11-uri=auto* einzufügen:

```
<Name> <Gerät> - luks,pkcs11-uri=auto...
```

Die bereits vorhandenen Parameter variieren bei den unterschiedlichen Linux Distributionen. Danach ist noch das Bootimage neu zu bauen mit:

```
> 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.

6. 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 Smartcard im Format eines USB-Sticks gibt es bei Nitrokey, Yubikey oder GnuK. Die Idee ist einfach erklärt: Es wird die 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 erstmal 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 Schlüssel der Nitrokey Smartcard anzustoßen:

```
> gpg2 --export "User-ID" > /tmp/luks-gpg-key.gpg
> sudo gpg2 --import /tmp/luks-gpg-key.gpg
> sudo gpg2 --card-status
> rm /tmp/luks-gpg-key.gpg
```

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 Original 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 /boot Partition 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 einem LUKS Container, die mit einem Challenge-Response Verfahren arbeitet.

Die Passphrase wird als Challenge an den Yubikey gesendet, der mit kryptografischem Voodoo einen Response abgeleitet, der als Schlüssel zum Öffnen des Containers dient. Die Passphrase (Challenge) kann dabei einfach und leicht merkenbar sein, da der Yubikey als zweiter Faktor für das Öffnen des Containers nötig ist und ein starkes PW ableitet.

1. Die Software kann mit dem bevorzugten Paketmanager installiert werden:

```
> sudo apt install yubikey-luks yubikey-personalization
```

2. Der zweite PW-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. Es wird dabei 2x das neue Challenge Passwort für den Yubikey und 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 Container 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.

15.5.4 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 Repositories:

```
> sudo apt install cryptsetup-nuke-password
```

Im zweiten Schritt werden die Nuke Passphrase konfiguriert, die man 2x eingeben muss, und im Hintergrund 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 dass die Daten nicht mehr entschlüsselt werden können. Wenn man ein Backup des LUKS Header off-site speichert, kann man mit einer Linux Live-DVD die Daten wieder lesbar machen.

1. Ein Backup des LUKS Header 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-password* 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.)

15.6 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 dem zuluCrypt GUI arbeiten. Es verwaltet einerseits die geöffneten Container in einem übersichtlichen Hauptfenster und kann andererseits 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.

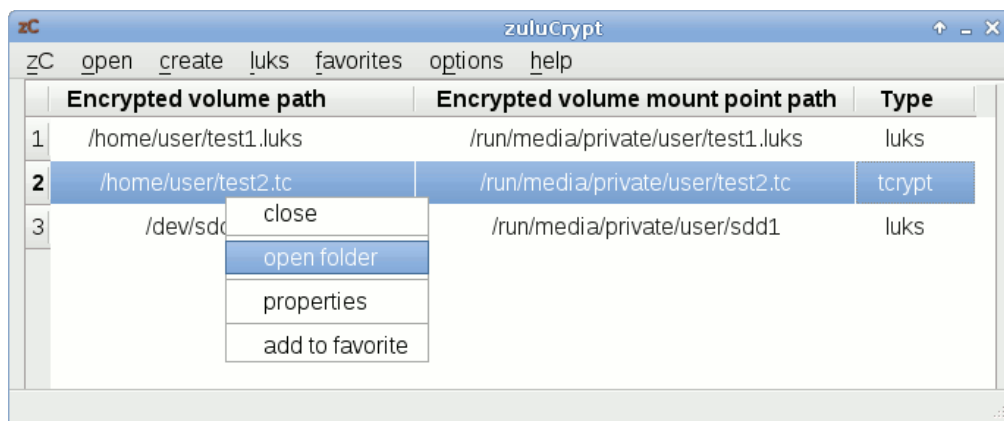


Abbildung 15.5: Hauptfenster von zuluCrypt

15.7 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.

Für das Backup der persönlichen Daten habe ich eine kleine Ideensammlung zusammengestellt, die keinen Anspruch auf Vollständigkeit erhebt. 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.

1. Die persönlichen Daten oder einzelne Verzeichnisse mit häufig geänderten Dateien könnte man regelmäßig mit einer Kopie auf einem verschlüsselten Datenträger synchronisieren (USB-Stick, externe Festplatte). Da nur Änderungen übertragen werden müssen, geht es relativ schnell.
2. Einzelne, in sich geschlossene Projekte könnten platzsparend als komprimiertes verschlüsseltes Archiv auf einem externen Datenträger abgelegt werden.
3. Größere abgeschlossene Projekte könnten auf einem optischen Datenträger dauerhaft archiviert werden.

15.7.1 Schnell mal auf den USB-Stick

Inzwischen gibt es preiswerte USB-Sticks mit beachtlicher Kapazität. Aufgrund der einfachen Verwendung sind sie für Backups im privaten Bereich gut geeignet. Für große Datenmengen kann man auch eine externe USB-Festplatte nutzen. Wer eine Beschlagnahme der Backupmedien befürchtet, findet vielleicht eine Anregung bei true-random¹⁰.

Das Backupmedium sollte man mit Veracrypt oder DM-Crypt 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 öffnen¹¹. 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.¹²

Unison-GTK

Für die Synchronisation der Daten steht z. B. Unison-GTK¹³ für verschiedene Betriebssysteme (auch WINDOWS) zur Verfügung und bietet ein GUI für die Synchronisation. Die Installation ist einfach: Download, Entpacken und Binary starten. Linuxer können das Paket *unison-gtk* mit der Paketverwaltung installieren.

¹⁰<http://true-random.com/homepage/projects/usbsticks/small.html>

¹¹<http://heise.de/-270060>

¹²<http://heise.de/-894962>

¹³<http://www.cis.upenn.edu/~bcpierce/unison/>

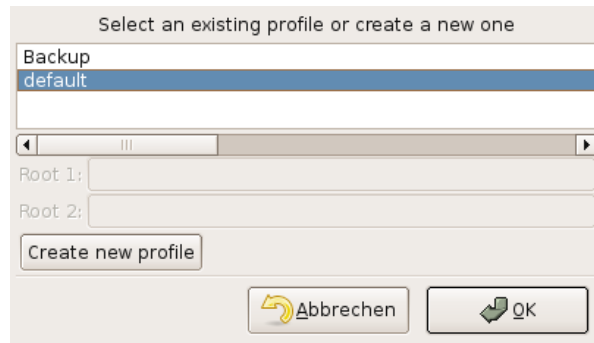


Abbildung 15.6: Profil nach dem Start von Unison-GTK auswählen

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 Profiles (Bild 15.6).

Nach Auswahl des Profiles analysiert Unison die Differenzen und zeigt im Hauptfenster an, welche Aktionen das Programm ausführen würde. Ein Klick auf *Go* startet die Synchronisation.

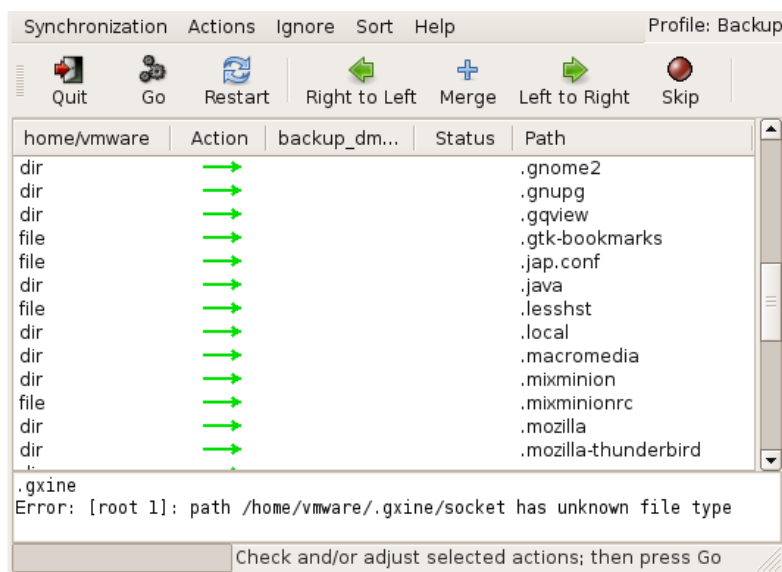


Abbildung 15.7: Hauptfenster von Unison-GTK

Achtung: Unison synchronisiert in beide Richtungen und eignet 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, kann Unison auch ein Backup auf einem anderen Rechner via FTP oder SSH synchronisieren.

rsync

Das Tool *rsync* ist in allen Linux-Distributionen enthalten und insbesondere für Skripte einfach verwendbar. Es synchronisiert die Dateien eines Zielverzeichnisses mit dem Quell-

verzeichnis und überträgt dabei nur die Änderungen. Ein Beispiel zeigt das Sichern der E-Mails und Adressbücher von Thunderbird:

```
rsync -av --delete $HOME/.thunderbird /backup_dir/
```

Der Befehl legt im *backup_dir* ein Verzeichnis *.thunderbird* 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.

Eine zweite Variante zum Sichern des gesamten *\$HOME* inklusive der versteckten Dateien und exklusive eines Verzeichnisses (mp3) mit großen Datenmengen:

```
rsync -av --delete --include=$HOME/. --exclude=$HOME/mp3 $HOME /backup_dir/
```

Die Option *-delete* löscht im Original nicht mehr vorhandene Dateien auch in der Sicherungskopie. Weitere Hinweise liefert die Manualpage von *rsync*.

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 alle versteckten Verzeichnisse und Dateien mit gesichert.

Ein Script, welches alle nötigen Verzeichnisse synchronisiert, ist schnell gestrickt. Eine backup-freundliche Struktur im *\$HOME*-Verzeichnis erleichtert dies zusätzlich.

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 wird ein Quell - und ein Zielverzeichnis sowie die *rsync*-Parameter zugeordnet. Ein Klick auf die kleine Rakete oben rechts startet die Synchronisation (Bild 15.8).

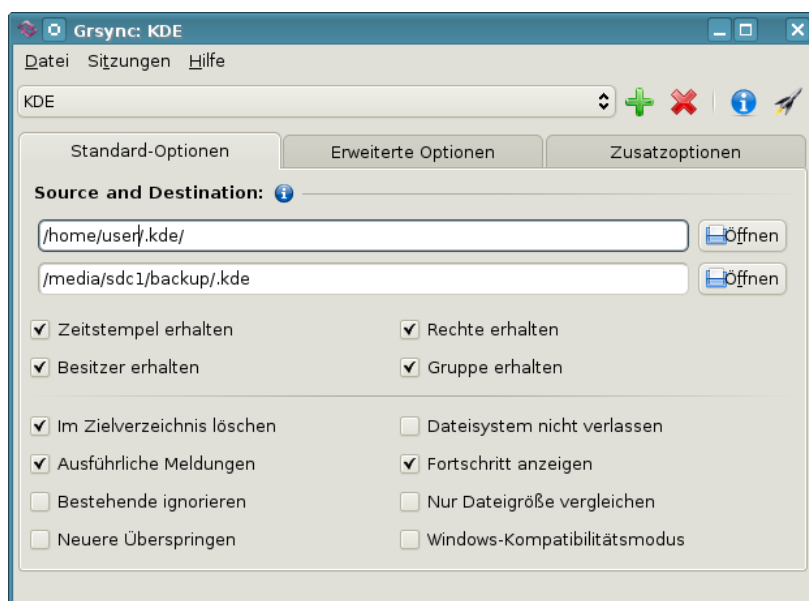


Abbildung 15.8: Hauptfenster von Grsync

15.7.2 Online Backups

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 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 Backuptool für Linux, dass die Daten lokal ver- und entschlüsselt, bevor sie in einen beliebigen Cloud-Speicher hochgeladen werden. Für die unverschlüsselten Cloud-Speicher kann man Verzeichnisse transparent mit *Boxcryptor*¹⁵ oder *Cryptomator*¹⁶ verschlüsseln. Beide gibt es für Windows, MacOS, Linux und diverse Smartphones.

E. Snowden hat in Interviews mehrfach vor Dropbox, Facebook und Google gewarnt und den amerikanischen Cloud-Provider Spideroak empfohlen, weil dieser Cloud-Provider die Daten irgendwie verschlüsselt. E. Snowden weiß aber nicht genau, wie Spideroak die Daten verschlüsselt. Hmmm - ein US-amerikanischer Provider, der die Daten irgendwie verschlüsselt. Ist das als Empfehlung ausreichend? Nein - für uns reicht es nicht.

Duplicity für Linux

Duplicity ist ein Backuptool 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.

Debian und Ubuntu stellen in der Regel alles Nötige für die Installation in den Repositories bereit. *aptitude* spült es auf die Platte:

```
> sudo aptitude install duplicity
```

Duplicity ist ein Kommandozeilen Tool. Ein verschlüsseltes Backup schiebt man mit folgendem Kommando auf den Server:

```
> duplicity Verzeichnis Backupadresse
```

¹⁴<https://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t>

¹⁵<https://www.boxcryptor.com>

¹⁶<https://cryptomator.org>

Vom lokalen Verzeichnis wird ein Backup erstellt, mit OpenPGP symmetrisch verschlüsselt und unter der Backup Adresse abgelegt. Ein vorhandenes Backup wird aktualisiert. Das Passwort für die Verschlüsselung wird entweder beim Start des Programms abgefragt oder es wird die Environment Variable \$PASSPHRASE verwendet. Um das Backup mit cron zu automatisieren, kann man ein kleines Shellscrip schreiben:

```
#!/bin/sh
PASSPHRASE="gutes_passwort"
duplicity Verzeichnis Backupadresse
```

Möchte man statt der symmetrischen Verschlüsselung einen OpenPGP-Key nutzen, verwendet man die 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 Backupadresse
```

Die **BackupAdresse** kodiert das Übertragungsprotokoll, den Server und das Verzeichnis auf dem Server. Duplicity kann mit vielen Protokollen umgehen. BackupAdressen haben folgenden Aufbau:

- Alle Anbieter von Online-Speicherplatz unterstützen webdav oder die SSL-verschlüsselte Übertragung mit webdavs:

```
webdavs://user[:password]@server.tld/dir
```

- 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
```

- Das sftp-Protokoll (ssh) ist vor allem für eigene Server interessant. Loginname und Passwort werden ebenfalls in der Adresse kodiert. Statt Passwort sollte man besser einen SSH-Key nutzen und den Key mit ssh-add vorher freischalten.

```
ssh://user[:password]@server.tld[:port]/dir
```

- 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 2 Slash, also `//dir`.

Ein **Restore** erfolgt nur in ein leeres Verzeichnis! Es ist ein neues Verzeichnis zu erstellen. Beim Aufruf zur Wiederherstellung der Daten sind Backupadresse und lokales Verzeichnis zu tauschen. Weitere Parameter sind nicht nötig.

```
> mkdir /home/user/restore
> duplicity Backupadresse /home/user/restore
```

Weitere Informationen findet man in der manual page von *duplicity*.

Kapitel 16

Daten löschen

Neben der sicheren Aufbewahrung von Daten steht man gelegentlich auch vor dem Problem, Dateien gründlich vom Datenträger zu putzen. 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.

16.1 Dateien in den Papierkorb werfen

Unter WIN wird diese Variante als *Datei(en) löschen* bezeichnet, was etw. 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 können und Dateien aus den Fragmenten wieder zusammensetzen.

16.2 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 shredern 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 shreddern.
- 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.

16.3 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 Repositories installieren.

Nach der Installation ist Bleachbit als Administrator bzw. root zu starten und nur die Option *Free disk space* zu aktivieren (Bild 16.1). Außerdem ist in den Einstellungen ein schreibbares Verzeichnis auf jedem Datenträger zu wählen, der gesäubert werden soll. Anschließend startet man die Säuberung mit einem Klick auf den Button *Clean*.

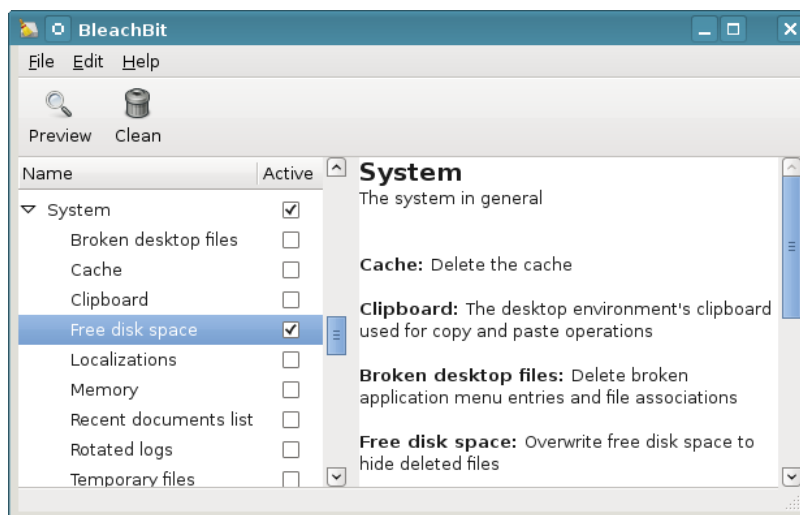


Abbildung 16.1: Bleachbit

Die Säuberung einer größeren Festplatte dauert einige Zeit. Dabei werden nur die als *frei* gekennzeichneten Bereiche überschrieben, das Dateisystem bleibt intakt.

¹<http://www.bleachbit.org>

16.4 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 den Speicherzellen eines Blocks einige Zeit nach dem Löschen der Datei auf den Ursprungszustand zurück gesetzt. Weitere Maßnahmen zum sicheren Löschen sind nicht nötig.

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 disableddeletenotify
```

Wenn ein Wert = 0 ausgegeben wird, ist Trim aktiviert. Wird ein Wert = 1 ausgegeben (weil man eine SSD nachträglich eingebaut hat oder den AHCI Mode im BIOS erst nachträglich aktiviert), aktivieren sie die Trim Funktion mit dem Kommando:

```
> fsutil behavior set disableddeletenotify 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 in dem 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 unused blocks once a week
Loaded: loaded
Active: active (waiting)
...
```

Aktivierung/Deaktivierung der wöchentliche Säuberung erfolgt mit:

```
> sudo systemctl enable/disable fstrim.timer
```

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 Mountoption *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 Mountoption *discard* hinzufügt:

```
sda2-crypt /dev/sda2 none luks,discard
```

Nach dem Ändern der Mountoptionen in */etc/fstab* oder */etc/crypttab* ist es eine gute Idee, die *initramfs* Images neu zu bauen:

```
> sudo update-initramfs -u -k all
```

²https://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf

³<https://github.com/CyberShadow/trimcheck>

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.

16.5 Gesamten Datenträger säubern (Festplatten)

Bevor ein Laptop oder Computer entsorgt oder weitergegeben wird, sollte man die Festplatte gründlich putzen. Am einfachsten erledigt man diesen Job mit Darik's Boot and Nuke (DBAN) ⁴ Live-CD. Nach dem Download ist das ISO-Image auf eine CD zu brennen und der Computer mit dieser CD zu booten. Es werden automatisch alle gefundenen Festplatten gelöscht - fertig.

Eine beliebige Linux Live-CD tut es auch (wenn man bereits eine Live-CD nutzt). Nach dem Booten des Live Systems öffnet man ein Terminal (Konsole) und überschreibt die gesamte Festplatte. Bei einem Aufruf wird der Datenträger 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, alles andere ist paranoid.)

16.6 Gesamten Datenträger säubern (SSDs)

Das komplette Löschen einer SSD-Platte oder eines USB-Sticks funktioniert am besten, wenn der Datenträger den ATA-Befehl SECURE-ERASE unterstützt. Diese Funktion muss allerdings durch den Datenträger bereitgestellt werden. Unter Linux kann man das Tool *hdparm* nutzen, um diese Funktion aufzurufen.

Als erstes ist zu prüfen, ob SECURE-ERASE unterstützt wird:

```
> sudo hdparm -I /dev/sdX
```

Das Ergebnis muss einen Abschnitt *Security* enthalten und muss auf *not frozen* stehen. Falls die Ausgabe *frozen* liefert, wird SECURE-ERASE im Bios des Rechners blockiert.

Security:

```
Master password revision code = 64060
supported
not enabled
not locked
not frozen
expired: security count
supported: enhanced erase
```

⁴<http://www.dban.org/>

Dann kann man ein Passwort setzen und den Datenträger vollständig löschen:

```
> sudo hdparm --user-master u --security-set-pass GEHEIM /dev/sdX  
> sudo hdparm --user-master u --security-erase GEHEIM /dev/sdX
```

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 wieder mit:

```
> dd if=/dev/zero of=/dev/sdc
```

16.7 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 professionellen Serviceanbieter, der das fachmännisch erledigt.

Die Berliner Firma Nitrokey.com bietet mit NiroShred⁵ diesen Service für Privatkunden und kleinere Unternehmen in Kooperation mit der Rhenus Data Office GmbH 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 geshreddert. Das Material wird am Ende recycled. 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.

⁵https://shop.nitrokey.com/de_DE/shop/product/nitroshred-datentragervernichtung-on-demand-106

Kapitel 17

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 Dokumentes 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 finden¹.

Der *StolenCameraFinder*² sucht anhand der KameraID 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>

17.1 Fotos und Bilddateien anonymisieren

- **Irfan View** ⁴ (Windows) kann in Fotos mit *Öffnen* und *Speichern* die Metatags entfernen. Im Batchmode kann man die Funktion *Konvertieren* nutzen, um mehrere Bilder mit einem Durchgang zu bearbeiten. Man konvertiert die Fotos von JPEG nach JPEG und gibt dabei in den Optionen an, dass keine EXIF, XMP und IPTC Daten erhalten bleiben sollen.

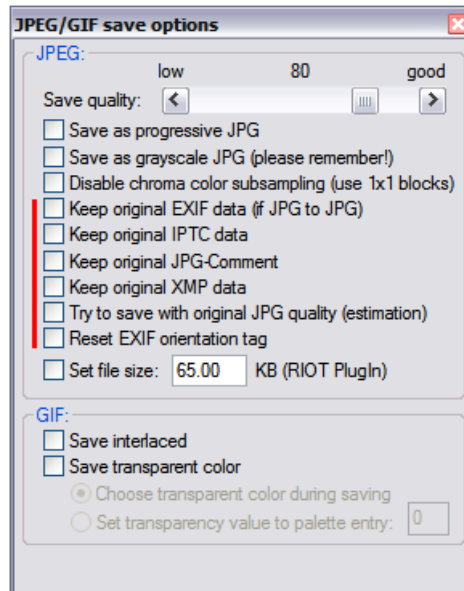


Abbildung 17.1: Informationen in Fotos löschen mit Irfan View

- **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:

```
> 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 ServiceMenü für Bilddateien in verschiedene Dateimanager integrieren. Für Konqueror und Dolphin (KDE) steht eine passende Datei auf der Webseite⁵ zum Download bereit.

17.2 PDF-Dokumente säubern

Man sollte ein PDF Dokument zuerst in eine neues PDF Dokument drucken, um die Metainformationen von eingebetteten Bildern und Medien zu entfernen. Dafür braucht man einen PDF-Drucker. Unter Linux stellt CUPS standardmäßig einen PDF-Drucker bereit. Unter Windows wird dieser Drucker z. B. vom *PDF Creator* von PDF24.org bereitgestellt. Nach der Installation des Paketes steht ein PDF-Drucker zur Verfügung.

⁴<http://www.heise.de/download/irfanview.html>

⁵https://www.privacy-handbuch.de/handbuch_43b.htm

Für **Windows** gibt es z. B. den *Hexonic PDF Metadaten Editor*⁶, um die restlichen Metadaten aus PDF Dokumenten zu entfernen. Nach dem Download und evtl. der Installation kann man das Tool starten und die zu säubernden PDF-Dokumente laden.

Unter **Linux** kann man die Metainformationen mit den Tools *exiftool* und *qpdf* entfernen. Beide Programme kann man mit dem bevorzugten Paketmanager installieren:

```
> sudo apt libimage-exiftool-perl qpdf
```

Nachdem das PDF mit einem PDF Viewer in eine neue PDF Datei *datei-print.pdf* gedruckt wurde, um die Metadaten von eingebetteten Bildern zu beseitigen, können alle Metadaten mit *exiftool* auf leere Werte gesetzt werden. Danach wird das PDF Dokument mit *qpdf* behandelt, 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:

```
> 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
```

⁶<http://www.hexonic.de/index.php/hexonic-pdf-metadata-editor>

```
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
```

Kapitel 18

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 Online¹, 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 der 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/>

18.1 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 Newsguppe 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.

18.2 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 Downloadseite bietet neben den Sourcen 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
```

18.3 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...5.0.

```
> stegdetect -s 2.0 bild.jpg
F5(***)
```

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:

²<http://www.outguess.org/download.php>

```
> 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 19

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.

19.1 Microsoft Windows

Mit Windows 8.0 hat Microsoft begonnen, dass 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-Account 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-Account 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 ...

Privaten Daten, die Microsoft in der Standardkonfiguration sammelt:

- Persönliche Interessen, die sich aus dem Surfverhalten ergeben sowie aus den per Apps gesammelten Daten 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 wird 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/Vidoe 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 Biometrics¹).
- Die eindeutige UUID, die Windows bei der Kommunikation mit Microsoftservern sendet (z. B. bei Softwareupdates), wird vom NSA und GCHQ als Selektor für Tailored 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 generierten 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 verhindern², 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...

19.1.1 Telemetrie in Windows 10

Windows 10 reagiert auf 1.000 - 1.200 Ereignisse, die eine Logmeldung triggern, welche dann an die Microsoft Telemetrie Server 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.⁴

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>

⁴<https://www.golem.de/news/datenschutz-aerger-microsoft-sammelt-bis-zu-25-000-ereignistypen-bei-office-1811-137815.html>

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 nicht durch die Konfiguration von Einstellungen vollständig deaktivierbar ist.

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 Trackingserver 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*.

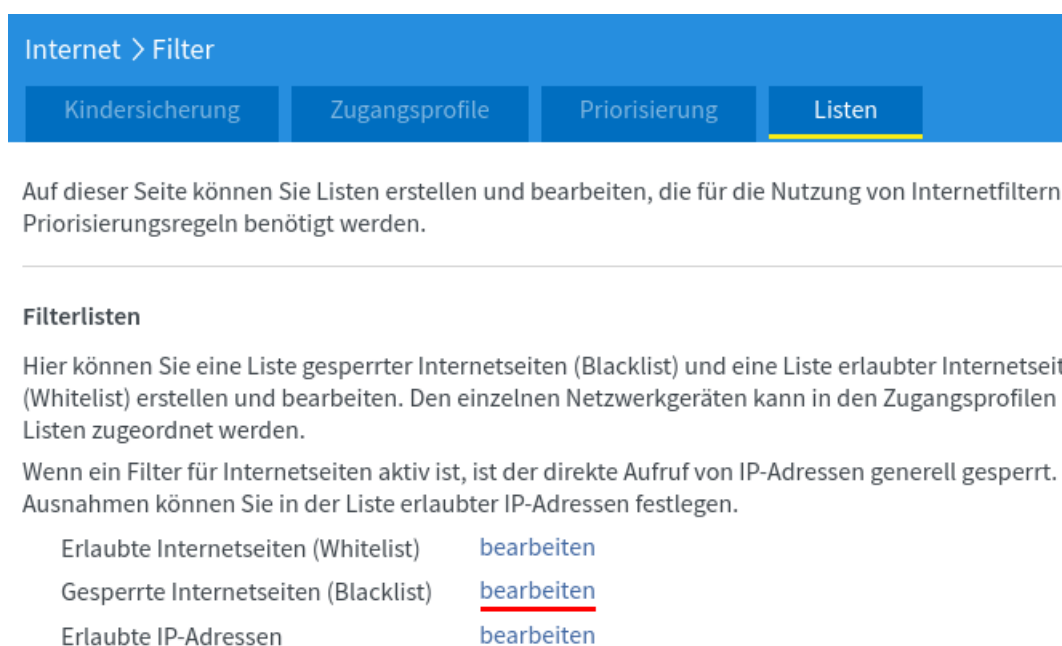


Abbildung 19.1: DNS Blacklist in der Fritzbox verwalten

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 Telemetrieserver 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*.

Die vom BSI untersuchte Version von Windows 10 sendete Daten an folgende Server:

```
geo.settings-win.data.microsoft.com.akadns.net
db5-eap.settings-win.data.microsoft.com.akadns.net
settings-win.data.microsoft.com
db5.settings-win.data.microsoft.com.akadns.net
asimov-win.settings.data.microsoft.com.akadns.net
db5.vortex.data.microsoft.com.akadns.net
v10-win.vortex.data.microsoft.com.akadns.net
geo.vortex.data.microsoft.com.akadns.net
v10.vortex-win.data.microsoft.com
v10.events.data.microsoft.com
v20.events.data.microsoft.com
us.vortex-win.data.microsoft.com
eu.vortex-win.data.microsoft.com
vortex-win-sandbox.data.microsoft.com
alpha.telemetry.microsoft.com
oca.telemetry.microsoft.com
ceuswatcab01.blob.core.windows.net
ceuswatcab02.blob.core.windows.net
eaus2watcab01.blob.core.windows.net
eaus2watcab02.blob.core.windows.net
weus2watcab01.blob.core.windows.net
weus2watcab02.blob.core.windows.net
```

Zukünftige Windows Versionen können weitere oder andere Server nutzen.

19.1.2 Virescanner sind Snakeoil

Für 90% der Windows Nutzer ist ein Virens scanner ein unverzichtbares Sicherheitstool aber nur 7% der Security Experten halten zusätzliche Virens scanner neben dem standardmäßig installierten Windows Defender für sinnvoll. Warum sind Sicherheitsexperten so skeptisch und bezeichnen diese Produktgruppe als Schlangenöl?

1. Virens scanner 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.^{5 6 7 8}

Da ein Virens scanner tief im System verankert ist und vollen Zugriff auf alle Systemkomponenten hat, kann ein Angreifer durch Ausnutzen von Bugs im Virens scanner das System vollständig kompromittieren ohne das der Anwender etwas bemerkt.

Außerdem wird die Implementierung von Sicherheitsfeatures durch Softwareentwickler (z. B. die konsequente Umsetzung von ASLR) durch Virens scanner behindert, wie der Robert O'Callahan berichtete. Er rät zur De-Installation.⁹

Schlussfolgerung: Virens scanner machen den Rechner unsicher.¹⁰

2. Viele Virens scanner brechen die TLS Transportverschlüsselung der Webbrowser und E-Mail Clients, um die verschlüsselten Inhalte zu scannen. Es ist ein klassischer man-

⁵<https://www.heise.de/-3250784>

⁶<https://www.heise.de/-3159436>

⁷<https://www.heise.de/-3149913>

⁸<https://www.heise.de/-2824437>

⁹<https://www.heise.de/-3609009>

¹⁰<https://www.golem.de/news/security-antivirens scanner-machen-rechner-unsicher-1407-108199.html>

in-the-middle Angriff mit Zustimmung der Anwender. Damit wird die Sicherheit der TLS Verschlüsselung massiv geschwächt.^{11 12}

Moderne Webbrowser bieten umfangreiche Sicherheitsfeatures für TLS wie Strict Transport Security (HSTS), Certificate Pinning (HKPS) oder mit Add-ons auch DANE/TLSA Validation. Vire Scanner beherrschen diese Sicherheitsfeatures in der Regel nicht. (Ich kenne kein Produkt der Schlangenöl Branche mit diesen Sicherheitsfunktionen.) Einige Vire Scanner 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.¹³

3. Mit der Installation eines Vire Scanners gibt der Nutzer praktisch die Hoheit über die Installation von Software teilweise auf. Es ist die Aufgabe eines Vire Scanners, 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 0day Exploits, um die Systeme zu kompromittieren. Die relativ teuren Angriffe mit 0day Exploits werden nur für gezielte Angriff auf besondere Ziele eingesetzt, und nicht bei Viren. Computer Viren nutzen in Regel 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 Vire Scanner.
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 Vire Scanner nicht schützen. Das konnte man anhand der Veröffentlichungen zur NSA-Cyberwaffe *Regin* verfolgen.

- Als erstes hat Fox-IT den Trojaner *Regin* bei der Analyse des Einbruchs bei Belacom gefunden. 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 Nov. 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 veröffentlichte. V. Thakur von Symantec sagte im Nov. 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 Dez. 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 Nov. 2014 ankündigte, über *Regin* zu berichten, haben die Anti-Virus Firmen reagiert und die Öffentlichkeit informiert.

19.2 Apple MacOS

Wenn man die Apple Datenschutzrichtlinie liest, erkennt man, das MacOS sich nicht als Betriebssystem eignet, wenn man seine Privatsphäre nicht mit Apple teilen möchte:

¹¹<https://www.heise.de/-2482344>

¹²<https://www.heise.de/-3095024>

¹³<https://www.heise.de/-3620159>

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.

19.3 Linux Distributionen

Es gibt eine Vielzahl von Linux Distributionen, so dass man als potentieller Anwender erst einmal vor der Qual der Wahl steht: Debian und Derivate, OpenSuSE, OpenMandriva, Fedora, Gentoo für Bastler, Minidistributionen wie Puppy oder Fortress Linux als gehärtete Variante, KaliLinux... 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 Stabilität der viele 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 einem eleganteren Desktop, der vor allem Umsteigern von Windows die Arbeit erleichtert. Für den Unterbau werden die originalen Debian Pakete verwendet, also eine große aber nicht immer brandaktuelle Softwareauswahl.
- **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. Andere Tools sind aber eng mit dem Unity Desktop verflochten, wie das Location Tracking Tool *geoclue*, das den Unity Anwendungen Informationen über die aktuelle Position zur Verfügung stellt, oder das Logging Tool *Zeitgeist*, welches alle Aktivitäten protokolliert. Um diese Tools zu deinstallieren, müsste man zuerst einen anderen Desktop installieren. Dann kann man aber auch gleich Xubuntu oder Kubuntu wählen.

- **Ubuntu LTS** (Long Term Support): neben der halbjährlich aktualisierten Distribution gibt es Ubuntu in einer LTS Version, die man nur alle zwei Jahre komplett aktualisieren muss. Der Long Term Support gilt nur für die 9.000 Pakete des Main-Repository. Der Rest der 45.000 Pakete wird oft nur mangelhaft mit Sicherheitsupdates versorgt.
- **Xubuntu** oder **Kubuntu** sind für Linux Einsteiger gut geeignet. Die gute Hardware Unterstützung für neue Technik kombiniert mit einfacher Standardinstallation umfangreicher Software inklusive Multimedia, klarem Bedienkonzept des Desktop ohne irgendwelche Cloud Anbindungen oder Übertragung von Daten an Dritte sowie Full-Disc-Encryption bei der Installation erleichtern den Einstieg.

Den privacy-invasiven Crash Reporter von Ubuntu und das Report Submission Tool *whoopsie*, das täglich den Server *daisy.ubuntu.com* kontaktiert, kann man nach der Installation problemlos mit der bevorzugten Paketverwaltung entfernen. Im Terminal erledigt man das mit:

```
> sudo apt purge whoopsie apport
```

Die Deinstallation überflüssiger Software ist ein Sicherheitsfeature. Ein Bug im Crash Reporter *apport* konnte beispielsweise jahrelang dazu genutzt werden, um den Rechner aus der Ferne zu kompromittieren.¹⁴

Wenn man gerade mit dem Paketmanager spielt, könnte man auch folgendes Paket installieren, um Angriffe über TMP-Dateien zu erschweren:

```
> sudo apt install libpam-tmpdir
```

- **Mint Linux** möchte das bessere Ubuntu sein und bietet vor allem einen anderen Desktop, der sehr hübsch ist und Windows Umsteigern den Einstieg erleichtert. Allerdings ist Mint keine komplett selbständige Distribution sondern schmarotzt bei Ubuntu, was öfters für Verstimmung bei Canonical sorgte und die Probleme mit der mangelhaften Versorgung für Sicherheitsupdates einschließt. Mit LMDE gibt es auch eine Variante, die auf Debian basiert.

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 Software Auswahl als Debian (vor allem bei Multimedia).

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 ext. Repositories einbindet.

- **Fedora** ist die Community Version von RedHat, für die man auch ohne Lizenz Updates bekommt. In der Verbreitung liegt Fedora hinter Ubuntu auf Platz 2.

Um eine mit Ubuntu vergleichbare gute Unterstützung für Multimedia zu erhalten, kann man das RPMfusion Repository einbinden¹⁵ und die gewünschten Multimedia Pakete installieren (was allerdings auch 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, so dass man ein System regelmäßig komplett aktualisieren muss.

Distributionen auf Basis von Arch Linux:

- **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 vollständigen System Upgrades des Gesamtsystems sind nicht nötig.

Um Probleme bei Updates zu vermeiden, sollte man Rolling Release Distributionen 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.

Immutable (unveränderbare) Distributionen:

- **Silverblue** ist ein immutable Desktop System auf Basis von Fedora. Mit Toolbox können Container für verschiedene Arbeits- und Testumgebungen erstellt werden.

¹⁴<https://www.golem.de/news/linux-sicherheit-ubuntu-bug-ermoeoglicht-das-ausfuehren-von-schadcode-1612-125112.html>

¹⁵<https://rpmfusion.org/Configuration>

- Ein Container ist keine abgeschlossene Umgebung wie eine VM. Ein neuer Container stellt anfangs die gleiche Umgebung wie der Host zur Verfügung. Man kann die Daten im Homeverzeichnis aus dem Hostsystem lesen aber Änderungen und neue Dateien sind nur innerhalb des Containers verfügbar.
- In einem Container kann man Software ganz normal installieren, compilieren, testen usw. Die zusätzliche Software steht nur im Container zur Verfügung.

Immutable (unveränderbare) 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. Das Hostsystem ist nicht veränderbar und damit stabil. Alle Modifikationen, Installation von Software erfolgen in sogenannten Containern, die man einfach erstellen, nutzen und wegwerfen kann.

Eine Linux Distribution für besondere Sicherheitsanforderungen:

- **Qubes OS** ist eine Besonderheit unter den Linux Distributionen. 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
- getrennter Netzwerkzugriff für jede der VMs
- Schutz gegen BadUSB Devices durch eine Proxy-VM für USB-Geräte, mit der kontrolliert, welche USB Geräte in den Arbeits-VMs zur Verfügung stehen
- umfangreiche graphische Integration der virtuellen Maschinen inklusive Farben zur visuellen Abgrenzung der VMs untereinander
- 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 Repositories bereits vorbereitet, sie müssen nur aktiviert werden:

```
> su
# dnf config-manager --set-enabled rpmfusion-free
# 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 umfangreich anpassbar und unter 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.

19.3.1 Linux-taugliche Hardware

- Die deutsche Firma TUXEDO Computers bietet 100% Ubuntu/OpenSUSE compatible Laptops und PCs in vielen Varianten, darunter auch Notebooks im edlen Design. (Andere Linux Distributionen funktionieren auch, aber der Support kennt nur Ubuntu und OpenSUSE.)¹⁶
- Die Business Laptops von Lenovo (X2x0, T4x0, T5x0) sind robust und kompatibel mit aktuellen Linux Distributionen. Man kann sie auch gebraucht noch gut verwenden.

¹⁶<https://www.tuxedocomputers.com>

Hardware für besondere Sicherheitsanforderungen

- **NitroPad X230**¹⁷ (12,5"Display, 1366x768) und **NitroPad T430**¹⁸ (14"Display, 1600x900) basieren auf etwas älteren, robusten Thinkpad Business Laptops und ermöglicht ein neues Sicherheitserlebnis. Die Hardwareausstattung ist konfigurierbar.
 - 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.
 - Der 12,5 Bildschirm des X230 ist wirklich klein. Auf dem Schreibtisch sind ein zusätzlicher Monitor, Maus und Tastatur empfehlenswert für ergonomisches Arbeiten.
- 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).¹⁹
 - 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 2-Faktor-Auth. genutzt werden kann.
 - Hardware Kill Switches für Mikrofon, Kamera, Wi-Fi und Bluetooth schützen gegen Angriffe, die das Gerät in eine Spionage-Wanze verwandeln.²⁰

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.²¹

19.3.2 Boot-Medium für die Linux Installation erstellen

Wenn man das ISO-Image mit dem Installer einer Linux Distribution herunter geladen hat oder das Image eines Live-Systems, muss man daraus irgendwie ein Bootmedium für den Computer erstellen. Man hat die Wahl zwischen einer DVD-RW oder einem USB-Stick.

Wenn man noch ein DVD-RW Laufwerk hat und ein beschreibbare DVD, 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 simple. Das ISO-Image und den gewünschten USB-Stick wählen und auf den Button *Schreiben* klicken (Abb. 19.2).
- 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!!!

¹⁷https://shop.nitrokey.com/de_DE/shop/product/nitropad-x230-67

¹⁸https://shop.nitrokey.com/de_DE/shop/product/nitropad-t430-119

¹⁹<https://puri.sm/posts/the-librem-key-makes-tamper-detection-easy/>

²⁰<https://puri.sm/learn/hardware-kill-switches/>

²¹<https://puri.sm/posts/qubes4-fully-working-on-librem-laptops>

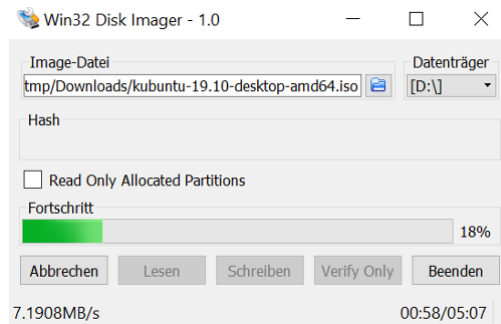


Abbildung 19.2: Win32 Disk Imager

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-Stick zu kopieren. Nach dem Anschließen des USB-Stick 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
```

19.4 NetBSD und OpenBSD

Diese beiden BSDs sind konsequent und ohne Kompromisse hinsichtlich Benutzbarkeit auf Sicherheit 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 Allokieren 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 der höchsten Sicherheitsstufe von NetBSD und OpenBSD nicht installieren. In NetBSD muss man in der Datei `/etc/mk.conf` folgende Option setzen:

```
ALLOW_VULNERABLE_PACKAGES=yes
```

19.5 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 im Vortrag *BadUSB - On Accessories that Turn Evil*²² gezeigt, wie der Internettraffic 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 Nov. 2016 hat Samy Kamkar mit *PoisonTap*²³ 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...) des Targets übernehmen, die mit diesem Browser genutzt wurden. Der Angreifer muss nur *PoisonTab* am USB Port anschließen und warten.

Ein besonderes Risiko sind USB-Sticks oder USB-Festplatten, die man bedenkenlos an unterschiedlichen Computern in verschiedenen Netzen nutzt.

- Ein Beispiel aus der Praxis: Vor einigen Jahren war ich für ein paar Monate als IT-Administrator für eine Firma tätig. Dort habe ich einmal eine Woche lang jeden Tag den gleichen Virus gejagt. Am Abend war das Firmennetzwerk sauber, am nächsten Morgen war der Virus wieder da. Eine Sekretärin hatte am Abend Dokumente mit nach Hause genommen und am Morgen mit dem verseuchten USB-Stick den Virus von ihrem privaten Computer zuhause wieder ins Firmennetzwerk eingeschleppt.
- Einige spektakuläre Beispiele aus den Medien zeigen, dass es im Cyberwar üblich ist, Malware auf USB-Stick in schwer zugängliche Netzen zu transportieren. Dabei kann der USB-Stick extra präpariert werden oder man greift die schlecht gesicherten Rechner mehrere Targets zuhause an und hofft, dass der Trojaner von einem Wirt mit einem USB-Stick 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 nichtklassifizierte Netzwerke) mit dem russischen Trojaner *agent.bz*. Es dauerte 14 Monate und kostete mehrere Mio. Dollar, die Netzwerke zu säubern.
 - *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.

²²<https://www.youtube.com/watch?v=nuruzFqMgIw>

²³https://www.schneier.com/blog/archives/2016/11/hacking_passwor.html

- 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 Aples I/O-Technik Thunderbolt gab es von Anfang an Sicherheitsbedenken²⁴. Dokumente von HBGary belegen, dass US-Behörden schon 2011 ein Framework nutzen, 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.²⁵
4. *USBGuard* für Linux²⁶ 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-Blocker²⁷ von securityXploded.com)
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 der Thunderbolt-Controller, um Bedrohungen für BitLocker zu reduzieren.*²⁸
 - 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 Kernelmodule 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
```

²⁴<https://heise.de/-1198049>

²⁵<https://heise.de/-3222811>

²⁶<https://dkopecek.github.io/usbguard/>

²⁷<http://securityxploded.com/windows-usb-blocker.php>

²⁸<https://support.microsoft.com/kb/2516445/de>

USBGuard für Linux

USBGuard 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:

- 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 Booten 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 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 Kommando 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:

```
IPCAIlowedUsers = 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.

19.6 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.

19.6.1 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 beispw. 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.

Den Status der Firewall kann man mit folgendem Kommando prüfen:

```
> sudo ufw status verbose
```

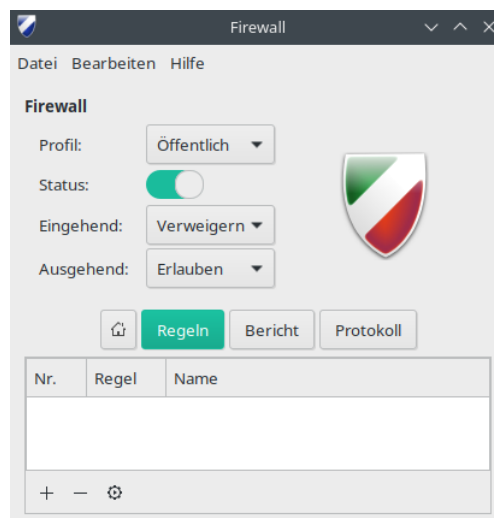


Abbildung 19.3: GFW Hauptfenster

Es gibt ein grafisches Frontend GFW, dass man mit dem bevorzugten Paketmanager installiert, wenn es noch nicht vorhanden ist, unter Debian/Ubuntu mit:

```
> sudo apt install gufw
```

GFW 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.

19.6.2 RHEL Firewall

Bei RHEL wird standardmäßig der *firewalld* und ein GUI zur Verwaltung der Firewall Regeln installiert. *firewalld* unterscheidet zwischen einer temporären Runtime Konfiguration und einer permanenten Konfiguration. Wenn man Regeln dauerhaft speichern möchte,

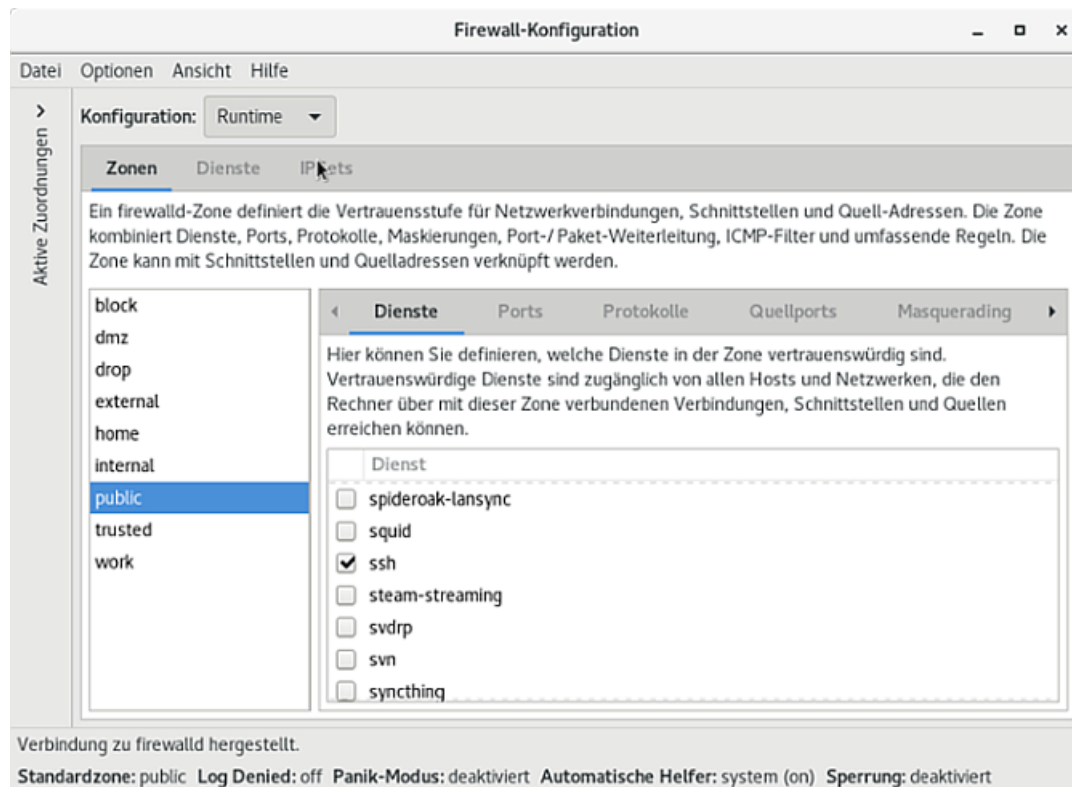


Abbildung 19.4: RedHat Firewall Konfigurator

dann darf man nicht vergessen, auf die permanente Konfiguration umzuschalten.

firewalld unterscheidet zwischen Zonen, für die unterschiedliche Firewallregeln gelten können. Für jede Netzwerkschnittstelle kann festgelegt werden, welcher Zone sie zugeordnet ist. Es ist ein Tool, das sich gut für komplexe Server Architekturen eignet.

Die *firewalld* Konfiguration in Fedora erlaubt standardmäßig eingehende Verbindungen von außen auf den nicht-privilegierten Ports > 1024.

19.6.3 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. 19.5).

19.7 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*

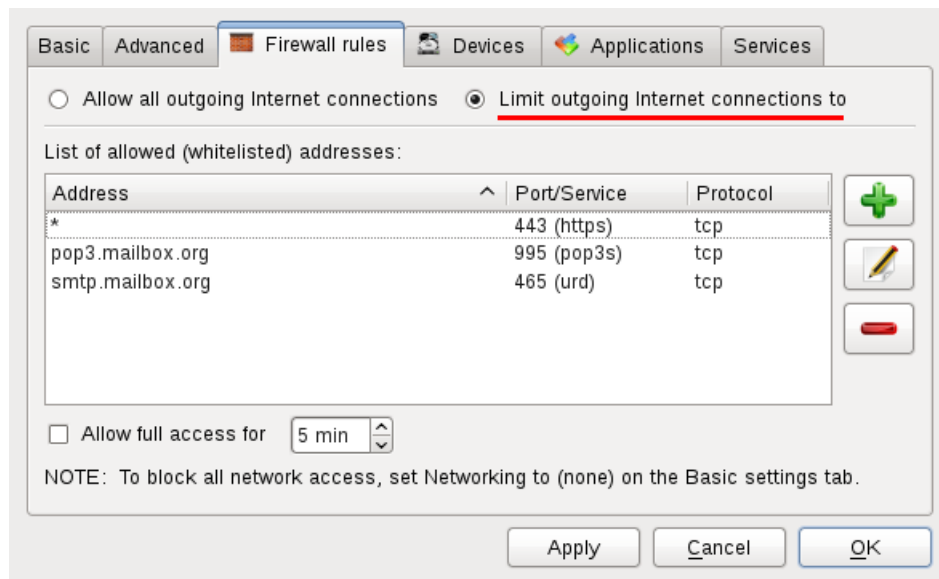


Abbildung 19.5: QubesOS: Firewall Konfiguration einer VM

options enable device tracking²⁹ 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, Internetcafé, 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.
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.³⁰
- Mit den *Probes* auch eine Liste der bevorzugten WLANs gesendet, mit denen sich der Laptop automatisch verbinden würde (Preferred Network List, PNL). Diese Preferred Network List liefert Informationen über Orte, an denen sich der Besitzer des Laptops bevorzugt aufhält.

²⁹<https://tools.ietf.org/html/draft-huitema-perpass-dhcp-identifiers-00>

³⁰<https://tools.ietf.org/html/draft-huitema-perpass-dhcp-identifiers-00>

- Praktische Angriffe mit den Informationen aus den *Probes* hat die Security Firma Sensepost mit der Drohne *Snoopy* vorgestellt. Diese Drohne simuliert die SSID eines bevorzugten WLANs. Der Laptop meldet sich automatisch bei der Drohne an, der Internet Traffic läuft über die Drohne und kann dort analysiert werden. Es wurde z. B. demonstriert, wie Snoopy die Login Credentials für PayPal, Yahoo! usw. abreifen konnte.³¹

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.

19.7.1 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 19.6.

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.
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.

19.7.2 MAC-Adresse faken (Linux)

Der NetworkManager enthält alle nötigen Features, um die MAC-Adressen zu faken. Zusätzliche Tools sind nicht nötig. Beim Netzwerkskan wird standardmäßig eine zufällig generierte MAC-Adressen verwendet. Beim Verbindungsaufbau verwendet der Networkmanager standardmäßig die echte MAC-Adresse.

Um beim Verbindungsaufbau eine Fake MAC zu verwenden, kann man die folgende Konfigurationsdatei unter */etc/NetworkManager/conf.d/50-macchange.conf* speichern:

```
[connection-mac-randomization]
ethernet.cloned-mac-address=random
wifi.cloned-mac-address=stable
```

Für die Generierung der Fake MAC-Adressen gibt es zwei Möglichkeiten:

- **random:** es wird bei jedem Verbindungsaufbau eine neue Fake Adresse generiert.

³¹<https://www.golem.de/news/drohne-snoopy-schnueffelt-im-vorbeiflug-1403-105329.html>

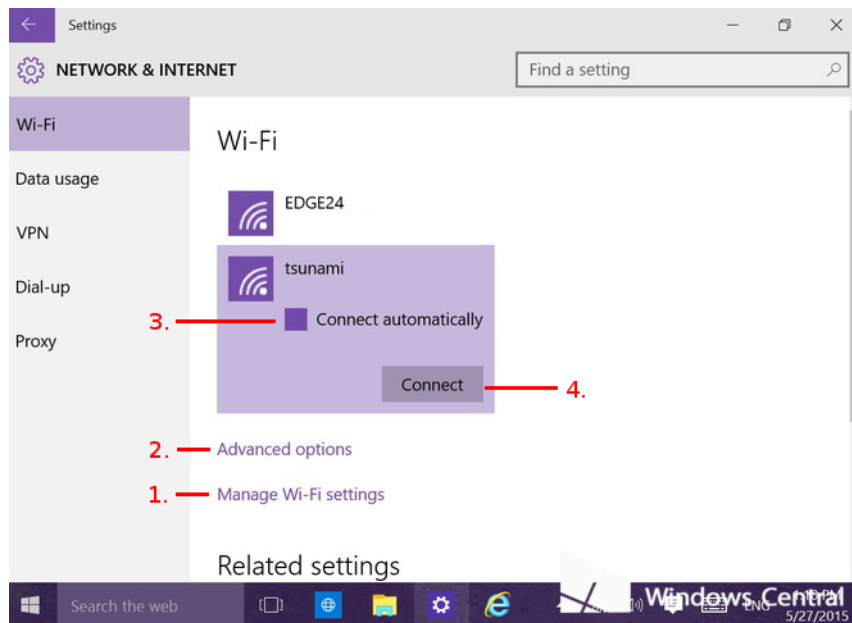


Abbildung 19.6: MAC-Adresse faken für Windows 10

- **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: 19.7).

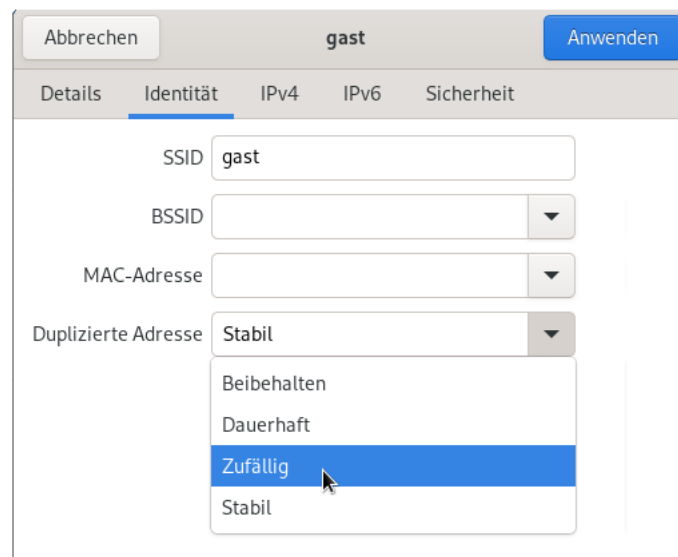


Abbildung 19.7: Fake Mode für MAC Adresse im NetworkManager anpassen

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 Kom-

mando ändert die Fake Methode für das WLAN mit dem Namen WIFlonICE auf *random*:

```
> nmcli connection show
...
> nmcli connection modify "WIFlonICE" wifi.cloned-mac-address random
```

19.7.3 Automatische Anmeldung für bevorzugte WLANs deaktivieren

Wenn man die *automatische Anmeldung* für WLANs aktiviert hat, sendet der Laptop unterwegs (am Flughafen, im Hotel, in der U-Bahn...) ständig sogenannte *Probes*, um die Umgebung nach den bevorzugten WLANs zu scannen.

Diese *Probes* haben einen eindeutigen Fingerprint und können in gleicher Weise wie MAC-Adressen für das Tracking der Geräte verwendet werden, wie die Analyse *Why MAC Address Randomization is not Enough* demonstrierte. In den Einstellungen der WLAN-Verbindungen muss man für alle konfigurierten WLANs die Option *Automatisch Verbinden* abschalten, um *Probes* unterwegs mit dem Laptop zu vermeiden (Abb: 19.8).

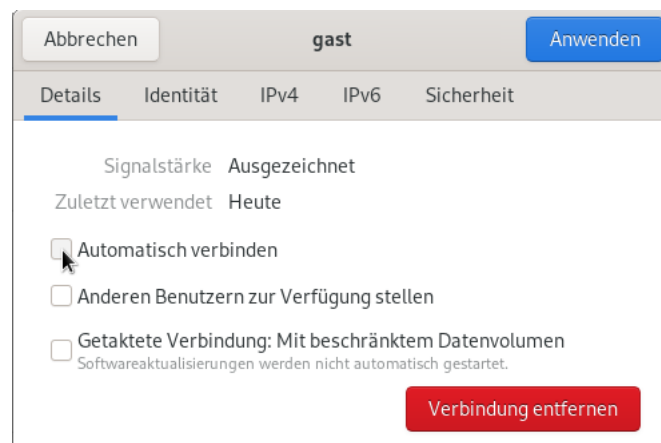


Abbildung 19.8: Automatische Anmeldung für WLANs deaktivieren

19.7.4 Hostname und DNS-Domain konfigurieren

Hostname und Domain kann man bei der Installation des Betriebssystems festlegen oder nachträglich ändern. Es gibt keine wirklich anonyme Empfehlung für diese Werte. Wir empfehlen die folgende nichts aussagende Werte, die auch von Live-DVDs wie TAILS u.a. verwendet werden:

```
Hostname: host
Domain:   localdomain
```

Wenn man Linux verwendet, kann man den Hostnamen nachträglich mit folgenden Kommandos ändern:

```
> sudo hostname host
```

Um die DNS-Domain unter Linux nachträglich zu ändern, sind folgende Zeilen in der Datei */etc/hosts* anzupassen:

```
127.0.0.1 host.localdomain host
::1 host.localdomain host
```

Man kann den NetworkManager auch dazu überreden, beim Aufbau einer Netzwerkverbindung keinen den Hostnamen an den DHCP-Server zu senden. Dafür sind folgende Zeilen in der Datei */etc/NetworkManager/NetworkManager.conf* einzutragen:

```
[ipv4]
dhcp-send-hostname=false
```


Kapitel 20

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...- aber immer ist man online und auf der Jagd nach Likes.)

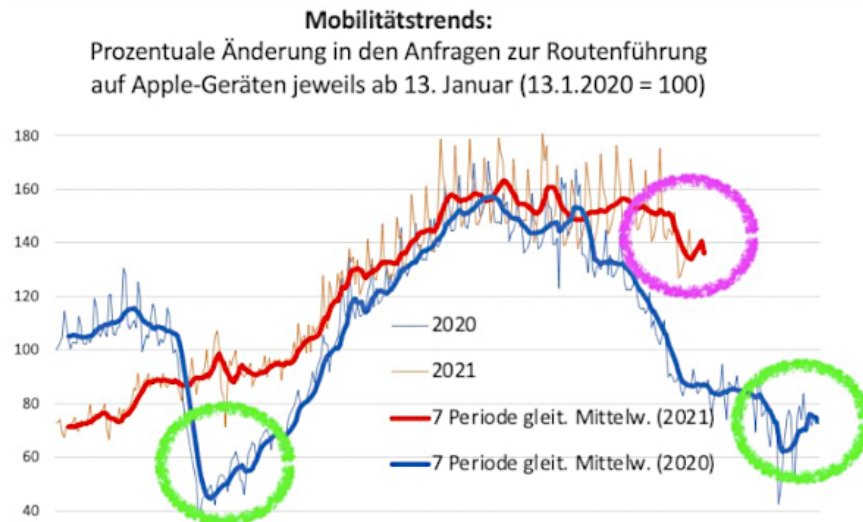
Mit der zunehmenden Verbreitung von Smartphones entstehen neue Gefahren für die Privatsphäre, die deutlich über die Gefahren durch datensammelnde Webseiten beim Surfen oder E-Mail scannen bei Mail Providern wie Google hinaus gehen. Da wir die handliche Wanze immer mit uns umhertragen und unterwegs nutzen, 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.

10 Jahre später sind die Vision von Greg Skibiski Wirklichkeit. Bewegungsdaten von Smartphones werden in den Corona-Jahren 2020/21 routiniert verwendet, um die Bevölkerung zu durchleuchten und mehr oder weniger interessante Informationen zu gewinnen:

- Das Statistische Bundesamt analysiert 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 sind 2020 um 50% niedriger als im Vorjahr.
- Zu Weihnachten und Silvester 2020 führt das Statistische Bundesamt außerplanmäßige Sonderauswertungen der anonymisierten Mobilfunkdaten durch, um die Einhaltung der Coronabeschränkung 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, ist 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 haben die Menschen die Nase voll von den Reiseeinschränkungen. Die Auswertung der Navigationsanfragen von Apple iPhones zeigt, dass sich die deutsche Bevölkerung in ihrer Reiselust im November 2021 nur wenig einschränkt.



- Der CSU Politiker U. Brandl schlägt 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 zu Verfügung zu stellen, insbesondere um die Einhaltung der 15km-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.

(Btw: Die Ausgangsbeschränkungen in Bayern wurden nachträglich für verfassungswidrig erklärt.)

Man könnte den braven Bürger simulieren und das Smartphone zuhause lassen, wenn es nicht so schwer fallen würde, auf das kleine Gadget kurze Zeit zu verzichten.

20.1 Kommerzielle Datensammlungen

Bei den möglichen Gewinnen durch die Auswertung und Verarbeitung von Daten, die mit Smartphones und Apps gesammelt werden, wundert es nicht, dass viele Teilnehmer aggressiv bei den Datensammlungen beteiligt sind.

20.1.1 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

¹<https://www.br.de/nachrichten/bayern/15-kilometer-regel-brandl-fordert-auswertung-von-handy-daten>

²https://www.scss.tcd.ie/doug.leith/apple_google.pdf

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 Smartphonehersteller.

Seit iOS Version 8 übertragen Apples Mobilgeräte automatisch die Liste der Telefonanrufe an Apple-Server (Telefonnummer, Datum/Uhrzeit, Dauer). Diese Datenspeicherung kann man nur verhindern, wenn man die iCloud komplett abschaltet.

Mit iOS Version 10 hatte Apple diese Datenspeicherung ausgeweitet und überträgt die Metadaten der Kommunikation von allen Apps in die Apple Cloud, die mit CallKit-Unterstützung eingehende Anrufe auf dem Lockscreen anzeigen. Das betrifft neben Telefonie und SMS auch iMessage, WhatsApp, Skype und andere verschlüsselten VoIP Telefonate sowie Kommunikation via Messenger. Apple nennt es Call History.

Mit iOS Version 13 wird die Call History verschlüsselt in der Cloud gespeichert.

Die Kommunikationsdaten werden für 4 Monate im iCloud-Konto des Benutzers gespeichert und können dort ggf. von Behörden abgegriffen und für die Kommunikationsanalyse genutzt werden. Die Firma Elcomsoft bietet Geheimdiensten Tools, um diese Daten zu erschließen. Nur wenn die 2-Faktor-Authentifizierung für den Zugriff auf die iCloud aktiviert wurde, stellt die mit iOS 13 eingeführte Verschlüsselung die Geheimdienste vor ernsthafte Probleme.

Außerdem sendet ein iPhone 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

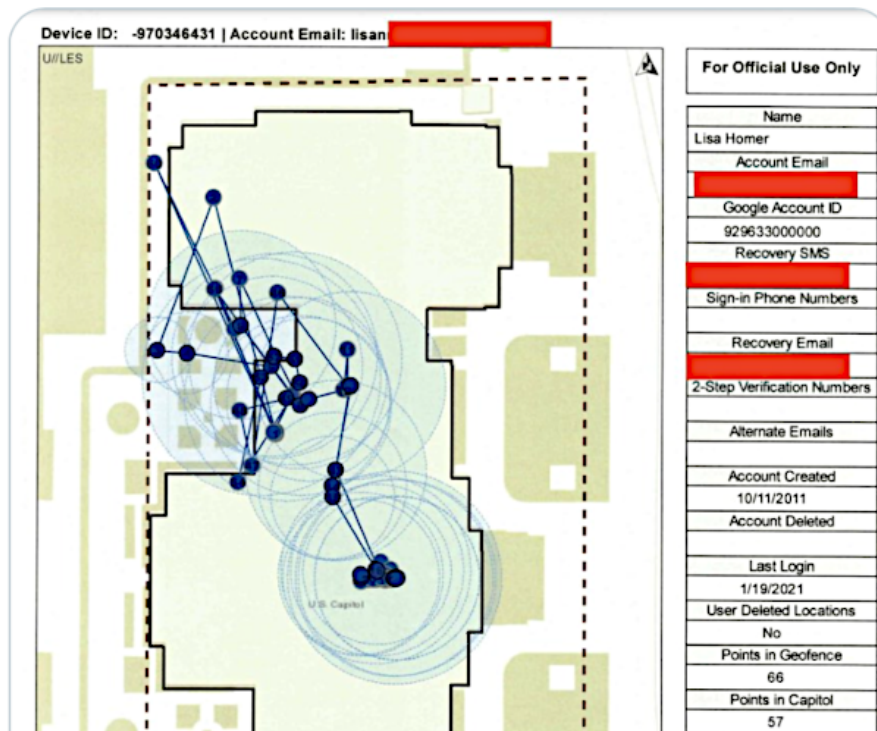
Google Android: die tief im System verankerte Google Play Service App sendet alle 20min folgende Daten an Google:

- Telefonnummer und SIM-Kartennummer
- Gerätenummer (IMEI) und Seriennummer des Gerätes
- WLAN-MAC-Adresse und IP-Adresse
- Android-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 Jan. 2021 beteiligt waren (Abb: 20.1). Bei der Erstürmung des Capitol im Jan. 2021 verwendeten einige militante Gruppen Wegwerf-Smartphones für die Kommunikation. Das FBI hat 300+ von diesen Wegwerf-Phones mit anonym gekauften SIM Karten identifiziert und deren Weg durch das Captitol verfolgt. 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 gepflegten Liste von Ausnahmen zugelassen. Apps sollen die Werbe-ID für das Tracking nutzen, die der Nutzer neu auswürfeln oder löschen kann. Den Zugriff auf eindeutigen 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 Datenschutz Policy steht:



Abbildungung 20.1: FBI Dokument zeigt Genauigkeit des Google Standorttrackings

Wenn Sie unsere Dienste nutzen, um Anrufe zu tätigen und zu erhalten oder um Nachrichten zu senden und zu empfangen, erheben wir möglicherweise Telefonie-Informationen wie Ihre Telefonnummer, die Anrufernummer, die Nummer des Angerufenen, Weiterleitungsnummern, das Datum und die Uhrzeit von Anrufen und Nachrichten, die Dauer, Routing-Informationen und die Art der Anrufe.

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.

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 App³ 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.⁴

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.

³<https://www.theverge.com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android>

⁴<https://android-developers.googleblog.com/2019/01/reminder-smsscall-log-policy-changes.html>

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.

20.1.2 Privacy-freundliche Alternativen für Android

Für Android Smartphones gibte 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...

Ein verschlüsseltes Backup der Daten kann man auf einen USB-Datenträger ablegen oder in einer (eigenen) Nextcloud. Es wird keine Google Cloud verwendet.

Nach Einschätzung von Viktor Chebyshev (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.

Man kann GrapheneOS selbst auf ein unterstütztes Phone flashen. Alternativ bietet die Nitrokey GmbH mit NitroPhone ein Google-freies Pixel 4a 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.⁵

CalyxOS kann man ebenfalls nur auf den Google Pixel Smartphones installieren (und dem Xiaomi Mi A2). Es fokussiert als Google-freie Alternative ebenfalls auf Sicherheit, ist aber nicht so restriktiv wie GrapheneOS. Man kann beispw. mit microG auch die Google Push Services nutzen und somit Apps installieren, die diese Dienste unbedingt benötigen.

Auf der Webseite findet man Installationsanleitungen, um ein Smartphone zu flashen.⁶

iodéOS ist ein Fork von LineageOS Projekt mit einigen Verbesserungen für die Privatsphäre. F-Droid ist als App Store vorinstalliert, ein standardmäßig aktiver Werbeblocker funktioniert auch mit VPNs, die microG Bibliothek für Google Push Support kann man deinstallieren usw.

Man iodéOS selbst auf ein gerootetes Samsung, Xiaomi oder Sony Smartphone flashen.

Im Shop gibt es iodéOS vorinstalliert auf einem neuen Terracube und Fairphone-3 oder auf gebrauchten, frisch aufbereiteten Smartphones von Samsung, Xiaomi oder Sony.⁷

/e/ Android ist als eine Alternative für ältere Smartphones geeignet.

Um ältere Hardware zu unterstützen, die von Herstellern nicht mehr supported wird, kommt ein etwas angestaubter Linux Kernel in /e/ zum Einsatz. Auch die Apps im /e/ Store sind nicht immer taufrisch, was ein Nachteil hinsichtlich Sicherheit ist.

/e/ ist Google-frei und verwendet standardmäßig keine Cloud Dienste und übertragen keine Daten an die /e/ Foundation. Um Cloud Funktionen zu nutzen, kann

⁵https://shop.nitrokey.com/de_DE/shop/product/nitrophone-1-199

⁶<https://calyxos.org/install>

⁷<https://iode.tech/en/#new-phones>

man einen Account bei der /e/ Cloud erstellen oder eine beliebige andere Nextcloud Instanz nutzen.

Erfahrene Nutzer können das Costum ROM von /e/ auch auf einem vorhandenen Google Smartphone installieren und damit Google rauswerfen. Es werden aktuell 93 Android Smartphones unterstützt (Stand Okt. 2020).

Man kann Phones mit vorinstalliertem /e/ im Shop der /e/ Foundation kaufen.⁸

20.1.3 Datensammlungen mit Smartphone Apps

Standortdaten: Tausende Apps sammeln überflüssigerweise Standort- und Bewegungsdaten der Nutzer. Der ehem. Bundesdatenschutzbeauftragte erwähnt beispielsweise 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.^{9 10}

Außerdem zahlt US Customs and Border Protection (CBP) jährlich fast eine halbe Mio. Dollar an die Firma Vettel 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 und Spielen und bereitet sie auf.¹¹

Der norwegische Journalist M. Gundersen hat in einer Recherche die Datensammlung der Firma Venntel genauer analysiert. Im Februar 2020 hat er auf einem neuen Smartphone 160 Apps installiert und dieses Smartphone ständig bei sich getragen. Keine der 160 Apps nannte die Firma Venntel in ihren Datenschutzklauseln.¹²

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 Smartphone. Als Antwort erhielt er 75.406 Datenpunkte mit Location und Zeitstempel, die in den 6 Monaten gesammelt wurden. Anhand der Daten konnte sein Wohnort, seine Arbeitstelle und auch seine Wanderungen in der Freizeit nachvollzogen werden sowie jede Bank, auf der er sich während der Wanderung ausgeruht hatte. Abb. 20.2 zeigt den Ausschnitt von 36min aus einer Wanderung mit einer Rast.

Venntel informiert 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, dass 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 dafür bezahlt. Diese Apps senden damit laufend die Standortdaten von einigen hundert Mio. Nutzern an das US-amerikanische Unternehmen und von dort aus weiter an US Geheimdienste.¹³

⁸<https://esolutions.shop/>

⁹<https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x>

¹⁰<https://www.vice.com/en/article/jgk3g/secret-service-phone-location-data-babel-street>

¹¹<https://www.vice.com/en/article/k7qyv3/customs-border-protection-venntel-location-data-dhs>

¹²<https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants>

¹³<https://www.wsj.com/articles/u-s-government-contractor-embedded-software-in-apps-to-track-phones-11596808801>



Abbildung 20.2: Illustration: Harald K. Jansson/Norge i bilder

Laut Eigenwerbung verfolgt Anomaly Six täglich 230 Mio. Smartphones und sammelt pro Jahr 280 TeraByte Standortdaten (Stand 2022). In einer Demonstration zeigt Anomaly Six, wie der Weg von NSA Mitarbeiter vom Hauptsitz in Fort Meade nach Jordanien verfolgt werden kann oder der Einsatz von russischen Wagner Söldnern.¹⁴

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.

Metadaten der Kommunikation werden von den standardmäßig auf den Android Smartphones installierten Apps für SMS (Google Messaging App) und Telefonie (Google Dialer 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 zu reduzieren, kann man **Signal App** oder **Silence** als Default-App für SMS/MMS aktivieren. Silence ermöglicht auch verschlüsselte SMS.

¹⁴<https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-signal-surveillance-cia-nsa/>

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
- ...

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 suspekten 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:

- ungefähre (netzwerkbasierter) Standort
- genauer (GPS-)Standort
- uneingeschränkter Internetzugriff
- Browserverlauf und Lesezeichen lesen
- Browserverlauf und Lesezeichen erstellen
- Telefonstatus lesen und identifizieren
- 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 datensammelnde 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 oder... 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 Interessen aus. So sammelt Facebook beispielsweise über diesen Weg große Mengen an Daten über Nichtmitglieder, die in sogenannten Schattenprofilen geführt werden.

Die Webseite **Exodus Privacy**¹⁵ 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 das 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.

Neben den negativen Beispielen mit mehr als 30 Tracking Bibliotheken in einzelnen Apps findet man auf Exodus Privacy auch positive Beispiele ohne Tracker¹⁶. 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 privacy-freundlichen Browser (z. B. Firefox Klar) genutzt werden kann.

¹⁵<https://reports.exodus-privacy.eu.org/en/>

¹⁶https://reports.exodus-privacy.eu.org/en/reports/?filter=no_trackers

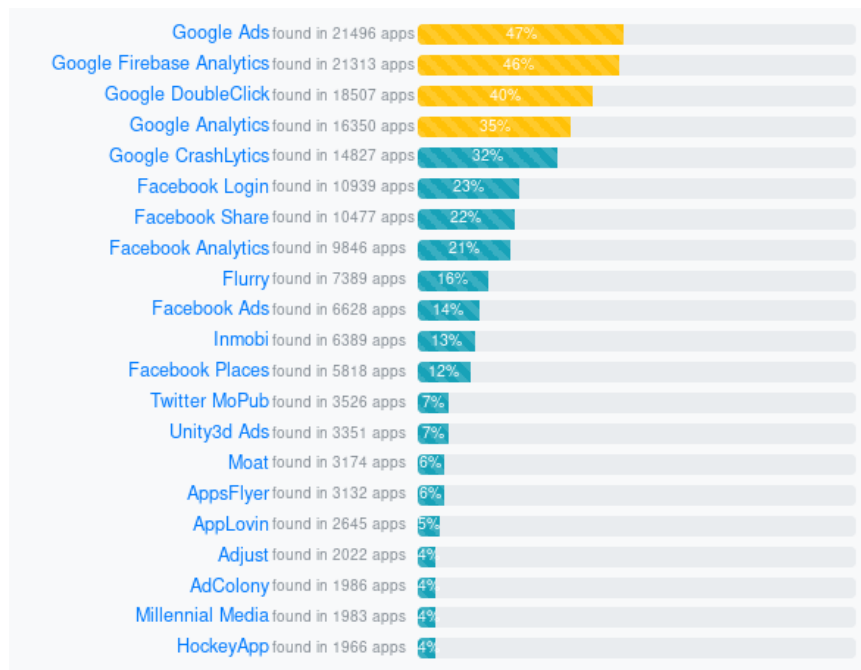


Abbildung 20.3: Die häufigsten Tracking Bibliotheken in Android Apps

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 verboten¹⁷. 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 an 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 Ka-

¹⁷<https://www.scmagazineuk.com/eu-parliament-blocks-microsoft-outlook-apps-over-privacy-fears/article/537584/>

mera 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**¹⁸ oder **FairEmail**¹⁹. Nach dem Wechsel auf eine vertrauenswürdige App sind die Passwörter für die betroffenen E-Mail Accounts zu wechseln!

20.2 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.
- 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 Communities werden systematisch analysiert, ohne dass die Personen im Verdacht stehen, eine Straftat begangen zu haben.²⁰
- 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 u.ä. Diktaturen.
- In der Ukraine wurden die Geofencing Daten von Handys bereits im Jan. 2014 zur Einschüchterung von Demonstranten genutzt. Teilnehmer einer Demonstration gegen den damals amtierenden Präsidenten bekamen eine SMS mit dem Inhalt:²¹

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.²²
- 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.²³ Die Überwachung Handys der Aktivisten begann bereits zwei Jahre vor dem G8-Gipfel in Heiligendamm.

¹⁸<https://k9mail.app>

¹⁹<https://email.faircode.eu>

²⁰<https://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims/>

²¹<https://www.heise.de/-2095284>

²²<https://www.heise.de/tp/artikel/34/34973/1.html>

²³<https://www.heise.de/tp/artikel/35/35043/1.html>

- 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 Verfassungsschutz sind.

- Die Bundeswehr entwickelt zusammen mit Airbus Group das Spionagesystem ISIS. Es soll an Bord einer Drohne die Überwachung von Mobilkommunikation aus der Luft ermöglichen. Wenn die Drohne über dem Gebiet Kassel, Gotha, Fulda oder Suhl kreist, könnte man mit ISIS das gesamte Gebiet der BRD überwachen.



Die Nutzung des Systems gegen Protestler wird ausdrücklich beworben:

Bei Protestcamps, Besetzungen u. ä. werden üblicherweise in größeren Umfang lizenzfreie Handfunkgeräte, Wi-Fi-Knoten, Schnurlostelefone und in geringerem Umfang auch Satellitentelefone eingesetzt. Üblicherweise werden diese Funksysteme von Gruppen oder Menschen mit hohem Organisationsgrad verwendet, die sich nicht auf das Funktionieren der überlasteten oder örtlich nicht verfügbaren Mobilfunknetze verlassen wollen. Der Inhalt dieser Funkverbindungen ist demzufolge aus Sicht eines Abhörers oft hochwertig, weil er Zugang zu strategischen Informationen verspricht. Für die Lokalisierung, Identifizierung und Aufzeichnung aller dieser Funksysteme ist ISIS hervorragend geeignet.

Die Aufgaben von ISIS kann man kurz zusammenfassen: Information, Spionage, Überwachung, Identifizierung. Das System soll aus den verarbeiteten Daten die Sprecher identifizieren können und mehrere tausend Mobilfunkgeräte gleichzeitig lokalisieren und verfolgen.

20.3 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.²⁴

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.

²⁴<http://news.cnet.com/2100-1029-6140191.html>

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 Mikrophone der Smartphones zur Raumüberwachung, um in Kombination mit den GPS Standortdaten nach der unzensurierten öffentliche Übertragung von Ligaspielen zu fahnden. Die App hat ca. 10 Mio. Nutzer in Spanien.²⁵
- Die Hamas hat anlässlich der WM ebenfalls eine App für Fußball Fans 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:²⁶

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 gelber-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.



20.4 WLAN 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.

Wenn man mit aktiviertem WLAN Modul und automatischem Login für die bevorzugte WLANs unterwegs ist, dann sendet das Smartphone oder der Laptop regelmäßig aktive Probes, um die Umgebung nach den bevorzugten WLANs zu scannen. Dabei wird neben der weltweit eindeutigen MAC Adresse auch eine Liste der SSIDs der bevorzugten WLANs gesendet, mit denen sich das Smartphone automatisch verbinden würde (Preferred Network List, PNL). Diese Liste liefert Informationen über Orte, an denen sicher der Besitzer des Smartphones bevorzugt aufhält. (Home, Office...)

Mit geringem technischen Aufwand kann man diese Daten der aktiven WLAN Probes zum Tracking und für Angriffe nutzen:

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.²⁷

²⁵<https://heise.de/-4075636>

²⁶<https://www.rt.com/news/431663-hamas-dating-app-idf-israel>

²⁷<http://apps.opendatacity.de/relog/>

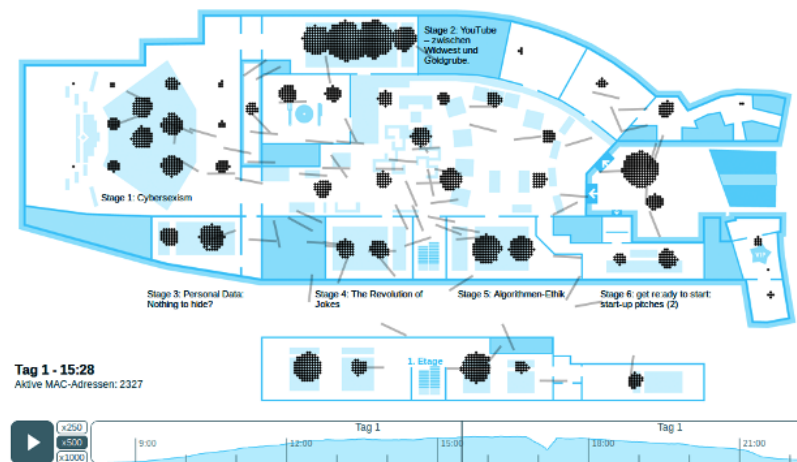


Abbildung 20.4: WLAN Tracking auf der re:publica 2013

2. Forscher der Università di Roma sind mit der Studie *Signals from the Crowd: Uncovering Social Relationships through Smartphone Probes*²⁸ einen Schritt weiter gegangen. Sie haben gezeigt, dass man die aktiven WLAN Probes für eine soziale Analyse der Crowd nutzen kann. Crowd steht dabei für eine Ansammlung von Personen (Teilnehmer von Veranstaltungen oder Demonstrationen, Bordell Besucher usw.).
3. Die Security Firma Sensepost ging noch einen Schritt weiter. Auf der Blackhat Asia 2014 wurde die *Drohne Snoopy*²⁹ vorgestellt. Diese Drohne wertet die Probes der WLAN Module aus und simuliert dann die SSID eines bevorzugten WLANs des Smartphones. Das Smartphone meldet sich 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. Auf Github.com steht der Source Code für Snoopy, Server und Webinterface für eigene Experimente zum Download bereit.
4. Android Smartphones kann ein Angreifer durch einen Fehler in der Funktion Wi-Fi Direct kompromittieren. Dabei stellt ein Angreifer einen virtuellen Accesspoint mit einer bösartigen SSID auf. Damit kann er verwundbare System in Funkreichweite lahm zu legen, Speicherinhalte auszulesen und potenziell sogar Schadcode zur Ausführung zu bringen. Das Problem betrifft auch Linux auf dem PC oder Laptop. Solange der Fehler nicht behoben wurde, können Linuxer in der Datei `/etc/wpa_supplicant/wpa_supplicant.conf` folgende Option als Schutz gegen diesen Angriff aktivieren:

```
p2p_disabled=1
```

Es gibt bereits erste praktische Ansätze der Werbeindustrie, um die WLAN Probes der Smartphones zum Schnüffeln zu nutzen:

- Die Werbefirma Renew 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 wurde über 4 Mio. Geräte auf dem Weg durch die Londoner City verfolgt.³⁰

We will cookie the street. (K. Memari, chief executive of Renew)

²⁸<http://conferences.sigcomm.org/imc/2013/papers/imc148-barberaSP106.pdf>

²⁹<http://www.sensepost.com/blog/7557.html>

³⁰<https://www.rt.com/news/trash-bin-surveillance-wifi-402/>

- **Ins Netz gegangen** (Pressemitteilung der BVG, PDF)³¹: Die Berliner Verkehrsbetriebe werden in Zusammenarbeit mit HOTSPLOTS auf den U-Bahnhöfen kostenfreien Wi-Fi zur Verfügung stellen. Bis Ende 2016 sollen 76 U-Bahnhöfe mit den Access Points ausgestattet werden. Die Bahnhöfe wurden so gewählt, das rechnerisch 2/3 der täglich 1,5 Mio U-Bahn-Kunden erfasst werden können. Außerdem wird mit kostenfreiem WLAN auf den Buslinien 200 und 204 experimentiert.

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 wird kein Name und E-Mail Adresse abgefragt.

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 gem. TKG und gemäß 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.

- Auf dem Flughafen Amstersam-Schiphol findet man folgendes Schild, das auf Wifi- und Bluetooth-Tracking hinweist (Abb: 20.5). Auf der Webseite des Flughafens findet man die Erklärung, dass das Wifi-Tracking genutzt wird, um die Anzahl und Bewegung der Reisenden in den unterschiedlichen Bereichen des Flughafens zu beobachten und damit die Anzeigen für die geschätzten Wartezeiten zu aktualisieren.



Abbildung 20.5: Wifi-Tracking am Flughafen Amsterdam-Schiphol

- Die Technik zur Verfolgung der Besucher- bzw. Kundenströme mittels Wifi-Tracking wird auch von mehrere Handelsketten wie z. B. Karstadt Sports und Escada eingesetzt, um Bewegungen der Kunden im Einkaufsbereich zu verfolgen.³²

Neben WLAN Tracking wird auch Bluetooth in Einkaufsfilialen eingesetzt, weil Bluetooth Beacons eine genauere Standortbestimmung der Kunden in der Filiale ermöglichen. Leider gibt es in Deutschland kein Gesetz, das ähnlich wie bei der Videoüberwachung einen deutlichen Hinweis auf das Wifi-Tracking fordert.

U. Spaan vom Handelsforschungsinstitut EHI schätzt, das 20% der Einzelhändler in Deutschland derzeit (Feb. 2018) mit Trackingmethoden in Läden experimentieren.

³¹<http://unternehmen.bvg.de/de/index.php?section=downloads&cmd=180&download=2070>

³²<https://www.heise.de/-3973727>

- Die Firma AdNear experimentiert mit Drohen, welche die Wi-Fi und Baseband Signale der Smartphones auswerten. Anhand der MAC Adresse der WLAN Module werden die Bewegungen der Nutzer verfolgt.³³

Today we started initial tests with drones to collect data. And the results have been fantastic! Besides, this turns out to be the most efficient mode.

Schlussfolgerung: WLAN abschalten, wenn man es nicht braucht.

20.5 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 eingetroffenen 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 beide Anforderungen zu erfüllen. Sie funktionieren folgendermaßen:

1. Eine App, die von einem Server über Neuigkeiten benachrichtigt werden möchte, fordert vom Push Service APN (Apple) oder FCM (Google) ein Push Token an.
2. Dann registriert die App dieses Push Token bei dem Server, der die App bei Neuigkeiten benachrichtigen soll (Mailserver o.ä.), und legt sich schlafen.
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 weiter.
5. Das Smartphone empfängt die Nachricht, weckt die passende App auf und übergibt ihr den (verschlüsselte) Inhalt der Push Nachricht. Alle weiteren Aktionen übernimmt die App.

Für Android Apps gibt es Projekte, die Push Services bereitstellen, die unabhängig von Google arbeiten. Bei iPhones ist man immer auf APN von Apple angewiesen.

Polling ist eine Alternative zu Push Services. Statt auf eine Benachrichtigung zu warten fragt die Smartphone App alle 10-20min 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 für die Privatsphäre

- Bei Verwendung von Push Benachrichtigungen kann der Push Service (APN oder FCM) protokollieren, wieviel Benachrichtigungen ein Nutzer für eine bestimmte App bekommt, also wie intensiv die App genutzt wird. Die konkreten Inhalte der Nachricht sind i.d.R verschlüsselt.
- Behörden zur Strafverfolgung und Geheimdienste haben gem. Bestandsdatenauskunft in DE des Recht, alle Informationen abzufragen, die ein Provider (E-Mail, Messenger, Cloud...) 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.

³³<https://adnear.com/february2015/experimenting-with-drones-for-data-collection.php>

Mit diesen Push Token könnten sich die Behörden an Google oder Apple wenden und dort weitere Informationen zum dem Smartphone abrufen, dass das Token registriert hat: Telefonnummer, IMEI, und MAC- und IP-Adressen, SIM Nummern. . .

Mit diesen Daten könnten sich die Behörden an die Mobilfunkprovider wenden und bekommen dort Namen, Adressen, Kontonummern. . . der gesuchten Personen.

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, haben französische Behörden via Europol vom E-Mail Provider Protonmail im Sep. 2021 neben einem Logging der IP Adressen vermutlich auch die Herausgabe der Push Token verlangt.³⁴

Konfiguration von Push oder Poll in den Smartphone Apps

- Messenger auf dem iPhone verwenden immer Push via APN, keine Alternative.
- Einige Privacy-freundliche Messenger für Android bieten eigene Push Services:
 - In Threema 4.71+ kann man unter *Einstellungen - Über Threema - Fehlerbehebung - Threema Push benutzen* auf den eigenen Push Service von Threema umschalten.
 - Signal App bietet auf der Webseite ein APK zum Download für Nutzer mit hohen Sicherheitsanforderungen, dass keine Google Services nutzt.

Diese eigenen Push Services funktionieren nur, wenn man der Messenger App *Hintergrundaktivität* und *Hintergrunddatenverkehr* erlaubt. Bei einigen Android Phones muss man zus. die Option *bei Akku Betrieb nicht einschränken* für diese Apps aktivieren.

- E-Mail Server müssen nicht unbedingt Push Services unterstützen. Deshalb bieten alle E-Mail Apps für die allgm. Verwendung die Möglichkeit, *Push* oder *Poll* für jeden Server einzeln zu konfigurieren.
- Bei spezielle E-Mail Apps für einen besonderen Dienst ist es bei Android unterschiedlich. Tutanota verwendet keine Push Services für die Android App. Die Protonmail App verwendet ausschließlich 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 oder /e/ für ältere Smartphones unterstützen kein Push via FCM. (Damit sind einige Apps auf diesen Systemen nicht nutzbar.)

20.6 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.³⁵

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:

³⁴<https://netzpolitik.org/2021/auf-anordnung-von-europol-protonmail-gab-ip-adressen-von-nutzerinnen-heraus/>

³⁵<https://reports.exodus-privacy.eu.org>

- Apple unterstützt die Trackingdienste dabei mit der Implementierung von DNS-over-TLS oder DNS-over-HTTPS in iOS Version 14+. Apps haben die Möglichkeit, mit wenig Code einen eigenen, unzensierten DNS Server via DoT oder DoH zu verwenden statt des Servers, der in den Systemeinstellungen konfiguriert wurde, und damit die Zensur durch den Nutzer zu umgehen. Ein Video erklärt die Schritte.³⁶
- Android Nutzer beschwerten sich seit Sept./Okt. 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 Android und iOS ist die Variante (2) empfehlenswert.

(1) Man könnte die Apps **Blokada** (Android, iPhone) oder **DNSCloak** (iPhone) installieren und als Trackingblocker nutzen. Beide Apps registrieren sich als VPN Dienst, so dass andere Apps den Traffic über zu diesen 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 auswählt.

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 Werbeserver 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*.

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 herunter zu laden, z. B. vom bekannten russischen DNS Anbieter AdGuard.³⁷
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.

20.7 Zugriff auf Standortdaten einschränken

Im Dez. 2020 hat der norwegische Journalist M. Gundersen eine Recherche veröffentlicht, die demonstrierte, dass viele Apps Standortdaten sammeln und an irgendwelche Firmen im

³⁶<https://developer.apple.com/videos/play/wwdc2020/10047/>

³⁷<https://adguard.com/en/blog/encrypted-dns-ios-14.html>

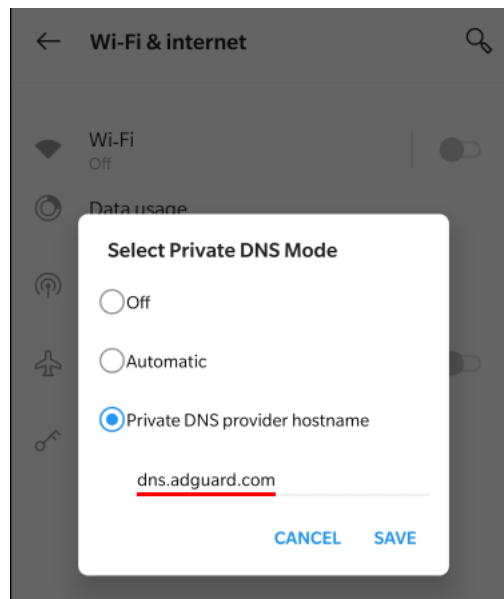


Abbildung 20.6: DNS-over-TLS Server in Android konfigurieren (Privates DNS)

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: 20.7).

- 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, ob es u.U. einmal sinnvoll sein könnte, der App Zugriff auf den Standort zu geben, wählt man *Nächstes Mal fragen* (z. B. Messenger).
- 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. könnte es hilfreich sein, dass 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 Industries³⁸ dazu übergegangen, das Standorttracking vor allem in Apps einzubauen, die einen exakten Standort benötigen (beispw. 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.

20.8 Krypto-Apps

Eine Warnung: Jede kryptografische Anwendung braucht einen vertrauenswürdigen Anker. Üblicherweise geht man davon aus, dass der eigene PC oder 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 Switch³⁹ hat Google die Möglichkeit, auf Android Handys beliebige Apps zu deinstallieren, zu installieren oder auszutauschen. Das iPhone⁴⁰ und Windows

³⁸<https://blog.appcensus.io/2021/10/25/what-the-huq/>

³⁹<https://mashable.com/2011/03/06/android-kill-switch>

⁴⁰<https://www.telegraph.co.uk/technology/3358134/Apples-Jobs-confirms-iPhone-kill-switch.html>



Abbildung 20.7: Zugriff auf Standortdaten für iPhone Apps konfigurieren

Phone⁴¹ haben ebenfalls einen Kill Switch. Jede Crypto-Anwendung aus den Markets muss also als potentiell kompromittiert gelten. Sie kann genau dann versagen, wenn man den Schutz am nötigsten braucht.

2. Smartphones sind leicht kompromittierbar:

- Remote Code Execution ist normalerweise ein schwerer Sicherheitsfehler. Bei Android Smartphones ist es ein Feature. Apps können Code aus dem Internet nachladen, der weder von Sicherheitsscanner auf dem Smartphone noch von den Sicherheitsprüfungen in App Stores kontrolliert werden kann. Viele kostenlose Apps für Spiele nutzen diese Möglichkeit für Werbezwecke. Da die Verschlüsselung der Internetverbindungen zu den Servern nicht immer dem aktuellen Stand entspricht oder garnicht vorhanden ist, kann ein Angreifer gezielt bestimmte Smartphones mit Trojanern verseuchen, indem er den Download on-the-fly modifiziert.
- 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 Privacy-Einstellungen verschärfen (je nach Intention).

OpenPGP-Verschlüsselung

Man kann OpenPGP auch auf dem Smartphone nutzen, aber:

Never store your private PGP key on your mobile phone... Mobile phones are inherently insecure. (Mike Cardwell)

Der Yubikey NEO hat eine OpenPGP Smartcard, die via NFC genutzt werden kann. Der private Schlüssel wird dabei auf dem Yubikey gespeichert und verlässt diese Umgebung nie. Die PIN zur Freigabe des Schlüssel wird zusammen mit den zu entschlüsselnden oder

⁴¹<https://www.heise.de/-1131297>

zu signierenden Daten via NFC an den Yubikey gesendet und das Ergebnis der Kryptooperation wird zurück an das Smartphone gegeben.

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 Version 3.2 vom 06. Mai 2015 wird der Yubikey NEO via NFC als OpenPGP Smartcard unterstützt.
 - Das E-Mail Programm **K9mail** kann direkt mit OpenKeychain zusammenarbeiten und integriert Buttons zum Verschlüsseln bzw. Entschlüsseln von E-Mails.
 - Der Jabber/XMPP Client **Conversations** kann in Kombination mit OpenKeychain die Chats mit OpenPGP verschlüsseln, der private Key liegt dabei aber auf dem Smartphone. OTR- und OMEMO-Verschlüsselung sind auch möglich.
2. Den Yubikey NEO bereitet man am einfachsten mit Enigmail auf einem PC vor (siehe: OpenPGP Smartcards). 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 aus Enigmail 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.

20.9 Stille SMS ind IMSI-Catcher erkennen

Die App **SnoopSnitch** von SRLabs steht seit Januar 2015 für Android im F-droid Store und im PlayStore bereit. Die App erkennt ISMI-Catcher und erkennt außerdem, ob jemand die Gespräche belauscht und mit einem SS7-Exploit die Verschlüsselung gehackt hat. Für die Installation ist ein Rooten des Smartphone nötig. Die App funktioniert nur, wenn das Smartphone einen Qualcomm Chipsatz hat.

Das **GSMK CryptoPhone** hat einen ganz gut funktionierenden IMSI-Catcher-Detector onBoard. Mit diesem Detector wurden in Washington DC in der Umgebung des White House und US Capitol sowie in der Nähe von Botschaften 18 IMSI-Catcher aufgespürt ⁴².

I would bet money that there are governments that are spying in DC. (C. Soghoian)

Washington DC ist kein Einzelfall. Auch in Oslo wurden IMSI-Catcher im Regierungsviertel gefunden. Leider mussten die Journalister einer Zeitung mit einem GSMK CryptoPhone die norwegische Spionageabwehr erst darauf aufmerksam machen. ⁴³

Die gefundenen Geräte seien nicht auf dem freien Markt erhältlich, sie seien sehr ausgereift und teuer. Nur Organisationen mit großen Ressourcen, etwa ausländische Geheimdienste, seien zu einer solchen Überwachung in der Lage.

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. Das Abhören von SMS und Telefonaten ist vermutlich eher nebensächlich. Das Smartphone ist eine Trackingwanze, die wir freiwillig mit uns umhertragen!

⁴²<https://rt.com/usa/189116-washington-dc-spying-phone>

⁴³<https://www.zeit.de/digital/datenschutz/2014-12/norwegen-spionage-oslo>

20.10 Angriffe mit Staatstrojanern erschweren

Der in den Medien bekannteste Staatstrojaner ist derzeit 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 Kryptohandys des spanischen Regierungschef und seine Verteidigungsministerin...

Die Pegasus Spionagesoftware ist in mehreren Preisstufen verfügbar:

- **Einsteigerversion:** bietet nur 1-Klick-Exploits zur Infektionen 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 für Smartphones.

Es gibt keinen 100% Schutz gegen einen Angreifer, der nahezu unbegrenzte finanzielle Mittel zur Verfügung hat. Aber trotzdem kann man Angriffe deutlich erschweren.

Die Sicherheitsfirma Kaspersky hat einige Tipps zum Schutz gegen Pegasus und andere Trojaner veröffentlicht und das Team von GrapheneOS fügt auch noch etwas hinzu:

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 vertrauenswürdigen VPN nutzen. (Oder Tor? - Hmmm, eher nicht.)
Man sollte einen VPN Provider wählen, der keine persönlichen Informationen abfragt. Statt den Apps der VPN Provider sollte man native VPN Apps wie Wireguard o.ä. bevorzugen. Die bevorzugte VPN App sollte Netzwerk Kill-Switch und Always-On-VPN unterstützen.
- Man kann die Zielerkennung erschweren, indem man nie Telefonnummern weitergibt und Messenger verwendet, die nicht an Telefonnummern gebunden sind (Threema, Session).
Hinweis: Man kann mit Threema oder Session Messenger auch telefonieren.
- Das Smartphone täglich rebooten, da persistente Exploits, die einen Reboot überstehen, teuer sind und selten genutzt werden.
- Gelegentlich sollte man den Akku Smartphone auch vollständig entladen lassen (*phone dies the natural death*) um es von NoReboot Trojanern zu reinigen.
- Ein gehärtetes Smartphone OS verwenden (GrapheneOS legt die Latte höher).

iPhones (Empfehlungen von Kaspersky)

- iMessages und Facetime deaktivieren, da sie am häufigsten angegriffen werden.
- Regelmäßige Backups in der iCloud speichern inklusive Systemstatus, um einen Trojanerbefall mit dem MVT Toolkit analysieren zu können.

Android (Empfehlungen von Kaspersky)

- Firefox Focus (Klar) statt Safari als Standardbrowser verwenden, da dieser nicht auf Webkit basiert, was zwar nicht generell sicherer ist aber Standardangriffe ins Leere laufen lässt.
- Das Smartphone nicht rooten und eine Sicherheitssuite installieren, die bei Jailbreaks warnt.

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 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 böartigem 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 vom Browser Vanadium in der Sektion *Datenschutz und Sicherheit* aktivieren.

Die Hinweise sind als Denkanstöße gedacht. Man muss sie nicht zu 100% umsetzen und sie bieten auch keinen 100% sicheren Schutz. Aber sie frustrieren einen Angreifer.

20.11 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 Malware auf einem Smartphone zu installieren oder Daten sowie Passwörter zu stehlen.

In Deutschland sind diese Angriffe kaum bekannt, weil es nur wenige öffentliche Ladestationen gibt. International ist man schon weiter, sowohl bei der Bereitstellung öffentlicher Ladestationen an Flughäfen, in Hotels und öffentlichen Plätzen, als auch...

Die Behörden von Los Angeles (USA) haben im Nov. 2019 eine dringende Warnung vor öffentlichen Ladestationen für Smartphones mit USB-Anschluss veröffentlicht.⁴⁴

Travellers should avoid using public USB power charging stations in airports, hotels and other locations because they may contain dangerous malware.

Moderne Smartphone haben einen Softwareschutz gegen diese Angriffe (in Android deaktivierbar). Das Smartphone sollte den Nutzer erst fragen, ob der Gegenüber vertrauenswürdig ist, wenn 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 o.ä. Händlern mit internationaler Lieferung bestellen.

20.12 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 Kontrolle des Hidden OS.

⁴⁴<http://da.lacounty.gov/community/fraud-alerts/juice-jacking-criminals-use-public-usb-chargers-steal-data>

Los Angeles County District Attorney's Office

USB Charger Scam



Travelers should avoid using public USB power charging stations in airports, hotels and other locations because they may contain dangerous malware.


In the USB Charger Scam, often called "juice jacking," criminals load malware onto charging stations or cables they leave plugged in at the stations so they may infect the phones and other electronic devices of unsuspecting users.

The malware may lock the device or export data and passwords directly to the scammer.


Helpful Tips

- Use an AC power outlet, not a USB charging station.
- Take AC and car chargers for your devices when traveling.
- Consider buying a portable charger for emergencies.

To learn about other frauds, visit <http://da.lacounty.gov/community/fraud-alerts>



IF YOU OR SOMEONE YOU KNOW HAS BEEN THE VICTIM OF A SCAM, PLEASE CONTACT YOUR LOCAL LAW ENFORCEMENT AGENCY



Jackie Lacey
Los Angeles County District Attorney

<http://da.lacounty.gov>
[@LADAOoffice](#)
[#FraudFriday](#)

Abbildung 20.8: Warnung vor USB Charger Scam

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..⁴⁵
- Mit den *Hexagon challenges* wurde auf der PacSec 2013 ein verbesserter Angriff auf das Hidden OS von Rals Phillip Weinmann vorgestellt..⁴⁶
- 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..⁴⁷

⁴⁵<http://www.securitytube.net/video/5372>

⁴⁶<http://pacsec.jp/speakers.html>

⁴⁷<http://phys.org/news/2013-08-firmware-tweak-block-subscriber-berlin.html>

- 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. Es wurden alle verfügbaren erfolgreich Smartphones kompromittiert.⁴⁸

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 pwned smartphones.

Der Angriff ist relativ aufwändig und wird daher wahrscheinlich sehr selten eingesetzt, da es einfachere Möglichkeiten durch Verteilung kompromittierter Apps via Play Store oder ähnliches gibt.

⁴⁸https://www.theregister.co.uk/2013/03/07/baseband_processor_mobile_hack_threat/Malware-flingers%20can%20pwn%20your%20mobile%20with%20over-the-air%20updates