

# Privacy-Handbuch

Spurenarm Surfen mit Mozilla Firefox,  
E-Mails verschlüsseln mit Thunderbird,  
Anonymisierungsdienste nutzen  
und Daten verschlüsseln  
für WINDOWS + Linux

20. September 2015

**Wir sind die Vielen,  
wir könnten einen Beat stampfen,  
der jede Macht pulverisieren wird.**

# Inhaltsverzeichnis

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>Scroogled</b>                         | <b>8</b>  |
| <b>2</b> | <b>Angriffe auf die Privatsphäre</b>     | <b>21</b> |
| 2.1      | Big Data - Kunde ist der, der bezahlt    | 22        |
| 2.1.1    | Google                                   | 22        |
| 2.1.2    | Datenhändler                             | 30        |
| 2.2      | Techniken der Datensammler               | 32        |
| 2.3      | Tendenzen auf dem Gebiet des Tracking    | 37        |
| 2.4      | Geotagging                               | 40        |
| 2.5      | Kommunikationsanalyse                    | 42        |
| 2.6      | Überwachungen im Internet                | 45        |
| 2.7      | NSA & Co.                                | 52        |
| 2.8      | Rechtsstaatliche Grundlagen              | 53        |
| 2.9      | Bundesamt für Verfassungsschutz auflösen | 55        |
| 2.10     | Ich habe doch nichts zu verbergen        | 60        |
| <b>3</b> | <b>Digitales Aikido</b>                  | <b>64</b> |
| 3.1      | Nachdenken                               | 64        |
| 3.2      | Ein Beispiel                             | 68        |
| 3.3      | Schattenseiten der Anonymität            | 70        |
| <b>4</b> | <b>Spurenarm Surfen</b>                  | <b>72</b> |
| 4.1      | Auswahl des Webbrowsers                  | 73        |
| 4.2      | Datensparsame Suchmaschinen              | 75        |
| 4.3      | Cookies                                  | 81        |
| 4.4      | EverCookies                              | 85        |
| 4.5      | JavaScript                               | 87        |
| 4.5.1    | NoScript für Mozilla Firefox             | 88        |
| 4.6      | iFrames                                  | 91        |
| 4.7      | Werbung, HTML-Wanzen und Social Media    | 93        |
| 4.7.1    | Tracking-Filter für Firefox              | 93        |
| 4.7.2    | Adblock für Mozilla Firefox              | 94        |
| 4.8      | History Sniffing                         | 98        |
| 4.9      | Browsecache                              | 98        |
| 4.10     | Referer                                  | 100       |
| 4.11     | Risiko Plugins                           | 101       |
| 4.11.1   | PDF Reader Plugins                       | 101       |
| 4.11.2   | Java-Applets                             | 102       |

|          |  |            |
|----------|--|------------|
| 4.11.3   | Flash-Applets und Flash-Videos                     | 103        |
| 4.11.4   | Weitere Anwendungen                                | 106        |
| 4.11.5   | H.264 Plug-in und Adobe Primetime deaktivieren     | 106        |
| 4.12     | HTTPS-Verschlüsselung nutzen                       | 107        |
| 4.13     | Vertrauenswürdigkeit von HTTPS                     | 108        |
| 4.13.1   | Verbesserung der Vertrauenswürdigkeit von HTTPS    | 111        |
| 4.13.2   | Firefox Add-ons                                    | 112        |
| 4.13.3   | OCSP abschalten                                    | 114        |
| 4.13.4   | Tracking via SSL Session                           | 114        |
| 4.13.5   | Tracking via HTTP Strict Transport Security (HSTS) | 115        |
| 4.13.6   | Schwache SSL-Cipher deaktivieren                   | 116        |
| 4.14     | Starke Passwörter nutzen                           | 119        |
| 4.15     | Zwei-Faktor-Authentifizierung                      | 121        |
| 4.16     | Installierte Schriftarten verstecken               | 122        |
| 4.17     | HTML5 Canvas Elemente                              | 124        |
| 4.18     | User-Agent modifizieren für Firefox                | 125        |
| 4.19     | Hardware Fingerprinting                            | 126        |
| 4.20     | Sonstige Maßnahmen                                 | 127        |
| 4.21     | Snakeoil für Firefox (überflüssiges)               | 130        |
| <b>5</b> | <b>Bezahlen im Netz</b>                            | <b>133</b> |
| 5.1      | Kreditkarten                                       | 134        |
| 5.2      | Bezahlsysteme der Deutschen Bahn                   | 135        |
| 5.3      | Paysafecard, UKash, Pecunix                        | 135        |
| 5.4      | Anonyme Online-Zahlungen vor dem Aus?              | 137        |
| 5.5      | Bargeld  | 138        |
| 5.6      | Bitcoin  | 140        |
| 5.6.1    | Exchanger / Marktplätze                            | 141        |
| 5.6.2    | Bitcoin Software                                   | 142        |
| 5.6.3    | Anonymität von Bitcoin                             | 145        |
| 5.6.4    | Bitcoin anonym nutzen                              | 146        |
| <b>6</b> | <b>E-Mail Kommunikation</b>                        | <b>149</b> |
| 6.1      | E-Mail Provider                                    | 149        |
| 6.2      | Mozilla Thunderbird                                | 153        |
| 6.2.1    | Account erstellen                                  | 153        |
| 6.2.2    | Sichere Optionen für SSL/TLS-Verschlüsselung       | 156        |
| 6.2.3    | Sichere Konfiguration des E-Mail Client            | 161        |
| 6.2.4    | Datenverluste vermeiden                            | 163        |
| 6.2.5    | Wörterbücher installieren                          | 164        |
| 6.2.6    | X-Mailer Kennung modifizieren                      | 165        |
| 6.2.7    | Spam-Filter aktivieren                             | 166        |
| 6.2.8    | Spam vermeiden                                     | 167        |
| 6.2.9    | Private Note                                       | 170        |
| 6.2.10   | RSS-Feeds  | 171        |
| 6.2.11   | Filelink   | 173        |
| 6.3      | ProtonMail und Lavaboom                            | 173        |

|  |            |
|--|------------|
| <b>7 E-Mails verschlüsseln</b>                       | <b>177</b> |
| 7.1 GnuPG und Thunderbird                            | 179        |
| 7.1.1 Installation von GnuPG                         | 179        |
| 7.1.2 Verbesserte Konfiguration von GnuPG            | 179        |
| 7.1.3 Installation der Enigmail-Erweiterung          | 180        |
| 7.1.4 Schlüsselverwaltung                            | 182        |
| 7.1.5 Signieren und Verschlüsseln erstellter E-Mails | 184        |
| 7.1.6 Adele - der freundliche OpenPGP E-Mail-Roboter | 186        |
| 7.1.7 Verschlüsselung in Webformularen               | 187        |
| 7.1.8 GnuPG SmartCard nutzen                         | 188        |
| 7.1.9 OpenPGP Keyserver                              | 192        |
| 7.1.10 OpenPGP-Verschlüsselung für Kontaktformulare  | 194        |
| 7.1.11 Web des Vertrauens                            | 196        |
| 7.1.12 Schlüssel zurückrufen                         | 199        |
| 7.2 S/MIME mit Thunderbird                           | 200        |
| 7.2.1 Kostenfreie Certification Authorities          | 200        |
| 7.2.2 Erzeugen eines Zertifikates                    | 201        |
| 7.2.3 S/MIME-Krypto-Funktionen aktivieren            | 202        |
| 7.2.4 Zertifikate der Partner und der CA importieren | 203        |
| 7.2.5 Nachrichten verschlüsseln und signieren        | 204        |
| 7.3 Root-Zertifikate importieren                     | 205        |
| 7.3.1 Webbrowser Firefox                             | 206        |
| 7.3.2 E-Mail-Client Thunderbird                      | 206        |
| 7.4 Eine eigene Certification Authority              | 207        |
| 7.5 Ist S/MIME-Verschlüsselung unsicher?             | 209        |
| 7.6 Eine Bemerkung zum Abschluß                      | 212        |
| <b>8 E-Mail jenseits der Überwachung</b>             | <b>214</b> |
| 8.1 Anonyme E-Mail Accounts                          | 214        |
| 8.2 Private Messages in Foren nutzen                 | 215        |
| 8.3 alt.anonymous.messages                           | 215        |
| 8.4 Mixmaster Remailer                               | 215        |
| <b>9 Instant Messaging (Jabber/XMPP)</b>             | <b>223</b> |
| 9.1 Jabber (XMPP)                                    | 223        |
| 9.2 Jabbern mit Jitsi                                | 225        |
| <b>10 Internettelefonie (VoIP)</b>                   | <b>230</b> |
| 10.1 Open Secure Telephony Network (OSTN)            | 231        |
| 10.1.1 OSTN-Provider                                 | 232        |
| 10.2 VoIP-Client Jitsi                               | 232        |
| <b>11 Anonymisierungsdienste</b>                     | <b>235</b> |
| 11.1 Warum sollte man diese Dienste nutzen?          | 235        |
| 11.2 Tor Onion Router und JonDonym                   | 237        |
| 11.2.1 Finanzierung der Anonymisierungsdienste       | 240        |
| 11.2.2 Security Notes                                | 241        |
| 11.3 Tor Onion Router nutzen                         | 242        |
| 11.3.1 Anonym Surfen mit Tor                         | 242        |
| 11.3.2 Tor Bad Exit Nodes                            | 247        |

|           |  |            |
|-----------|--|------------|
| 11.3.3    | Tor Good Exit Nodes                        | 249        |
| 11.3.4    | Tor Hidden Services                        | 251        |
| 11.4      | JonDonym nutzen                            | 254        |
| 11.4.1    | JonDonym Premium Account einrichten        | 256        |
| 11.4.2    | Anonym Surfen mit dem JonDoFox             | 258        |
| 11.5      | Anonyme E-Mails mit Thunderbird            | 262        |
| 11.6      | Anonym Bloggen                             | 267        |
| 11.7      | Anonymes Instant-Messaging (Jabber/XMPP)   | 268        |
| 11.8      | Anonymes Instant-Messaging mit TorChat     | 271        |
| 11.9      | Anonymes Filesharing                       | 273        |
| 11.10     | POND - die bessere E-Mail                  | 275        |
| 11.11     | proxychains für Linux                      | 278        |
| 11.12     | Finger weg von unseriösen Angeboten        | 280        |
| 11.12.1   | Tor-Boxen                                  | 280        |
| 11.12.2   | Web-Proxys                                 | 280        |
| 11.12.3   | Free Hide IP                               | 281        |
| 11.12.4   | ZenMate                                    | 281        |
| 11.12.5   | 5socks.net                                 | 282        |
| 11.12.6   | BlackBelt Privacy, Cloakfish und JanusVM   | 284        |
| 11.12.7   | Proxy-Listen                               | 285        |
| <b>12</b> | <b>Anonyme Peer-2-Peer Netzwerke</b>       | <b>286</b> |
| 12.1      | Invisible Internet Project (I2P)           | 288        |
| 12.1.1    | Installation des I2P-Routers               | 288        |
| 12.1.2    | Konfiguration des I2P-Router               | 290        |
| 12.1.3    | Anonym Surfen mit I2P                      | 292        |
| 12.1.4    | I2P Mail 1 (Susimail)                      | 294        |
| 12.1.5    | I2P Mail 2 (Bote)                          | 297        |
| 12.1.6    | I2P IRC                                    | 300        |
| 12.1.7    | I2P BitTorrent                             | 302        |
| 12.2      | DSL-Router und Computer vorbereiten        | 303        |
| <b>13</b> | <b>Daten verschlüsseln</b>                 | <b>304</b> |
| 13.1      | Konzepte der vorgestellten Tools           | 305        |
| 13.2      | Gedanken zum Passwort                      | 306        |
| 13.3      | Quick and Dirty mit GnuPG                  | 309        |
| 13.3.1    | GnuPG für WINDOWS                          | 309        |
| 13.4      | EncFS für Windows, Linux, MacOS und BSD    | 310        |
| 13.5      | dm-crypt für Linux                         | 312        |
| 13.5.1    | Bis zu 8 Passwörter mit LUKS               | 313        |
| 13.5.2    | Verschlüsselten Container erstellen        | 313        |
| 13.5.3    | Passwörter verwalten                       | 315        |
| 13.5.4    | Verschlüsselten Container öffnen/schließen | 315        |
| 13.5.5    | Debian GNU/Linux komplett verschlüsseln    | 318        |
| 13.5.6    | Ubuntu komplett verschlüsseln              | 319        |
| 13.5.7    | HOME-Verzeichnis verschlüsseln             | 319        |
| 13.5.8    | SWAP und /tmp verschlüsseln                | 319        |
| 13.6      | Backups verschlüsseln                      | 321        |
| 13.6.1    | Schnell mal auf den USB-Stick              | 321        |
| 13.6.2    | Online Backups                             | 324        |

|   |            |
|---|------------|
| <b>14 Daten löschen</b>                         | <b>327</b> |
| 14.1 Dateien in den Papierkorb werfen           | 327        |
| 14.2 Dateien sicher löschen (Festplatten)       | 327        |
| 14.3 Dateireste nachträglich beseitigen         | 328        |
| 14.4 Dateien sicher löschen (SSDs)              | 329        |
| 14.5 Gesamten Datenträger säubern (Festplatten) | 330        |
| 14.6 Gesamten Datenträger säubern (SSDs)        | 331        |
| <b>15 Daten anonymisieren</b>                   | <b>332</b> |
| 15.1 Fotos und Bilddateien anonymisieren        | 332        |
| 15.2 PDF-Dokumente säubern                      | 333        |
| 15.3 Metadata Anonymisation Toolkit (MAT)       | 333        |
| <b>16 Daten verstecken</b>                      | <b>336</b> |
| 16.1 Allgemeine Hinweise                        | 337        |
| 16.2 steghide                                   | 338        |
| 16.3 stegdetect                                 | 339        |
| <b>17 Betriebssysteme</b>                       | <b>340</b> |
| 17.1 Risiko USB, Firewire und Thunderbolt       | 345        |
| 17.2 Linux Firewall konfigurieren               | 347        |
| 17.3 Privacy Leaks mit DHCP                     | 350        |
| <b>18 Live-DVDs</b>                             | <b>354</b> |
| 18.1 USB-Sticks als Bootmedium vorbereiten      | 355        |
| 18.2 BIOS-Einstellungen für Win8 Rechner        | 356        |
| <b>19 Smartphones</b>                           | <b>357</b> |
| 19.1 Kommerzielle Datensammlungen               | 358        |
| 19.2 Überwachung                                | 359        |
| 19.3 Stille SMS und IMSI-Catcher erkennen       | 361        |
| 19.4 WLAN ausschalten, wenn nicht genutzt       | 362        |
| 19.5 WhatsApp Alternative                       | 365        |
| 19.6 Crypto-Apps                                | 368        |

# 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 Labradors 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 präsentierten, die sie nicht aufrufen können, würde sie das doch nur frustrieren - das wäre ein mieses Nutzererlebnis.*”

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

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

“... verraten und vergoogelt.”

“Voll und ganz”, nickte sie.

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

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

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

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

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

“Tu es”, sagte er.

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

Nun gut, das sollte ihm recht sein.

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

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

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

Er entfernte Kette und Riegel und öffnete die Tür. Maya huschte an ihm vorbei, gefolgt von den Hunden und ihrer Freundin. Sie war schweißüberströmt, ihr normalerweise gekämmtes Haar hing strähnig in die Stirn. Sie rieb sich die 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 beobachteten mich - jeden Klick, jede Suche. Zeit zu verschwinden, jedenfalls aus ihrer Reichweite.”

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

“Wir müssen jetzt los”, beharrte sie.

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

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

“Greg, kommst du nun?”

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

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

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

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

zwei Männer vor seiner Tür standen.

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

Greg hatte diese Szene eine Woche lang im Geist durchgespielt, und er hatte sich allerlei mutige Dinge zurechtgelegt, die er hatte sagen wollen. Es war eine willkommene Beschäftigung gewesen, während er auf Mayas Anruf 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 Fahrradständern parkte, hatte er sich selbst überzeugt. Während er sich noch fragte, welche Sorte Bio-Fruchtshake er heute in der Kantine bestellen würde, verweigerte seine Codekarte den Zugang zu Haus 49. Die rote LED blinkte immer nur blöde vor sich hin, wenn er seine Karte durchzog. In jedem anderen Gebäude würde immer mal jemand raus- und wieder reinkommen, dem man sich anschließen könnte. Aber die Googler in 49 kamen höchstens zum Essen raus, und manchmal nicht einmal dann.

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

“Greg, kann ich Sie bitte sprechen?“

Der verschrumpelte Mann legte einen Arm um seine Schulter, und Greg atmete den Duft seines Zitrus-Rasierwassers ein. So hatte sein Tauchlehrer in Baja geduftet, wenn sie abends durch die Kneipen 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 Wöhrl dafür, dass sie den Text unter einer Creative Commons Lizenz zur Nutzung durch Dritte bereitstellen.*

## Kapitel 2

# Angriffe auf die Privatsphäre

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

Im Internet ist es genau umgekehrt. Von jedem Nutzer werden Profile erstellt. Websitebetreiber sammeln Informationen (Surfverhalten, E-Mail-Adressen), um beispielsweise mit dem Verkauf der gesammelten Daten ihr Angebot zu finanzieren. Betreiber von Werbe-Servern nutzen die Möglichkeiten, das Surfverhalten websiteübergreifend 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, unsere Kommunikation wird gescannt, Geheimdienste sammeln kompromittierendes Material. . .

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

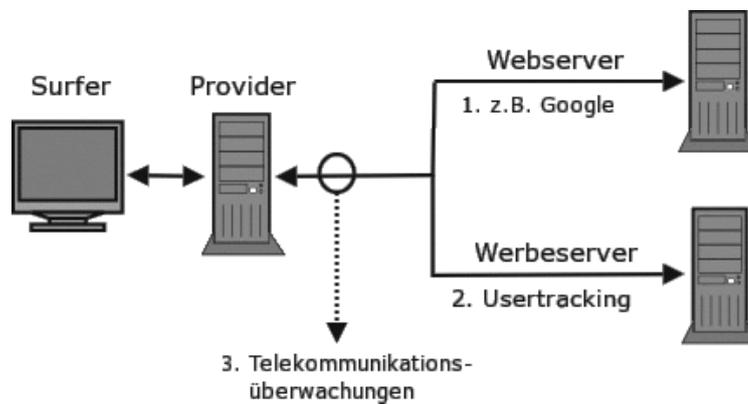


Abbildung 2.1: Möglichkeiten zur Überwachung im WWW

## 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)

#### Google Web Search

Googles Websuche ist in Deutschland die Nummer Eins. 89% der Suchanfragen gehen direkt an *google.de*. Mit den Suchdiensten wie Ixquick, Metager2, Web.de... die indirekt Anfragen an Google weiterleiten, beantwortet der Primus ca. 95% der deutschen Suchanfragen. (Stand 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 zeigt, wie gut diese Analyse der Suchanfragen bereits 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 alle Anderen 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 Bösenaufsicht 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* ebenfalls 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 wesentliche 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 Website Betreibern unterstützt.

97% der TOP100 Websites und ca. 80% der deutschsprachigen Webangebote sind mit verschiedenen Elementen von Google für die Einblendung kontextsensitiver Werbung und Traffic-Analyse infiziert! (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 politischen 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

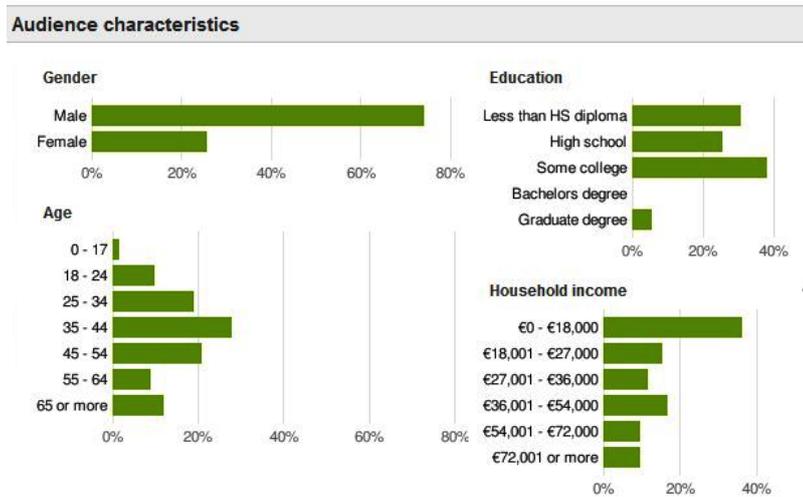


Abbildung 2.2: Ad-Planner Besucherstatistik (Beispiel)

Informationen zu Bildung und Haushaltseinkommen müssen im Vergleich zu allgemeinen Statistiken der Bevölkerung bewertet werden, was hier mal entfällt.

**Wie kommt das Imperium zu diesen Daten?** Es gibt so gut wie keine Möglichkeit, diese Daten irgendwo einzugeben. Google fragt NICHT nach diesen Daten, sie werden 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 Mail, Talk, News... und Google+ (personalisierte Dienste)

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

Börsennachrichten..... iGoogle)

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 Livestyle-Gadget getarnte Tracking Devices.

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

### Mozilla Firefox

Google ist der Hauptsponsor der Firefox Entwickler. Seit 2012 zahlt Google jährlich 300 Mio. Dollar an die Mozilla Foundation, um die voreingestellte Standardsuchmaschine in diesem Browser zu sein.

Das ist natürlich in erster Linie ein Angriff auf Microsoft. Die Entwickler von Firefox kommen ihrem 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 (z.B. bei der Variante *Iceweasel* von Debian GNU/Linux oder bei Ubuntu), 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, Surfer 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.<sup>1</sup>

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 wesentlich mit der NSA im Rahmen von PRISM kooperieren würden. Rajesh De, Leiter

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

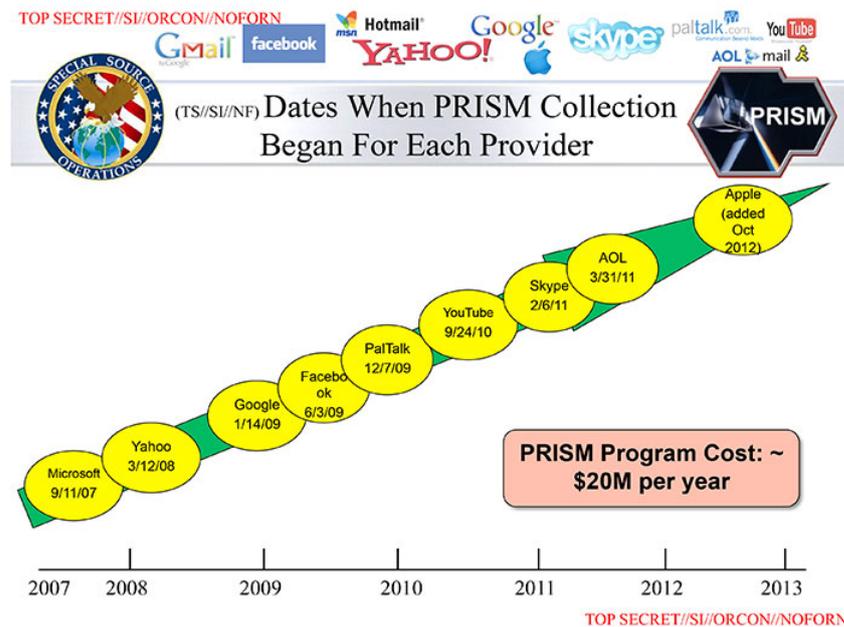


Abbildung 2.3: NSA-Folie zu den PRISM-Partnern

der Rechtsabteilung der NSA, dementierte die Dementis<sup>2</sup> 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 sicher<sup>3</sup>, dann kann man es als PR-Gag abtun. Google ist aufgrund geltender Gesetze zur Kooperation mit den weitreichenden Späh-Programmen der NSA verpflichtet. Lediglich für das Beschnüffeln der US-Bürger gibt es kleine Hürden.

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.

<sup>2</sup> <http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google-yahoo-co-nsa-anwalt-internetfirmen-wussten-von-ausspaehaktionen-1285553.html>

<sup>3</sup> <http://heise.de/-2138499>

### 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.

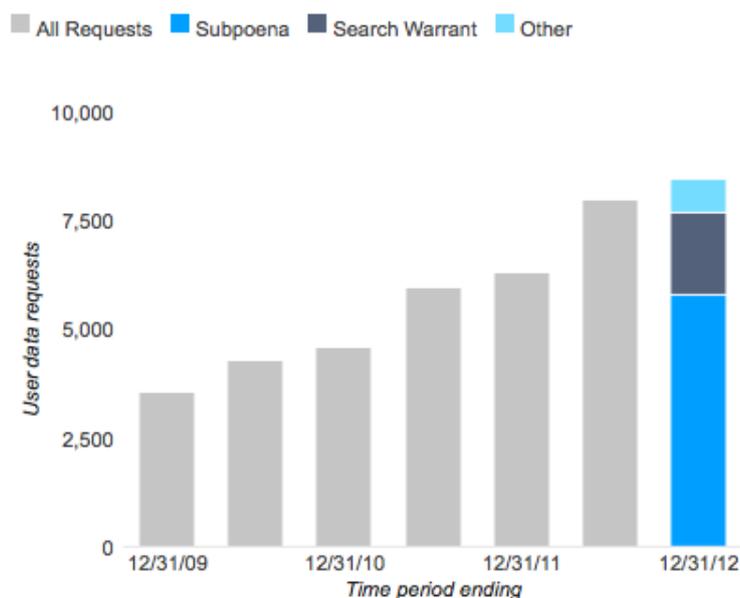


Abbildung 2.4: Steigerung der Auskünfte von Google an Behörden

### 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 Datenhändler**

Die Datensammler (Facebook, Amazon, Twitter...) 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 prahlt 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)*

**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.*

**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.

**RapLeaf** wurde von P. Thiel gegründet, der auch die Gründung von PayPal.com finanzierte, bei Facebook maßgeblichen Einfluss hat und dessen Credo eine totale Personalisierung des Internet ist.

RapLeaf sammelt selbst Daten über die Internetnutzung und verarbeitet hinzugekaufte Daten. Die Informationen werden anhand von E-Mail Adressen zusammengefasst. Jeder kann auf der Website eine Liste von E-Mail Adressen hochladen, bezahlen und nach Zahlungseingang die Daten abrufen. Ein kleiner Auszug aus der Preisliste (Stand 2011) soll den Wert persönlicher Informationen zeigen:

- Alter, Geschlecht und Ort: 0 Cent (Lockangebot)
- 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: 3 Cent pro E-Mail-Adresse
- Beruf und Ausbildung: 2 Cent pro E-Mail-Adresse
- Tätigkeit als Blogger: 3 Cent pro E-Mail-Adresse
- wohltätige Spenden: 3 Cent pro E-Mail-Adresse
- Präferenzen für hochwertige Marken: 3 Cent pro E-Mail-Adresse
- Präferenzen für Bücher, Zeitschriften: 3 Cent pro E-Mail-Adresse
- ...

## 2.2 Techniken der Datensammler

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

Es geht aber längst nicht nur um die Einblendung von Werbung. Sarah Downey warnt<sup>4</sup> 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.<sup>5</sup>

### Techniken zum Tracking des Surfverhaltens

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

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

Blockieren der Cookies von Drittseiten schützt nur teilweise vor dem Tracking mit Cookies. Die Datensammler haben Methoden entwickelt, um Tracking Cookies als First-Party Content zu platzieren<sup>6</sup>. 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

<sup>4</sup> <http://heise.de/-1628313>

<sup>5</sup> <http://heise.de/-1626368>

<sup>6</sup> <https://anonymous-proxy-servers.net/blog/index.php?/archives/377-Tracking-mit-Cookies.html>

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.

**Flash-Cookies** werden seit 2005 verwendet, um gelöschte Tracking-Cookies wiederherzustellen. Sie sind unabhängig vom Browser und funktionieren auch, wenn man verschiedene Browser oder Browserprofile für spurarmes Surfen und Fun-Surfen nutzt.

**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.

Die Like-Buttons verschiedener Social Networks und Werbebanner können 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 kann<sup>7</sup>. Das Verfahren kann für verschiedene Fragestellungen angepasst werden. Die Klicks auf Facebook Like Buttons können in der gleichen Weise ausgewertet werden. Forscher der Universität Cambridge (Großbritannien) konnten bei einer Untersuchung die sexuelle Orientierung und politische Einstellung der Nutzer anhand der Klicks auf Like Buttons vorhersagen<sup>8</sup>.

**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 Techniken<sup>9</sup> erarbeitet. 38% der populären Webseiten nutzen bereits verschiedene EverCookie Techniken (Stand: Okt. 2012).

<sup>7</sup> <http://arstechnica.com/tech-policy/news/2010/10/more-privacy-headaches-for-facebook-gay-users-outed-to-advertisers.ars>

<sup>8</sup> <http://heise.de/-1820638>

<sup>9</sup> <http://samy.pl/evercookie>

**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 Panopticklick<sup>10</sup> 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 Canvoas in HTML5*<sup>11</sup> beschrieben.
4. Plug-in basiert: Informationen werden per Flash- oder Java-Plugin ausgelesen (installierte Schriftarten, Betriebssystem, Kernel Version, Multi-Monitor Setups, Bildschirmgröße).
5. Add-on basiert: Durch Seiteneffekte werden evtl. vorhandene Browser Add-ons analysiert (NoScript Whitelist, Adblock Blacklist, fehlerhaftes User-Agent Spoofing).
6. Hardware basiert: Informationen über die Hardware des genutzten Rechners werden gesammelt (Batteriestatus, Vibrator-API, Zugriff auf Mikrofon und Webcam, Performance der Grafikhardware).

Die Studien *Dusting the Web for Fingerprints*<sup>12</sup> (2013) und *The web never forgets*<sup>13</sup> (2014) der KU Leuven (Belgien) haben nachgewiesen, das Fingerprinting bereits für das Tracking genutzt wird:

- *Bluecava* nutzt ausschließlich Browser Fingerprinting und protzt mit 30% besseren Ergebnissen als Cookie-basierte Techniken.<sup>14</sup>
- *Zanox.com* nutzt den Fingerprint des Browser, wenn Cookies gelöscht oder per Browser-Einstellung blockiert werden.<sup>15</sup>

<sup>10</sup> <https://panopticklick.eff.org/browser-uniqueness.pdf> (PDF)

<sup>11</sup> <http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf>

<sup>12</sup> <http://www.cosic.esat.kuleuven.be/publications/article-2334.pdf>

<sup>13</sup> [https://securehomes.esat.kuleuven.be/gacar/persistent/the\\_web\\_never\\_forgets.pdf](https://securehomes.esat.kuleuven.be/gacar/persistent/the_web_never_forgets.pdf)

<sup>14</sup> <http://www.bluecava.com/visitor-insight-campaign-measurement>

<sup>15</sup> <http://blog.zanox.com/de/zanox/2013/09/11/zanox-stellt-tpv-fingerprint-tracking-vor/>

- *WebTreck* 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 (AN/AUS).<sup>16</sup>
- *Multicounter* nutzt den Fingerprint zusätzlich zu Cookies oder Ever-Cookies zur Verbesserung der Erkennungsraten.<sup>17</sup>
- *Piano Media* verwendet Flash-basiertes Fingerprinting, um Paywall Restriktionen für Online Medien durchzusetzen.
- *Anonymizer Inc.* verwendet Browser Fingerprinting auf allen Ihren Webseiten, verschweigt es aber im Privacy Statement. (Eine seltsame Auffassung für jemanden, der Anonymität verkaufen will.)
- *Yahoo! Web Analytics* nutzt Javascript Tracking Code, wenn Cookies blockiert werden.
- *AddThis.com* verwendete seit Februar 2014 testweise Canvas-Fingerprinting, hat nach eigenen Angaben diese Trackingmethode aber wieder aufgegeben.

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 Ad-Block, um Tracking-Scripte im First-Party Kontext 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 Tracking-feature.

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 entstehenden umfangreiche Sammlung der biometrischen Profile kann zukünftig zum Tracking und zur Deanonymisierung genutzt werden.

Für die Auswertung werden nicht nur die Informationen zur besuchten Webseite genutzt. Besonders aussagekräftig sind z.B. die Klicks auf Werbung.

---

<sup>16</sup> <http://www.webtrekk.com/de/index/datenschutzerklaerung.html>

<sup>17</sup> <http://www.multicounter.de/features.html>

### 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 Test<sup>18</sup> 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.

<sup>18</sup> <https://emailprivacytester.com/>

**Tracking von Dokumenten (PDF, Word usw.)**

Die Firma ReadNotify bietet 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.

**2.3 Tendenzen auf dem Gebiet des Tracking**

Obwohl 80% der Internetnutzer das Tracking des Surfverhaltens ablehnen, wird es stetig weiter ausgebaut. Dabei sind folgende Tendenzen erkennbar:

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              |

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 (Mai)  | 34% der Webseiten       |
| 2012 (Okt.) | 38% der Webseiten       |

3. Flash-Cookies (LSOs) werden seltener eingesetzt. Diese Technik befindet sich auf dem absteigenden Ast. Im Oktober 2012 setzten nur noch 11% der populären Webseiten Flash-Cookies ein. Dabei handelt es sich überwiegend um Webseiten mit Flash-Videos. *Youporn.com* speichert persönliche Präferenzen beispielsweise in Flash-Cookies.
4. Durch den Aufkauf kleinerer Anbieter durch die Großen der Branche erfolgt eine Marktvereinigung. Es bilden sich sogenannte Tracking-Familien, die die Daten untereinander austauschen und somit eine große Reichweite bei der Beobachtung des Surfverhaltens haben. Die größten Tracking-Familien sind:

- (a) Die Google-Familie ist unangefochten die Nummer Eins. 44% der weltweiten Umsätze in der Onlinewerbung werden durch diese

Gruppe erzielt. Das Google Imperium hat in den letzten Jahren die Firmen *YouTube*, *DoubleClick mit falkad.net*, *FeedBurner*, *Springs*, *Adscape*, *AdMob*, *Teracent*, *Invite Media*, *Admeld*, *Adelphic*, *Wildfire Interactive* u.a.m. aufgekauft. 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               |
| 2009 | auf 80% der Webseiten               |
| 2012 | auf 97% der Webseiten               |

- (b) Auf den Plätzen 2-4 folgen die Tracking-Familien von Microsoft (u.a. mit den Trackingdiensten *atdmt.com*, *adbureau.com*, *aquantive.com*), die Yahoo! Familie (mit den Trackingdiensten *adrevolver*, *yieldmanager*, *overture*) und die AOL-Familie (mit *adsonar.com*, *tacoda.net*, *advertising.com*) mit einem Marktanteil von jeweils 3-8%.
- (c) Die im Februar 2013 vereinbarte Kooperation von Facebook mit den bisher eigenständigen Trackingdiensten BlueKai und Epsilon bildet den Kern einer neuen bedeutenden Tracking Familie.
5. 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 *Axciom* und *Datalogix* bekannt gegeben. Diese Firmen werten umfangreiche Daten aus der realen Welt aus (Kreditkartenzahlungen, Rabattkarten usw.). Damit sollen die Werbeeinblendung 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.
  - 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)*

6. 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 das Surfverhalten der Internetnutzer für die Sicherheit der USA wichtig und notwendig ist.

Die EFF.org kommentierte:

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

Durch die Snowden-Dokumenten wurden konkrete Beispiele bekannt.<sup>19</sup>

- Die NSA beobachtet den Datenverkehr und nutzt z.B. 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).
7. 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.<sup>20</sup>

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

Außerdem zeigte Merkel sich überzeugt, dass...

<sup>19</sup> <https://www.eff.org/deeplinks/2013/12/nsa-turns-cookies-and-more-surveillance-beacons>

<sup>20</sup> <https://netzpolitik.org/2015/merkel-stellt-sich-gegen-datenschutz-und-netzneutralitaet/>

*... sehr viel mehr Arbeitsplätze geschaffen werden mit der Wertschöpfung aus der Kenntnis der Daten. Wenn wir uns diesen Teil der Wertschöpfung aber abkoppeln und in Europa nicht stattfinden lassen, dann werden wir ein großes Problem haben.*

Wir werden also zukünftig mehr auf Selbstschutz angewiesen sein.

## 2.4 Geotagging

Geotagging ist *the next big thing* unter den Angriffen auf die Privatsphäre. Es geht um die Frage, wo wir etwas tun oder getan haben und welche Bewegungsmuster erkennbar sind.

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.
2. 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* <sup>21</sup>.

Das Magazin Wired berichtete im Danger Room (Oktober 2011), dass das FBI Smartphones bereits seit Jahren mit der Zielstellung der "Durchleuchtung der Gesellschaft" trackt. Muslimische 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* <sup>22</sup>.

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

<sup>21</sup> <http://www.heise.de/tr/artikel/Immer-im-Visier-276659.html>

<sup>22</sup> <http://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims>

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.

- 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.<sup>23</sup>

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 Sicherheit<sup>24</sup>, 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.

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.

<sup>23</sup> <http://www.apple.com/chde/legal/privacy/>

<sup>24</sup> <http://heise.de/-2257924>



Abbildung 2.5: Lokalisierung eines Smartphones durch Facebook

### Nichts zu verbergen?

Wer ein praktisches Beispiel braucht: Einer Kanadierin wurde das Krankengeld gestrichen, weil sie auf Facebook fröhliche Urlaubsfotos veröffentlichte. Die junge Frau war wegen Depressionen krank geschrieben und folgte dem Rat ihres Arztes, einmal Urlaub zu machen und Zusammenkünfte mit Freunden zu suchen. Die Krankenkasse nutzte keine technischen Geo-Informationen sondern stellte visuell durch Beobachtung des Facebook-Profiles den Aufenthaltsort fest. Aber das Beispiel zeigt, dass die automatisierte Auswertung Konsequenzen haben könnte.<sup>25</sup>

Einen ähnlichen Fall gab es 2012 in Österreich. Aufgrund der bei Facebook veröffentlichten Fotos von einem Diskobesuch wurde gegen eine Linzer Kellerin Klage wegen Krankenstandsmissbrauch erhoben.<sup>26</sup>

## 2.5 Kommunikationsanalyse

Geheimdienste verwenden seit Jahren die Kommunikations-Analyse (wer mit wem kommuniziert), um die Struktur von Organisationen aufzudecken.

*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.

<sup>25</sup> <http://www.magnus.de/news/krankengeld-gestrichen-wegen-verfaenglichen-facebook-bildern-208271.html>

<sup>26</sup> [http://www.unwatched.org/20120601\\_Unachtsamer\\_Umgang\\_mit\\_Facebook\\_kann\\_unangenehme\\_Folgen\\_haben](http://www.unwatched.org/20120601_Unachtsamer_Umgang_mit_Facebook_kann_unangenehme_Folgen_haben)

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.

### 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.

Die Freundschaftsbeziehungen in sozialen Netzen wie Facebook oder ...VZ werden analysiert. Ehemalige Studenten des MIT demonstrierten mit *Gaydar - die Schwulenfalle*, wie man homosexuelle Orientierung einer Person anhand ihrer Freundschaftsbeziehungen erkennt. Twitter bietet einen 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. In diesen Communitys wird die Position einzelner Mitglieder analysiert, um die Meinungsmacher zu finden.

Gegenwärtig ist die Analyse von Gruppen Gegenstand intensiver Forschung (sowohl im zivilen wie auch geheimdienstlichen Bereich). Die TU Berlin hat zusammen mit der Wirtschaftsuniversität Wien erfolgversprechende Ergebnisse zur *Rasterfahndung nach Meinungsmachern* veröffentlicht. Die EU hat mit *INDECT* ein ambitioniertes Forschungsprojekt gestartet, um das Web 2.0 für die Dienste zu erschließen und direkt mit der ständig erweiterten Video-Überwachung zu verbinden.

### 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 2.6). Dabei wird nicht nur die Anzahl der Kommunikationsprozesse ausgewertet, es wird auch die zeitliche Korrelation einbezogen.

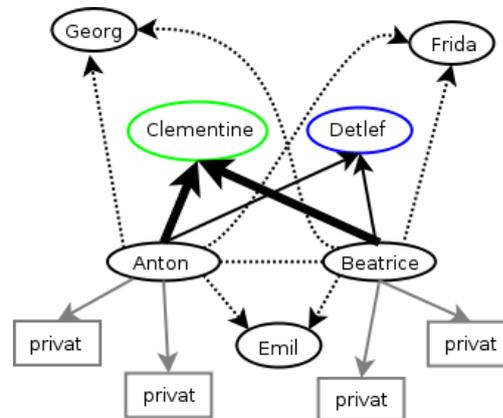


Abbildung 2.6: Soziales Netz von Anton und Beatrice

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

### 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 2.8 mit den Rohdaten erstellt.

Etwas besser aufbereitete Daten visualisiert Bild 2.9 mit den Kommunikationsdaten einer Woche von Ton Siedsmas.

Wenn man auch die Standortdaten des Smartphone mit auswerten kann, werden die Informationen deutlich detaillierter. Bild 2.10 zeigt einen Tag von Ton Siedsmas.

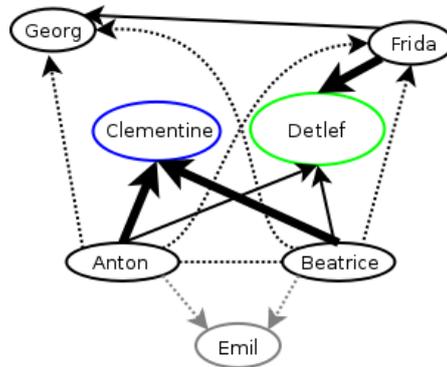


Abbildung 2.7: Präzisierte Struktur der "mg"

Analystools wie *i2 Analyst's Notebook* von IBM oder *rola rsCASE* können diese Daten sehr schön aufbereiten und die Schlapphüte bei der Analyse effektiv unterstützen (Bild 2.11).

## 2.6 Überwachungen im Internet

Unter <http://www.daten-speicherung.de/index.php/ueberwachungsgesetze> findet man eine umfassende Übersicht zu verschiedenen Sicherheits-Gesetzen der letzten Jahre. Neben einer Auflistung der Gesetze wird auch dargestellt, welche Parteien des Bundestages dafür und welche Parteien dagegen gestimmt haben. 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, denn **Du bist Terrorist!**<sup>27</sup>

**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. 1997 wurde die VDS aufgrund verfassungsrechtlicher Bedenken abgelehnt, 2002 wurde ein ähnlicher Gesetzentwurf vom Deutschen Bundestag abgelehnt und die Bundesregierung beauftragt, gegen einen entsprechenden Rahmenbeschluß auf EU-Ebene zu stimmen (siehe Bundestag-Drucksache 14/9801). Der Wissenschaftliche Dienst des Bundestages hat bereits 2006 ein Rechtsgutachten mit schweren Bedenken gegen die VDS vorgelegt.

<sup>27</sup> <http://www.dubistterrorist.de>

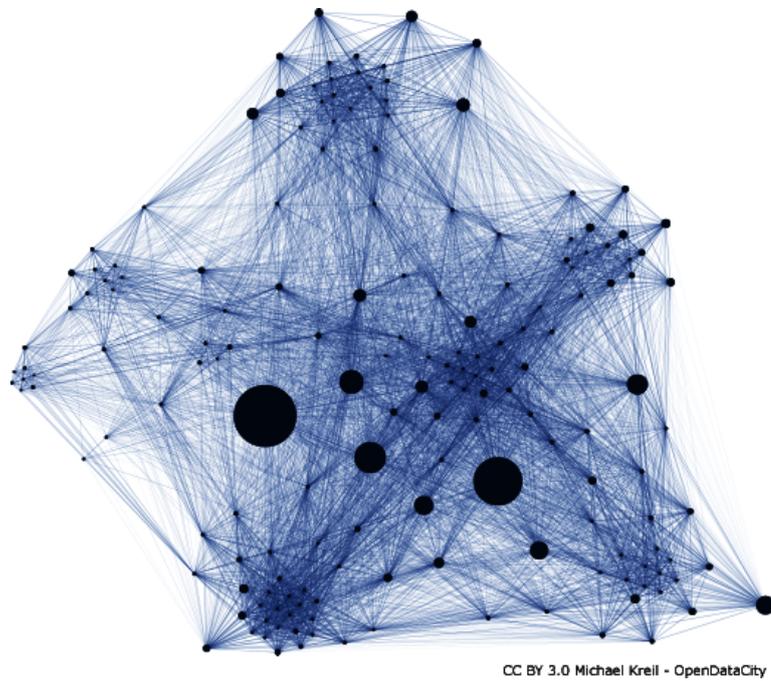


Abbildung 2.8: Kommunikationsnetzwerk von Malte Spitz

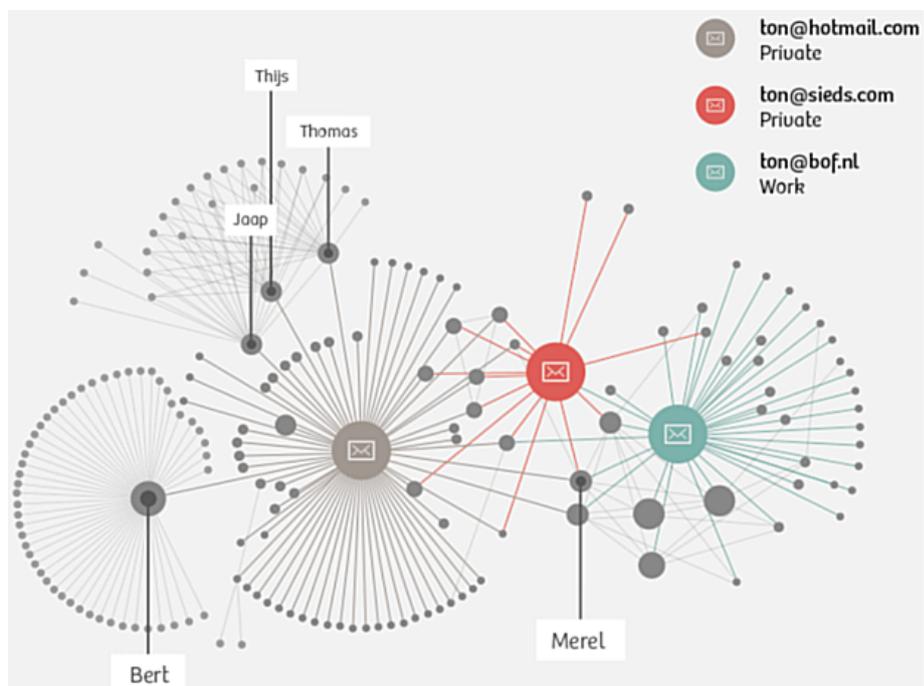


Abbildung 2.9: Aufbereitete Kommunikationsdaten von Ton Siedsmas

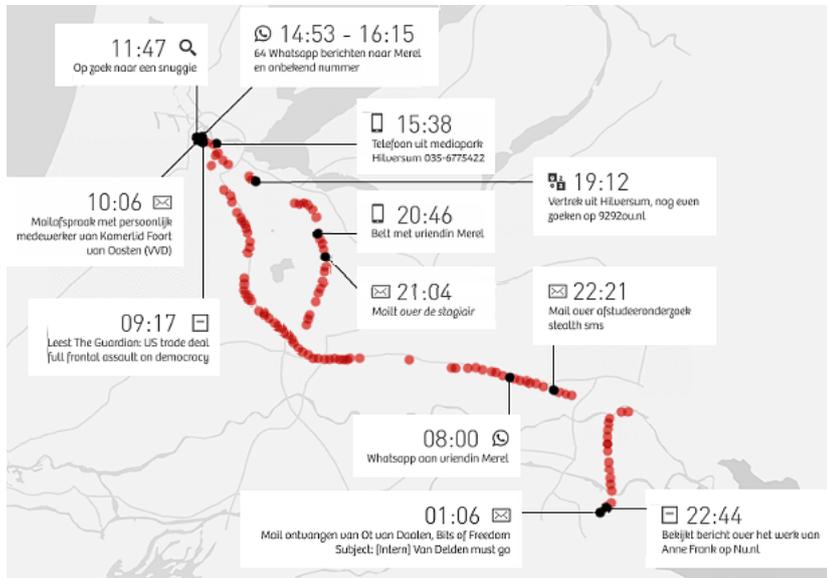


Abbildung 2.10: Standortdaten eines Tages von T. Siedsmas

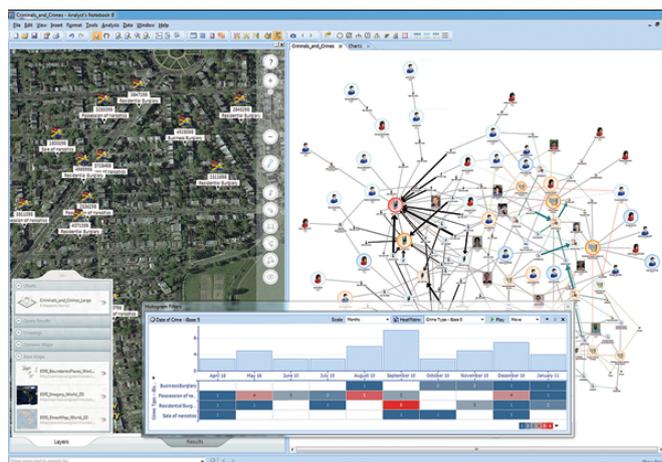


Abbildung 2.11: Screenshot von i2 Analyst's Notebook (IBM)

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.

|                            | 2007<br>(o. VDS) | 2008<br>(o. VDS) | 2009<br>(mit VDS) | 2010<br>(o. VDS) |
|----------------------------|------------------|------------------|-------------------|------------------|
| Straftaten im Internet     | 179.026          | 167.451          | 206.909           | 223.642          |
| Aufklärungsrate (Internet) | 82.9%            | 79.8%            | 75.7%             | 72,3%            |

Eine umfangreiche wissenschaftliche Analyse des Max-Planck-Instituts (MPI) für ausländisches und internationales Strafrecht belegt, 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 der Presse immer wieder herangezogenen Einzelbeispiele halten einer wissenschaftlichen Analyse nicht stand.

In einem offenen Brief sprachen sich Richter und Staatsanwälte gegen die VDS aus und widersprechen ebenfalls der Notwendigkeit für die Kriminalitätsbekämpfung.

**Bestandsdatenauskunft** Der IT-Sicherheitsforscher Pete Swire hat im April 2012 ein Paper <sup>28</sup> 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 möglichst gering sein.

Mit der Reform der Telekommunikationsüberwachung im Dezember 2012 kommt der Gesetzgeber den Wünschen der Geheimdienste weit entgegen. Ohne richterliche Prüfung dürfen die *Dienste* die sogenannten Bestandsdaten abfragen. Die Cloud-Provider und Mail-Provider sollen automatisiert nutzbare Schnittstellen dafür bereitstellen. Zu den Bestandsdaten zählen seit Dezember 2012 neben Name und Anschrift auch:

- 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.*

<sup>28</sup> [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2038871](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038871)

**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 Websites empfindlich ausgetrocknet werden kann. Die Aussagen wurden geprüft und für falsch befunden<sup>29</sup>.

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 Websites zu sperren, die vom BKA ohne nennenswerte Kontrolle erstellt werden sollte.
2. In der zweiten Stufe wurde am 18.06.09 das *Zugangsschwernisgesetz* 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<sup>30</sup>.
5. Die Auswertung des eco Verband zeigt, dass Webseiten mit dokumentiertem Missbrauch effektiv gelöscht werden können. 2010 wurden 99,4% der gemeldeten Webseiten gelöscht<sup>31</sup>. 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 Maffia 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<sup>32</sup>. Auch eine Abschätzung der EU-Kommision kommt zu

<sup>29</sup> <http://blog.odem.org/2009/05/quellenanalyse.html>

<sup>30</sup> <http://ak-zensur.de/2010/08/kapitulation.html>

<sup>31</sup> [http://www.eco.de/verband/202\\_8727.htm](http://www.eco.de/verband/202_8727.htm)

<sup>32</sup> [http://netzpolitik.org/wp-upload/bundestag\\_filter-gutachten.pdf](http://netzpolitik.org/wp-upload/bundestag_filter-gutachten.pdf)

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* <sup>33</sup>.

**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).

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 Verdächtigten zu wohnen oder möglicherweise in Kontakt mit ihm zu stehen.

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

**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.)

<sup>33</sup> <http://www.berlinonline.de/berliner-zeitung/print/politik/725127.html>

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

### Der Elektronische Polizeistaat

*Würde man noch den Mut haben, gegen die Regierung zu opponieren, wenn diese Einblick in jede Email, in jede besuchte Porno-Website, jeden Telefonanruf und jede Überweisung hat?*

Was unterscheidet einen elektronischen Polizeistaat von einer Diktatur? Gibt es dort auch eine Geheime Bundespolizei, die Leute nachts aus der Wohnung holt und abtransportiert, ohne juristischen Verfahren einsperrt...

Ein elektronischer Polizeistaat arbeitet sauberer. Es werden elektronische Technologien genutzt um forensische Beweise gegen BürgerInnen aufzuzeichnen, zu organisieren, zu suchen und zu verteilen. Die Informationen werden unbemerkt und umfassend gesammelt, um sie bei Bedarf für ein juristisches Verfahren als Beweise aufzubereiten.

Bei einem Vergleich von 52 Staaten hinsichtlich des Ausbaus des elektronischen Polizeistaat hat Deutschland einen beachtlichen 10 Platz belegt. Es verwundert nicht, dass an erster Stelle China und Nordkorea, gefolgt von Weißrussland und Russland stehen. Dann aber wird bereits Großbritannien aufgelistet, gefolgt von den USA, Singapur, Israel, Frankreich und Deutschland.

*Noch sei der Polizeistaat nicht umfassend realisiert, "aber alle Fundamente sind gelegt". Es sei schon zu spät, dies zu verhindern. Mit dem Bericht wolle man die Menschen darauf aufmerksam machen, dass ihre Freiheit bedroht ist.*

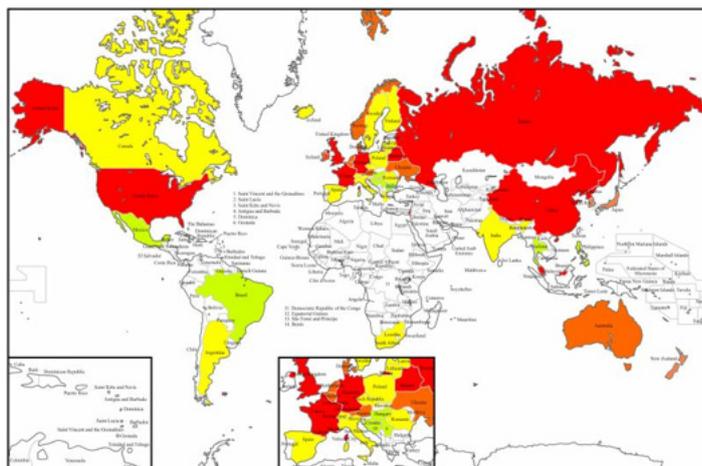


Abbildung 2.12: Vergleich der elektronischen Polizeistaaten

Das dieser Polizeistaat bereits arbeitsfähig ist, zeigt die Affäre Jörg Tauss. Ein unbequemer Politiker mit viel zu engen Kontakten zum CCC, der Datenschutz ernst nimmt, gegen das BKA-Gesetz und gegen Zensur auftritt, wird wenige Monate vor der Wahl des Konsums von KiPo verdächtigt. Die Medien stürzen sich auf das Thema. Innerhalb kurzer Zeit war Tauss als Politiker von der Springer-Presse demontiert, unabhängig von der später folgenden Verurteilung.

Ähnliche Meldungen hatten in den letzten Jahren viel weniger Resonanz:

1. *Auf dem Dienstcomputer eines hochrangigen Mitglieds des hessischen Innenministeriums sind vermutlich Kinderpornos entdeckt worden.* (25.07.2007)
2. *Kinderpornos: CDU-Politiker unter Verdacht* (01.04.2005)
3. *Der CDU-Politiker Andreas Zwickl aus Neckarsulm ist wegen Verdachts des Besitzes von Kinderpronografie...* (05.03.2009)

## 2.7 NSA & Co.

In den 1970er Jahren wurde durch einen Whistleblower ein gigantischer Überwachungsskandal von NSA, CIA und FBI aufgedeckt. Die Medien berichteten, dass die NSA über Jahre routinemäßig den kompletten Nachrichtenverkehr von und nach den USA überwachten. Die NSA verfügte bereits damals über *außerordentliche Fähigkeiten zur Telekommunikationsüberwachung*. Die wichtigsten amerikanischen Fernmeldegesellschaften lieferten auf Basis eines Abkommens mit der NSA illegaler Weise täglich Kopien aller in den USA abgesandten oder empfangenen Telegramme an den Geheimdienst.

Der parlamentarische Untersuchungsausschuss zur Aufklärung dieser Überwachungspraktiken kam 1976 zu dem Ergebnis:

*Die Regierung hat vielfach Bürger nur wegen ihrer politischen Überzeugung heimlich überwacht, auch wenn auf Grund dieser Überzeugungen weder Gewalt noch illegale Handlungen zu befürchten waren. [...] Ermittlungen gegen Gruppen, die als potenziell gefährlich eingestuft wurden und Gruppen, die mit potenziell gefährlichen Organisationen zusammengearbeitet hatten, wurden über Jahrzehnte fortgesetzt, obwohl diese nicht in rechtswidrige Aktivitäten verwickelt waren.*

Auch damals versuchten Verantwortliche, eine Begrenzung der Überwachung mit allen Mitteln zu verhindern. Eine Einschränkung der Überwachung gefährde die vitalen Interessen der USA. Trotzdem verabschiedete der Kongress 1978 den Foreign Intelligence Surveillance Act (FISA), um die ausufernde Überwachung etwas zu begrenzen. Ein Geheimgericht sollte für die Genehmigung von Überwachungsmaßnahmen gegen Amerikaner zuständig sein. Eine Begrenzung der Überwachung gegenüber Ausländern war ausdrücklich nicht vorgesehen.

Die FISA-Regeln wurden in der Folgezeit immer weiter aufgeweicht, insbesondere nach 9/11 durch den Patriot Act (2001) und den FISA-Amendments

Act (2008). Gemäß den aktuellen Auslegungen darf die NSA von den Telekommunikationsanbietern und Internetfirmen die Übermittlung kompletter Datenbanken verlangen, um darin selbst nach Einzelfällen zu suchen.

### 2013 ein Déjà-vu

Der von Snowden/Greenwald aufgedeckte Überwachungsskandal und die Beteiligung deutscher Geheimdienste als *second level partner* macht mich sprachlos. Man könnte viele Seiten füllen mit kurzen technischen Zusammenfassungen zu PRISM, QUANTUM, TAO, XKeyScore, ANT, BULLRUN, STORMBREW usw. Das würde nur zu folgender Schlussfolgerung führen:

#### **Diese Geheimdienste agieren außerhalb jeder Kontrolle.**

Besonders befremdlich ist für mich die Reaktion der deutschen Regierung. Als Konsequenz aus den Veröffentlichungen werden für den eigenen Gebrauch abhörsichere Crypto-Handys im Wert von 24 Mio. Euro bestellt. Der Bevölkerung gegenüber wird der NSA-Skandal ohne sichtbare Konsequenzen für beendet erklärt und ein Innenminister verkündet, dass sich jeder gefälligst selbst um die Sicherheit seiner Daten und privaten Kommunikation kümmern soll.

## 2.8 Rechtsstaatliche Grundlagen

*Es ist erkennbar, wohin die Reise gehen soll. Die Räder rollen bereits.  
Es wird Zeit, ein neues Ziel zu buchen, bevor der Zug abgefahren ist.*

Die Kriminalisierung der Protestler gegen den G8-Gipfel in Heiligendamm als Terroristen, die Diskussion um die weiträumige Funkzellenauswertung anlässlich der Anti-Nazi-Demo in Dresden 2011, das Gutachten des Bundesdatenschutzbeauftragten zum *Staatstrojaner* und die Beteiligung deutscher Geheimdienste an den weltweiten Überwachungsprogrammen der NSA/GCHQ zeigen deutlich die gesellschaftlichen Defizite bei der Begrenzung der Überwachung.

Der teilweise erfolgreiche Widerstand der Zivilgesellschaft gegen Vorratsdatenspeicherung, Zugangerschwernisgesetz, Online Durchsuchung, Großer Lauschangriff usw. reicht nicht aus. Die gesellschaftlich ausgehandelten Normen (Gesetze, Urteile des BVerfG...) zur Begrenzung der Überwachung werden nicht respektiert und anscheinend systematisch und ohne Konsequenzen für die Verantwortlichen missachtet.

### Gedanken für eine Gegenstrategie

1. Die Einhaltung der Normen für Polizei und Geheimdienste, die in einer demokratischen Diskussion ausgehandelt und als Gesetze bzw. Urteile des BVerfG niedergeschrieben sind, muss besser kontrolliert werden. Eine optionale Kontrolle ist unbrauchbar.

Auf der Veranstaltung *Soziale Bewegungen im Digitalen Tsunami* hat Dr. Thilo Weichert (ULD) die Situation aus Sicht des Datenschutz treffend beschrieben:

*Die Polizeibehörden fragen uns nur, wenn sie wissen, dass wir unser o.k. geben.*

2. Verstöße der Strafverfolger gegen geltendes Recht müssen geahndet werden, so wie es bei Verstößen gegen Gesetze auf anderen Gebieten üblich ist. Bisher agieren Strafverfolger anscheinend in einem "rechtsfreien Raum". Übertretungen der zulässigen Grenzen haben keine oder (bei starkem öffentlichen Druck) nur harmlose Konsequenzen.
3. Strafrechtliche Konsequenzen für die durch Snowden aufgedeckte geheimdienstliche Bespitzelung auf internationaler und europäischer Ebene, Strafverfolgung aller Mitwisser, Täter und Profiteure in Justiz und Exekutive und aller Amtsträger in Deutschland, deren Aufgabe es gewesen wäre, uns vor ausländischer Spionage zu schützen.
4. Die Besetzung der Posten von Entscheidungsträgern bei Polizei und Geheimdiensten sollte mit Personen erfolgen, die sich dem ausgehandelten Konsens verpflichtet fühlen. Wenn der neue Polizeipräsident von Dresden die weiträumige Funkzellenüberwachung in Dresden für richtig hält und in einer ähnlichen Situation wieder zu diesem Mittel greifen will, obwohl es für rechtswidrig erklärt wurde, dann ist er für die Aufgabe ungeeignet.

Udo Vetter stellt im lawblog die Frage:

*Wurde hier bewusst auf dem Rechtsstaat rumgetrampelt - oder sind die Verantwortlichen einfach so doof?*

5. 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 <sup>34</sup>
- Razzien im Vorfeld des G8-Gipfels waren rechtswidrig <sup>35</sup>
- Konstruieren und Schnüffeln mit §129a <sup>36</sup>
- Durchsuchungen beim LabourNet waren rechtswidrig <sup>37</sup>

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

<sup>34</sup> <http://de.indymedia.org/2008/10/228421.shtml>

<sup>35</sup> <http://www.ag-friedensforschung.de/themen/Globalisierung/g8-2007/bgh.html>

<sup>36</sup> <http://www.neues-deutschland.de/artikel/175230.konstruieren-und-schnueffeln-mit-s-129a.html>

<sup>37</sup> <http://www.labournet.de/ueberuns/beschlagnahme/index.html>

## 2.9 Bundesamt für Verfassungsschutz auflösen

Es wird Zeit, das Bundesamt für Verfassungsschutz aufzulösen. Seine Aufgabe als Bollwerk gegen die drohende Infiltration feindlicher Agenten aus der Sowjetunion oder der DDR besteht nicht mehr. Anti-Spionage und Anti-Terror Einsätze sowie Bekämpfung der Korruption und Verfolgung von Sachbeschädigungen sind Aufgabe von Polizei/BKA.

Die Humanistische Union fordert seit Jahren die Auflösung des BfV<sup>38</sup>. Die PiratenPartei Thüringen forderte im Beschluss des Parteitages im Nov. 2011 eine Auflösung des Thüringer Verfassungsschutzes<sup>39</sup> (wenige Tage bevor der NSU-Skandal bekannt wurde) und kritisiert die Übernahme der Strukturen in das Innenministerium. Die Linke in Hessen plädiert für die Auflösung des Verfassungsschutzes<sup>40</sup> und möchte statt dessen eine Informations- und Dokumentationsstelle einrichten für Bestrebungen gegen die Verfassung (ohne V-Leute und ohne geheimdienstliche Kompetenzen). Als Konsequenz aus dem NSA-Skandal forderte der Chaos Computer Club die Auflösung des BfV zur Wiedereinführung von Grundrechten und Rechtsstaatlichkeit<sup>41</sup>.

### V-Leute sind keine Lösung, sondern das Problem

- V-Leute des Verfassungsschutzes hatten erheblichen Anteil an der Radikalisierung der Studentenbewegung 1968. Vor allem der V-Mann Peter Urbach wird immer wieder als Agent Provocateur genannt, der auch Waffen und Molotow-Cocktails lieferte und nach seiner Enttarnung vom Verfassungsschutz ins Ausland gebracht wurde.<sup>42</sup>
- Die Verflechtungen von Verfassungsschutz und RAF sind noch immer nicht aufgeklärt. Aus alten Unterlagen der Stasi geht hervor, dass Verena Becker vom Verfassungsschutz "kontrolliert wurde". V. Becker spielte eine wesentliche Rolle beim Mord an Generalbundesanwalt Buback.<sup>43</sup>
- Der Verfassungsschutz hat die rechtsradikale Szene nicht unterwandert, sondern finanziell unterstützt und vor Strafverfolgung geschützt.
  - Laut einem BKA-Report<sup>44</sup> von 1997 soll der Verfassungsschutz rechtsradikale Neonazis systematisch geschützt haben. Die Vorwürfe werden mit konkreten Fällen untermauert. V-Leute wurden vor Durchsuchungen gewarnt und einer Straftat überführte Nazis wurden nicht angeklagt und verurteilt, wenn sie als V-Leute arbeiteten. Informationen wurden zu spät an die Polizei weitergeleitet, so dass rechtsradikale Aktionen nicht mehr verhindert werden konnten.

<sup>38</sup> [http://www.humanistische-union.de/fileadmin/hu\\_upload/doku/publik/huschrift17.pdf](http://www.humanistische-union.de/fileadmin/hu_upload/doku/publik/huschrift17.pdf)

<sup>39</sup> <http://www.piraten-thueringen.de/2012/10/verfassungsschutz-aufloesen-statt-umbetten/>

<sup>40</sup> <http://www.fr-online.de/rhein-main/hessen-linke-will-verfassungsschutz-aufloesen,1472796,17278430.html>

<sup>41</sup> <https://www.ccc.de/de/updates/2013/demonstration-wiedereinfuehrung-rechtsstaatlichkeit>

<sup>42</sup> <http://www.heise.de/tp/blogs/8/151641>

<sup>43</sup> <http://www.heise.de/tp/artikel/31/31120/1.html>

<sup>44</sup> <http://www.spiegel.de/panorama/justiz/verfassungsschutz-soll-rechte-v-leute-vor-straefverfolgung-geschuetzt-haben-a-865154.html>

- Bereits 2002 hat das LKA Sachsen-Anhalt dem Verfassungsschutz misstraut und aus *ermittlungstaktischen Gründen* nicht über Exekutivmaßnahmen in der rechten Szene informiert. Aus einem Vermerk des Bundesinnenministeriums:<sup>45</sup>

*Nach Rücksprache (...) stützen sich die "ermittlungstaktischen Gründe" vermutlich auf die Befürchtung, die Verfassungsschutzbehörden würden ihre Quellen über bevorstehende Exekutivmaßnahmen informieren.*

- 2008 wurden Ermittlungen gegen den Neonazi Sebastian Seemann eingestellt. Er baute das verbotene *Blood and Honour* Netzwerk auf und war im schwerkriminellen Milieu aktiv (Drogen- und Waffenhandel). Der Verfassungsschutz warnte ihn vor Exekutivmaßnahmen. Mitarbeiter des Verfassungsschutzes wurden daraufhin wegen Geheimnisverrats und Strafvereitelung im Amt angeklagt. Auf Veranlassung des Innenministers Dr. Ingo Wolff wurden die Anklagen eingestellt.<sup>46</sup>

Das ist seit mehreren Jahren bekannt. Konsequenzen? Nur die Landesregierung in Thüringen unter Führung von B. Ramelow (Linke) geht den entgegengesetzten Weg und schafft die V-Leute des BfV ab, weil das V-Leute-System nicht die Sicherheit erhöht, sondern die Demokratie gefährdet.<sup>47</sup> Der Bundesinnenminister möchte die Strafheit für staatlichen Spitzel erweitern, damit sie stärker an szenetypischen Aktionen teilnehmen können (z.B Brandanschläge auf Unterkünfte für Asylbewerber u.ä.)

### Strategie der Spannung

*Geheimdienste ... sind nach wie vor die große Unbekannte in der Entstehung und Entwicklung des Terrorismus, des bundesdeutschen ebenso wie des mit ihm verflochtenen internationalen Terrorismus. (W. Kraushaar)*

Viele Terrorgruppen in Deutschland wurden von V-Leuten des Verfassungsschutzes aufgebaut. Strafrechtliche Konsequenzen haben diese Terroristen nicht zu befürchten, wir sollten aber die sich daraus ergebende Beeinflussung der Gesetzgebung fürchten:

- Der V-Mann Melvüt Kar hat drei Terrorzellen aufgebaut und an die Behörden verraten. Melvüt Kar wurde in Deutschland nie angeklagt und lebt unbehelligt in Istanbul in der Türkei.<sup>48</sup>
  - Die erste Terrorzelle mit Mutlu A., Mohamed El-A. und Issam El-S wurde am 17. Februar 2003 von der GSG9 verhaftet und am gleichen Tag aus Mangel an Beweisen wieder freigelassen.
  - Die Verhaftung der zweiten Terrorzelle mit Dzavid B., Nedzad B., Ahmed H., Bekim T. und Blerim T. wurde von den Medien weitgehend ignoriert.

<sup>45</sup> <https://www.taz.de/Neonazi-Ermittlungen/!103340/>

<sup>46</sup> <http://www.nadir.org/nadir/initiativ/azoncao/donazi3.html>

<sup>47</sup> <http://www.taz.de/Verfassungsschutz-in-Thueringen/!156778/>

<sup>48</sup> <http://www.heise.de/tp/artikel/35/35986/1.html>

- Der größte Coup von Mevlüt Kar war die Sauerländer Terrorzelle, die von ihm für die Vorbereitung gigantischer Terroranschläge mit Sprengzündern usw. versorgt wurde

Melvüt Kar soll vom Verfassungsschutz nie aktiv zur Gründung von Terrorgruppen gedrängt worden sein. Er soll selbstständig gehandelt haben, um seinen Wert als V-Mann und damit seine Bezahlung zu verbessern. Das BfV hat das Treiben toleriert und gedeckt und vor allem die Sauerland Terrorzelle medial für die Schaffung einer Atmosphäre der Spannung (Terrorgefahr!) genutzt.

- Ein weiterer V-Mann des Verfassungsschutzes in der islamistischen Szene war Yehia Yousif, der mittlerweile in Saudi-Arabien lebt und auch eine Schlüsselrolle in der Radikalisierung der Sauerland Gruppe spielte. Yousif hat wesentlich zum Erstarren salafistischer Gruppen in Deutschland beigetragen.<sup>49</sup>
- Die *Globale Islamische Medienfront* (GIMF) drohte 2007 in Videos mit Terroranschlägen in Deutschland. Im Gerichtsverfahren gegen Mitglieder der GIMF kam heraus, dass der Anführer dieser Gruppe ein V-Mann des Verfassungsschutzes war. Irfan Peci soll monatlich 2.500 - 3.000 Euro vom Verfassungsschutz erhalten haben. Außerdem finanzierte das BfV die Ausbildung an Waffen in einem Terrorcamp in Bosnien und deckte Straftaten von Peci. Gegen den V-Mann wurde ebenfalls keine Anklage erhoben.<sup>50</sup>

Im Gegensatz zu M. Kar wurde I. Peci aktiv vom Verfassungsschutz geführt und hat seine Terrorgruppe unter Anleitung des BfV aufgebaut.

Ohne die zweifelhafte Rolle der V-Leute würden wir ruhiger leben und viele Sicherheitsgesetze wären nicht durchsetzbar gewesen.

### Schutz gegen Wirtschaftsspionage???

Der Verfassungsschutz warnt gelegentlich vor Wirtschaftsspionage aus Russland und China. Das ist wenig originell, dafür brauchen wir keinen Geheimdienst. Gegenüber unseren westlichen Verbündeten, insbesondere gegenüber der US-amerikanischen Wirtschaftsspionage gegen deutsche Unternehmen, stellt man sich blind. Verfassungsschutzpräsident Maaßen ließ sich im Rahmen des NSA-Skandal zu folgendem Statement hinreißen:

*Tatsächlich wurde bis zum heutigen Tage in ganz Europa kein einziger Fall amerikanischer oder britischer Wirtschaftsspionage nachgewiesen.*<sup>51</sup>

Ein anonymen Mitarbeiter des Verfassungsschutzes sagte dagegen bereits 1998 in der Sendung PlusMinus des WDR:

*Mir sind über 50 solcher Fälle von Wirtschaftsspionage bekannt. Wenn wir auf solche Aktivitäten stoßen, werden wir von unseren Vorgesetzten zurückgepiffen. Wir dürfen unsere Erkenntnisse meist weder an den*

<sup>49</sup> <http://www.heise.de/tp/blogs/8/150854>

<sup>50</sup> <http://www.heise.de/tp/blogs/8/150854>

<sup>51</sup> <http://heise.de/-1943975>

*Staatsanwalt noch an die betroffenen Firmen weitergeben. Aus Rücksicht auf unsere Verbündeten.*<sup>52</sup>

Den spektakulären Fall Enercon<sup>53</sup> findet man leicht, wenn man bei einer Suchmaschine der Wahl die passenden Suchbegriffe nach Wirtschaftsspionage der NSA in Deutschland eingibt, für Hr. Maaßen ist das wohl zuviel verlangt.

Auch dem BND waren die Ambitionen der NSA zur Wirtschaftsspionage seit Jahren bekannt, wie der Ex-General D. Urmann vor dem Untersuchungsausschuss des Bundestages erklärte.<sup>54</sup> Verfassungsschutzpräsident Maaßen wurde nicht darüber informiert? Schwer vorstellbar.

### NSU-Skandal

Der NSU-Skandal gilt als der größte Geheimdienstskandal der BRD. 10 Jahre zog ein rechtsradikales Trio mordend durch Deutschland. Der Verfassungsschutz erhielt viele Hinweise von V-Leuten, die nicht an die Polizei weitergegeben wurden. Nach Schätzungen waren bis zu 25 V-Leute des BfV in der Umgebung des NSU tätig. Die genaue Zahl ist nicht rekonstruierbar. Die meisten Akten über den NSU und über Tarnfirmen des BfV im rechtsradikalen Milieu wurden vernichtet, als das BKA die Ermittlungen übernahm. Sieben Zeugen aus dem Umfeld des NSU sind überraschend verstorben, bevor man ihre Aussagen aufnehmen konnte.

- Der V-Mann Florian H.<sup>55</sup> verbrannte beispielsweise in seinem Auto wenige Stunden bevor das BKA ihn als Zeuge vernehmen wollte. Die Polizei diagnostizierte Selbstmord aus Liebeskummer, obwohl seine Freundin nichts von Liebeskummer wusste und es keinen Abschiedsbrief gab. Die Familie des V-Manns erhebt schwere Vorwürfe wegen schlampiger Ermittlungen bei der Polizei.<sup>56</sup>
- Der wertvolle V-Mann Thomas R. lieferte dem BfV viele Informationen über den NSU. Vor Gericht verweigerte er die Aussage. Er starb überraschend an einem Zucker-Schock (Diagnose: nicht behandelte schwere Diabetis), bevor er in Beugehaft genommen werden konnte, um eine Aussage zu erzwingen.<sup>57</sup>

Welche Konsequenzen haben sich drei Jahre nach der Aufdeckung des NSU-Skandals für den Verfassungsschutz ergeben?

- 47 Mitarbeiter der Abteilung Rechtsextremismus wurden befördert. Drei Mitarbeiter, die direkt für die Aktenvernichtung verantwortlich waren, wurde auf andere Posten versetzt ohne dienstrechtliche oder strafrechtliche Konsequenzen.<sup>58</sup>

<sup>52</sup> <http://web.archive.org/web/20001208141100/http://www.wdr.de/tv/plusminus/archiv/980414/lauschangr.html>

<sup>53</sup> <https://de.wikipedia.org/wiki/Enercon>

<sup>54</sup> <http://heise.de/-2569294>

<sup>55</sup> <http://www.berliner-zeitung.de/nsu-prozess/nsu-prozess-wichtiger-zeuge-im-auto-verbrannt,11151296,24474928.html>

<sup>56</sup> <http://www.stuttgarter-zeitung.de/inhalt.nsu-untersuchungsausschuss-vorwuerfe-nach-ominoeser-selbsttoetung.a05cce3a-60a5-4d68-9b24-7a6693123002.html>

<sup>57</sup> <http://www.sueddeutsche.de/politik/nsu-prozess-tod-von-v-mann-corelli-wirft-fragen-auf-1.1940178>

<sup>58</sup> <http://www.taz.de/Verfassungsschutz-und-NSU/!150371/>

- Am 3. Jahrestag der Aufdeckung des NSU-Skandals besuchte Merkel offiziell das Bundesamt für Verfassungsschutz. Die Wahl dieses Datums für einen offiziellen Besuch ist ein politisches Statement.<sup>59</sup>
- Der Etat des Bundesamtes für Verfassungsschutz wurde um 21 Mio. Euro auf 231 Mio. Euro erhöht.<sup>60</sup>

### Aktive Rolle bei neuen Überwachungsgesetzen

Bei vielen Überwachungsgesetzen ist das BfV eine treibende Kraft. Geheimdienste sind zweifellos die Hauptnutznießer der vollständigen Protokollierung unseres Kommunikationsverhaltens.

Die Fernmeldeverkehr-Überwachungsverordnung (FÜV) wurde 1995 auf Initiative des Verfassungsschutzes beschlossen. Die Verordnung wurde 2002 durch die TKÜV ersetzt und verpflichtete Telekommunikationsanbieter zur Kooperation mit Strafverfolgung und Geheimdiensten.

Die Vorratsdatenspeicherung brachte 2009 so gut wie keine Verbesserungen bei der Aufklärung von Straftaten im Internet. Trotzdem forciert der Verfassungsschutz im Hintergrund weiterhin die Einführung der VDS (neudeutsch: Mindestspeicherfrist). Nachdem die VDS schon 2002 als nicht vereinbar mit der Verfassung vom Bundestag abgelehnt wurde und auf EU-Ebene offenbar nicht durchsetzbar ist, beteiligte sich der Verfassungsschutz 2012 aktiv an der Formulierung einer internationalen Richtlinie zur verpflichtenden Vorratsdatenspeicherung im Rahmen der UNODC, die allerdings ebenfalls nicht verbindlich umgesetzt wurde.<sup>61</sup>

### Zukünftige Schwerpunkte des Geheimdienstes

Das Bundesamt für Verfassungsschutz soll in den kommenden Jahren zu einer kleinen Mini-NSA werden. Die Kompetenzen und Fähigkeiten zur Überwachung im Internet soll massiv ausgebaut werden, wie Netzpolitik.org<sup>62</sup> anhand vertraulicher Unterlagen berichtete. Die neu zu schaffende Abteilung *Erweiterte Fachunterstützung Internet* (EFI, 75 neue Mitarbeiter) soll Soziale Netzwerke, Foren u.ä. automatisiert überwachen und dabei überwiegend unterhalb der Schwelle des G10-Gesetzes agieren, also ohne parlamentarische Kontrolle durch die G10-Kommision. Außerdem sollen neue Analysemethoden geschaffen werden, um anhand von Metadaten bessere Bewegungs- und Kommunikationsprofile zu erstellen.

Der Abgeordnete C. Ströbele bezeichnete die Aufgabenstellung für die Abteilung EFI als illegal und nicht mit der Verfassung vereinbar.<sup>63</sup>

<sup>59</sup> <http://www.heise.de/tp/news/Der-NSU-und-der-Verfassungsschutz-Dinge-von-gestern-2440935.html>

<sup>60</sup> [https://www.bundestag.de/dokumente/textarchiv/2014/kw48\\_ak\\_innere/341274](https://www.bundestag.de/dokumente/textarchiv/2014/kw48_ak_innere/341274)

<sup>61</sup> <https://netzpolitik.org/2012/uno-bericht-der-kampf-gegen-terroristen-beginnt-im-internet-mit-vorratsdatenspeicherung-und-identifizierungspflicht/>

<sup>62</sup> <https://netzpolitik.org/2015/geheime-referatsgruppe-wir-praesentieren-die-neue-verfassungsschutz-einheit-zum-ausbau-der-internet-ueberwachung/>

<sup>63</sup> <http://www.stroebele-online.de/bundestag/anfragen/8305504.html>

### Überwachung politischer Aktivisten

Der Verfassungsschutz entwickelt sich zu einem Geheimdienst zur Überwachung von politischen Aktivisten und unliebsamen Abgeordneten.

- R. Gössler: 38 Jahre zu Unrecht vom Verfassungsschutz überwacht <sup>64</sup>
- Verfassungsschutz in Bayern überwacht die linke Szene <sup>65</sup>
- Überwachung einer linken Gruppe durch Verfassungsschutz <sup>66</sup>
- Verfassungsschutz bespitzelt linke Abgeordnete <sup>67</sup>
- Gegner von Stuttgart21 vom Verfassungsschutz überwacht <sup>68</sup>
- Kultur- und Jugendprojekt Conne Island vom BfV überwacht <sup>69</sup>
- mg-Überwachung durch den Verfassungsschutz war illegal <sup>70</sup>
- Ohne demokratische Kontrolle (BfV in Bayern) <sup>71</sup>

## 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.

<sup>64</sup> <http://heise.de/-217246>

<sup>65</sup> <http://www.heise.de/tp/artikel/35/35942/1.html>

<sup>66</sup> <http://www.heise.de/tp/blogs/8/151499>

<sup>67</sup> <http://www.heise.de/tp/artikel/36/36316/1.html>

<sup>68</sup> <http://www.bei-abriss-aufstand.de/2012/02/25/>

<sup>69</sup> <http://www.bei-abriss-aufstand.de/2012/02/25/>

<sup>70</sup> <http://www.l-iz.de/Politik/Sachsen/2014/05/Verfassungsschutz-raeumt-Bespitzelung-von-Conne-ein-55195.html>

<sup>71</sup> <http://www.heise.de/tp/artikel/35/35942/1.html>

- Geheimdienste interessieren sich für die Erpressbarkeit von Target 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 Wusch 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.

### **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.<sup>72</sup>

### **Einzelbeispiele**

- Target 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 muss-

<sup>72</sup> <http://www.heise.de/tp/artikel/44/44538/1.html>

te der Vater kleinlaut zugegeben, dass seine Tochter wirklich schwanger war, er selbst aber nichts davon wusste.<sup>73</sup>

- Im Rahmen der Zulässigkeitsprüfung für Piloten wurde Herr J. Schreiber mit den vom Verfassungsschutz gesammelten Fakten konfrontiert<sup>74</sup>:
  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 einer Stellungnahme jedoch nicht eingeräumt.

- 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 sechs Jahren eine Psychotherapie durchführen musste und Drogenprobleme gehabt hätte.<sup>75</sup>
- 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 beziffern<sup>76</sup>.

Noch krasser ist das Ergebnis der *Operation Ore* in Großbritannien. 39 Menschen, zu Unrecht wegen Konsums von Kinderpornografie verurteilt, haben Selbstmord begangen, da ihnen alles genommen wurde<sup>77</sup>.

- "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 dient, weitere Sympathisanten zu identifizieren. Die Bundesanwaltschaft verteidigt die Maßnahme als legale Fahndungsmethode.

<sup>73</sup> <http://www.tagebau.com/?p=197>

<sup>74</sup> <http://www.pilotundflugzeug.de/artikel/2006-02-10/Spitzelstaat>

<sup>75</sup> <http://blog.kairaven.de/archives/998-Datenstigmaanekdote.html>

<sup>76</sup> <http://www.lawblog.de/index.php/archives/2008/03/11/>

<sup>77</sup> [http://en.wikipedia.org/wiki/Operation\\_Ore](http://en.wikipedia.org/wiki/Operation_Ore)

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”*<sup>78</sup> gibt es bei SPON.
2. Fahndung zur Abschreckung: In Vorbereitung des G8-Gipfels in Heiligendamm veranstaltete die Polizei am 9. Mai 2007 eine Großrazzia. Dabei wurden bei Globalisierungsgegnern Rechner, Server und Materialien beschlagnahmt. Die Infrastruktur zur Organisation der Proteste wurde nachhaltig geschädigt. Wenige Tage nach der Aktion wurde ein Peilsender des BKA am Auto eines Protestlers gefunden. Um die präventiven Maßnahmen zu rechtfertigen, wurden die Protestler als terroristische Vereinigung eingestuft. Das Netzwerk Attac konnte 1,5 Jahre später vor Gericht erreichen, dass diese Einstufung unrechtmäßig war. Das Ziel, die Organisation der Proteste zu behindern, wurde jedoch erreicht.
3. Dr. Rolf Gössner ist Rechtsanwalt, Vizepräsident der Internationalen Liga für Menschenrechte, Mitherausgeber des Grundrechte-Reports, Vizepräsident und Jury-Mitglied bei den Big Brother Awards. Er wurde vom Verfassungsschutz 38 Jahre lang überwacht. Obwohl das Verwaltungsgericht Köln bereits urteilte, dass der Verfassungsschutz für den gesamten Bespitzelungszeitraum Einblick in die Akten gewähren muss, wird dieses Urteil mit Hilfe der Regierung ignoriert. Es werden Sicherheitsinteressen vorgeschoben!

Mit dem Aufbau der “neuen Sicherheitsarchitektur” bedeutet eine Überwachung nicht nur, dass der direkt Betroffene überwacht wird. 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.

<sup>78</sup> <http://www.spiegel.de/politik/deutschland/0,1518,384374,00.html>

## Kapitel 3

# Digitales Aikido

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

- **Einsteiger:** Datensammler nutzen verschiedene Möglichkeiten, Informationen über die Nutzer zu generieren. Die Wiedererkennung des Surfers bei der Nutzung verschiedener Dienste kann mit einfachen Mitteln erschwert werden. Datensammler meiden und Alternativen nutzen, Cookies und JavaScript kontrollieren, Werbung filtern, SSL-verschlüsselte Verbindungen nutzen, E-Mail Client sicher konfigurieren...
- **1. Grad:** Persönliche Daten und Inhalte der Kommunikation werden verschlüsselt. Das verwehrt unbefugten Dritten, Kenntnis von persönlichen Daten zu erlangen. Festplatte und Backups verschlüsseln mit Truecrypt, dm-crypt oder FileVault, E-Mails verschlüsseln mit GnuPG oder S/MIME, Instant Messaging mit OTR...
- **2. Grad:** Anhand der IP-Adresse ist ein Nutzer eindeutig identifizierbar. Mixkaskaden (JonDonym) oder Onion Router (Tor) bieten eine dem realen Leben vergleichbare Anonymität. Remailer bieten die Möglichkeit, den Absender einer E-Mail zu verschleiern.
- **3. Grad:** Eine noch höhere Anonymität bietet Darknets wie z.B. das *Invisible Internet Projekt (I2P)* oder das *Freenet Projekt*. Eine dezentrale und vollständig 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.)

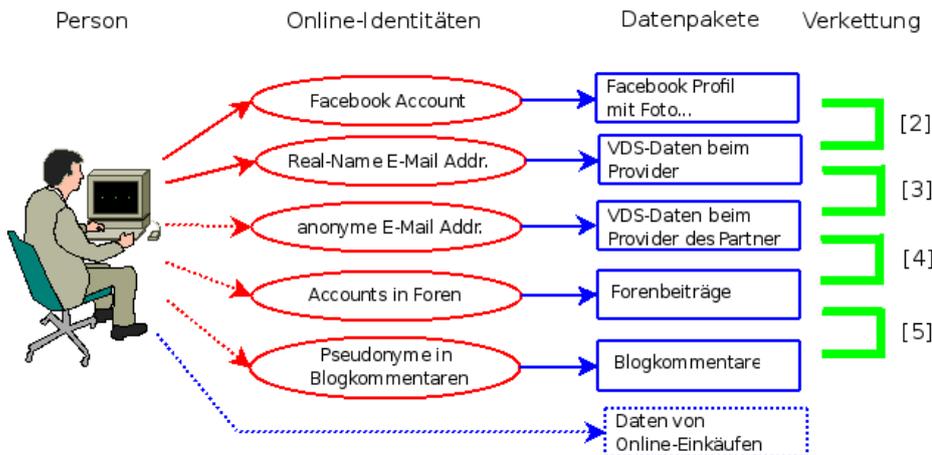


Abbildung 3.1: Datenverkettung

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.
- In Foren und Blogs findet man Postings und Kommentare, häufig mit den gleichen Pseudonymen, die auch für die E-Mail Adressen verwendet werden.
- Online-Einkäufe erfordern die Angaben zur Kontoverbindung und einer Lieferadresse, die der Person zugeordnet werden können.

### Verkettung der Informationen und Datenpäckchen

Die verschiedenen Datenpakete können auf vielfältige Art verknüpft werden. Diese Datenverkettung 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 <sup>1</sup>.
  - MIT-Studenten erkennen homosexuelle Neigungen ihrer Kommilitonen anhand der Informationen über Freundschaften in den Facebook-Profilen <sup>2</sup>.
  - Der Grünen-Vorsitzende Özdemir pflegte eine Freundschaft mit dem Intensivstraftäter Muhlis Ari, ist in seinem Facebook Profil erkennbar <sup>3</sup>.
2. Dem Facebook Profil kann man durch Kombination mit anderen Datenkrümeln den realen Namen und die meisten genutzten E-Mail Adressen zuordnen. Die Firma Rapleaf ist z.B. darauf spezialisiert. Auch pseudonyme Facebook Accounts können deanonymisiert werden.
3. Durch Analyse der im Rahmen der VDS gespeicherten IP-Adressen können bei zeitlicher Übereinstimmung beide E-Mail Adressen der gleichen Person zugeordnet werden. Ein einzelner passender Datensatz reicht aus. (Wenn nicht konsequent Anonymisierungsdienste für das anonyme Postfach verwendet werden.)

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

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

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

4. Die Verbindung zwischen anonymer E-Mail Adresse und Foren Account ergibt sich durch die Nutzung der E-Mail Adresse bei Anmeldung.
5. Durch Vergleiche von Aussagen und Wortwahl lassen sich Korrelationen zwischen verschiedenen 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 <sup>4</sup>)
  - Die Libris Shops (Zugang zu Bestellungen von 1000 Buchshops <sup>5</sup>)
  - Sparkassen-Shops (350.000 Rechnung online einsehbar <sup>6</sup>)
  - Acht Mio. Adressen von Quelle-Kunden sollen verkauft werden <sup>7</sup>

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.

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

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

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

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

- 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).
- 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 <sup>8</sup>.
- 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.<sup>9</sup>

### Ich habe doch nichts zu verbergen...

...oder habe ich nur zu wenig Fantasie, um mir die Möglichkeiten der Datensammler vorstellen, 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. Naheliegend ist es, die verschiedenen Netzwerke wie StudiVZ usw. nach F. abzusuchen. Bei Facebook wird

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

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

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 *Synchron-Saufen* im Internet. Scheinbar ist sie auch vereinsamt.
- F. ist offenbar lesbisch, sie sucht nach einer Frau bei abgefueckt.de.
- F. ist im linksradikalen Spektrum aktiv. Sie hat an mehreren Demonstrationen teilgenommen und berichtet über Erfahrungen mit Hausdurchsuchungen. Möglicherweise ist das die Ursache für ihre Angstzustände.
- Öffentlich prangert sie in einem Diskussionsforum die Firma ihres Vaters an (wegen Ausspionierens von Mitarbeitern).
- Ihre linksgerichtete Grundhaltung wird durch öffentliche Unterstützung der Kampagne *Laut ficken gegen Rechts* unterstrichen.
- Von regelmäßiger Arbeit hält sie nicht viel.
- Die angegebene Adresse ist falsch. F. wohnt in einer 11-Personen-WG in einem besetzten Haus in Alt-Moabit. Die WG sucht nach einem neuem Mitglied.
- Die Wunschliste bei Amazon und Fotos bei Flickr...

Würden sie als Personalchef diese fiktive Person einstellen?

Welche Ansatzpunkte ergäben sich für den Verfassungsschutz?

Was könnte zukünftig für die Krankenkasse interessant sein?

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

### 3.3 Schattenseiten der Anonymität

Auf den ersten Blick scheint Anonymität eine Lösung für fast alle beschriebenen Probleme zu sein. Anonymität verhindert das Tracking durch kommerzielle Datensammler, schützt die Privatsphäre vor neugierigen Blicken der Spammer, 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. Heute 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 heute jeder Hanswurst für beliebige Zwecke missbrauchen und die Bewegung diskreditieren.

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

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

Ein anonymer Schwarm vereinzelter Individuen kann sich zu einem Shits-torm 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.

Manchmal sind es nur Kleinigkeiten: Ich bekomme immer wieder kleine Nachrichten (Kommentare, Hinweise auf Programme und Blogartikel...) über mein Kontaktformular, dass eine unbeobachtete Kontaktaufnahme ermöglichen soll (auf Wunsch des Absenders auch anonym). So gut wie nie enthalten die Nachrichten einen Hinweis auf den Absender, alle wollen immer ganz doll anonym bleiben. Ein wiederkehrendes Pseudonym als Absender oder nur ein kleiner Strichcode wären für den Empfänger hilfreich, um den Inhalt zu bewerten. Wenn ich weiss, dass –/– meistens gute Hinweise/Kommentare gegeben hat, dann würde ich vielleicht nicht denken: *Och nö, heute nicht mehr*. Eine Antwortadresse (Spambog E-Mail, Jabber, POND) für Rückfragen oder Diskussionen erwarte ich eigentlich nicht mehr, es würde aber ein ernsthaftes Interesse an einer Diskussion andeuten.

(Das soll nur ein Denkanstoß sein. Es betrifft nicht nur mich. Wundert euch nicht, dass ihr als anonyme Nobodys behandelt werdet, wenn ihr anonyme Nobodys sein wollt.)

## Kapitel 4

# Spurenarm Surfen

Das auf den folgenden Seiten vorgestellte Konzept zum spurenarmen Surfen umfasst folgende Punkte:

1. Die Nutzung datensammelnder Webangebote kann man vermeiden.
2. Die Annahme von Cookies und die Ausführung von JavaScript wird auf vertrauenswürdige Webseiten eingeschränkt.
3. Werbung, HTML-Wanzen und die Like-Buttons (mit denen Social Networks wie Facebook Daten sammeln) werden durch Filter blockiert.
4. Verräterische Informationen des Browsers werden manipuliert oder beseitigt.
5. Risikoreiche und Privacy-unfreundliche Features wie PDF-Reader Plugins, Browser History, Geolocation, WebRTC usw. werden im Browser deaktiviert.
6. Die Sicherheit von HTTPS-Verbindungen wird durch zusätzliche Überprüfungen und Anzeigen verbessert. Unsichere Cipher werden deaktiviert, um vertrauenswürdige Verschlüsselung nach dem Stand der zivilen Forschung sicherzustellen.

Mit diesen Maßnahmen kann es vorkommen, dass Websites nicht wie erwartet funktionieren. Gute Webdesigner verzichten auf suspekten Technologien, JavaScript wird sinnvoll eingesetzt und der Surfer auf fehlende Freigaben hingewiesen. Cookies sind meist für Logins nötig und Javascript ermöglicht hübsche Animationen oder Prüfung von Eingaben.

 Um unsere Seiten komfortabel zu nutzen, empfehlen wir, Javascript zu aktivieren!

Weniger gute Webseiten liefern seltsame Fehlermeldungen:

**Forbidden** (403)

CSRF verification failed. Request aborted.

Ganz schlechte Websites machen irgendwas, aber nicht was man erwartet. Gelegentlich werden auch Referer oder User-Agent ausgewertet, obwohl es belanglos sein sollte, und Surfer werden nicht auf die notwendigen Freigaben hingewiesen. Hier ist man auf Probieren und Raten angewiesen. Als erstes kann man Cookies freigeben. Wenn das nicht hilft, kann man Javascript gezielt für einzelne Server freigeben oder unsichere SSL Verschlüsselung zulassen. Ob die Deaktivierung der Schutzmaßnahmen die volle Funktionalität aufwiegt, muss man bei Bedarf selbst entscheiden.

## 4.1 Auswahl des Webbrowsers

Firefox ist der Webbrowser der Mozilla Foundation. Er ist kostenfrei nutzbar und steht auf der Website des Projektes <sup>1</sup> für Windows, MacOS und Linux zum Download bereit. Linux-Distributionen enthalten den Browser in der Regel. Freunde von \*BSD finden Firefox im pkgsrc und können die aktuelle Version selbst compilieren.

Debian GNU/Linux enthält eine branded version des Browsers unter dem Namen *Iceweasel*, allerdings oft in einer veralteten Version. Das Mozilla Debian Team stellt eine aktuelle Version in einem extra Repository <sup>2</sup> bereit.

Die *Extended Support Releases*<sup>3</sup> (ESR-Versionen) von Firefox werden im Gegensatz zu den 6-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 auch aktuelle Verbesserungen in der SSL/TLS Verschlüsselung u.ä. Updates, die positiv für die Sicherheit sind.

Für **Linux i686** stelle ich auf der webseite [https://www.privacy-handbuch.de/handbuch\\_21browser.htm](https://www.privacy-handbuch.de/handbuch_21browser.htm) meinen selbst compilierten Firefox zum Download zur Verfügung. Dieser Firefox ist besser gehärtet als die Standard-Versionen der Linux Distributionen:

```
Position Independent Executable: yes
Stack protected: yes
Fortify Source functions: yes
Read-only relocations: yes
Immediate binding: yes
```

Außerdem wurden zur Verbesserung der Sicherheit und Privatsphäre einige überflüssige Features entfernt, die man zum Betrachten von Webseiten nicht braucht:

- Um keine Daten an Mozilla zu senden, wurde der Chrashreporter, der Maintenance Service und der Updater entfernt. Updates werden im RSS-Feed des Privacy-Handbuches angekündigt und müssen per Hand installiert werden.

---

<sup>1</sup> <https://www.mozilla.org/en-US/firefox/all/>

<sup>2</sup> <http://mozilla.debian.net>

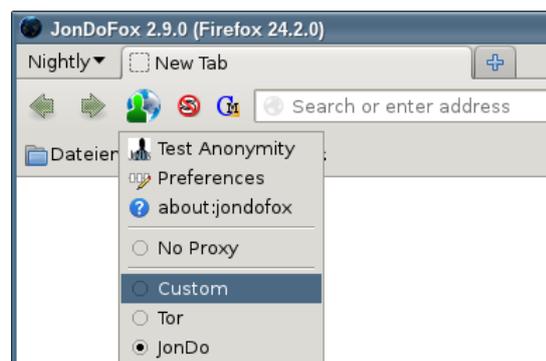
<sup>3</sup> <https://www.mozilla.org/en-US/firefox/organizations/all.html>

- WebRTC, die Gamepad-API und der StartupCache wurden entfernt.
- Um die Interaktionen mit dem Betriebssystem zu minimieren, wurden der Support für DBus, libnotify, GConf und Neko-Wifi entfernt.
- Dieser Browser verwendet aus Sicherheitsgründen grundsätzlich keine Plug-ins, die im Betriebssystem installiert wurden, also kein Flash o.ä.
- Die Standard-Suchmaschinen wurden entfernt. Nach der Erstinstallation muss man sich selbst Gedanken machen, welche Suchmaschinen man nutzen möchte und die Search Plug-ins von mycroftproject.com installieren oder man verwendet das JonDoFox-Profil.
- WICHTIG: Dieser Firefox hat eine BuildID, die sich von den Standard-Firefoxen unterscheidet und via Javascript auslesbar ist! Ich empfehle unbedingt, den aktuellen User Agent Fake für Windows nach dem ersten Start zu konfigurieren oder den benutzerdefinierten Proxy des JonDoFox passend zu konfigurieren.

### JonDoFox

Der JonDoFox<sup>4</sup> ist ein Browser-Profil für Firefox, das alle Einstellungen umsetzt, die auf den folgenden Seiten beschrieben werden.

Nach der Installation von Mozilla Firefox ist das JonDoFox-Profil zusätzlich zu installieren - fertig. Zukünftig fragt Firefox bei jedem Start, welches Profil genutzt werden soll. JonDoFox ist für anonymes Surfen mit JonDonym entwickelt worden, kann aber auch ohne Anonymisierungsdienst verwendet werden, indem man mit einem Klick auf das JonDoFox-XPI in der Toolbar auf *Kein Proxy* oder *Benutzerdefiniert* umschaltet.



Wenn man *Benutzerdefiniert* wählt, kann man in den Einstellungen vom JonDoFox einen User-Agent Fake auswählen. Es erschwert Angriffe aus dem Netz, wenn der User-Agent Fake nicht das Betriebssystem verrät.

**Firefox (Win32)** ist ein aktueller *Firefox (Windows)*. Diese Einstellung ist für Linux-Nutzer geeignet. Dabei werden allerdings die Plug-ins nicht deaktiviert (muss man selbst tun) und Do-Not-Track entsprechend den Privacy-Einstellungen gesendet.

<sup>4</sup> <https://www.anonym-surfen.de/jondofox.html>

**JonDo-UA** ist ein *Firefox ESR (Linux)* mit allen im JonDo-Mode aktiven Sicherheitsfeatures. Diese Einstellung ist für Windows- oder MacOS-Nutzer geeignet.

**Tor-UA** ist ein *Firefox ESR (Windows)*, bei aktiviertem Javascript aber als Fake erkennbar, da der TorBrowser etwas vom originalen Firefox abweicht.

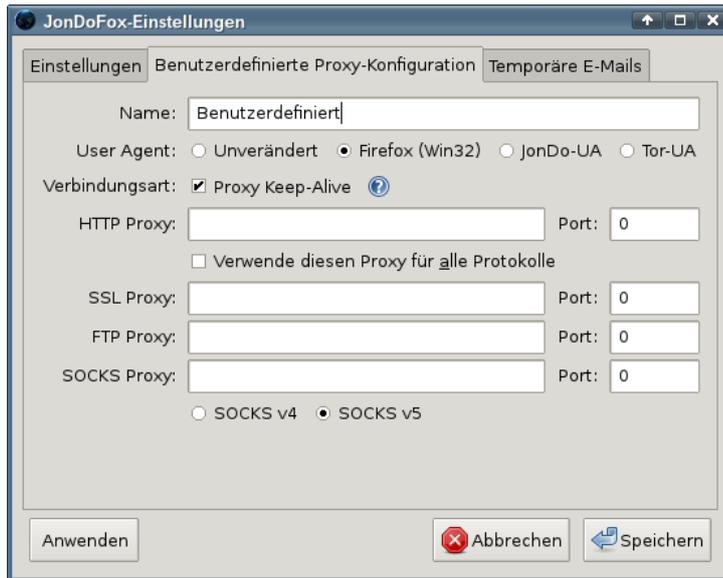


Abbildung 4.1: User-Agent Fake konfigurieren

Eine kurze Einführung in den Umgang mit JonDoFox gibt es im Kapitel Anonymisierungsdienste.

## 4.2 Datensparsame Suchmaschinen

Suchmaschinen werden sicher am häufigsten genutzt, um sich im Web zu orientieren. Neben den bekannten Datensammlern wie Google, MSN oder Yahoo gibt es durchaus 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 zu finden, die die Privatsphäre der Nutzer respektiert, einen umfangreichen Index zur Verfügung stellt und gute Ergebnisse liefert. Ein paar Vorschläge:

- **DuckDuckGo.com** (<https://duckduckgo.com>)  
DuckDuckGo ist eine privacyfreundliche Suchmaschine. Es gibt eine Javascript-freie Version (HTML). Neben der eigentlichen Suche bietet DuckDuckGo viele nette Erweiterungen <sup>5</sup>. Das Suchfeld kann als Taschenrechner genutzt werden, Einheiten können umgerechnet werden, Fragen nach dem Wetter können beantwortet werden (in englisch: *weather* oder *is it raining*)... u.v.a.m.
- **Qwant** (<https://www.qwant.com>)  
Qwant definiert sich selbst nicht als Suchmaschine sondern als Entdeckungsmaschine. Die Suchergebnisse sind nur mit Javascript sichtbar und die Darstellung der Ergebnisse ist etwas gewöhnungsbedürftig aber innovativ. Die Sprachauswahl der Ergebnisse wird anhand der IP-Adresse getroffen. Bei der Nutzung von Anonymisierungsdiensten sollte man auf die Wahl einer deutschen IP-Adresse achten.
- **Open Directory** (<http://www.dmoz.de> oder <http://www.dmoz.org>)  
Das Open Directory ist ein Katalog, der von Freiwilligen gepflegt wird. Man kann die Suche auf Kategorien eingrenzen und erhält übersichtliche Ergebnislisten.

### Meta-Suchmaschinen

Meta-Suchmaschinen leiten die Suchanfrage an mehrere Suchdienste weiter. Sie sammeln die Ergebnisse ein und sortieren sie neu.

- **Disconnect.me** (<https://search.disconnect.me/>)  
bietet einen privacy-freundlichen Such-Proxy für Google, Yahoo und Bing. Die Bildersuche von Disconnect.me ist bisher die einzige Suchmaschine, welche die Ergebnisse vollständig HTTPS-verschlüsselt lädt und mit den empfohlenen SSL Einstellungen funktioniert.
- **Ixquick.com** (<https://www.ixquick.com/deu>)  
wird von der niederländischen Firma Surfboard Holding B.V. betrieben. Die Suchmaschine speichert keine IP-Adressen und generiert keine Profile der Nutzer. Diese Meta-Suche fragt mehrere externe Suchmaschinen an, aber nicht Google. Ixquick.com ist mit dem Datenschutzsiegel EuroPriSe zertifiziert.

Als kleines Schmankerl bietet Ixquick die Möglichkeit, aus den Suchergebnissen heraus die Webseiten über einen anonymisierenden Proxy aufzurufen. Die aufgerufene Webseite sieht damit nur eine IP-Adresse von Ixquick. Neben den Ergebnissen findet man einen kleinen Link *Proxy*:

[Webinterface of "awxcnx" ★★★★★](#)  
HTTPS: <https://www.awxcnx.de>. MD5-Digest: 52:4A:8C:97:9D:C0:84:3D:12:63:08:  
<https://www.awxcnx.de/> - [Proxy](#) - [Markieren](#) - [1 weiteres Top-Ergebnis von dieser Site](#)

<sup>5</sup> <https://duckduckgo.com/goodies.html>

Aus Sicherheitsgründen entfernt der Proxy Javascript Code aus den aufgerufenen Webseiten. Es ist daher möglich, dass einige Webseiten nicht wie erwartet funktionieren. Außerdem ist KEINE Eingabe von Daten in Textfeldern der aufgerufenen Webseite möglich. Der Proxy kann die Webseiten nur darstellen.

- **Startpage** (<https://startpage.com>) wird ebenfalls von Surfboard Holding B.V. betrieben und ist mit dem Datenschutzsiegel EuroPriSe zertifiziert. Die Suchmaschine bietet privacy-freundlichen Zugriff auf die Google-Suche, ist also eine Ergänzung zu Ixquick.com. Einen Proxy zum anonymen Aufruf der Webseiten aus den Ergebnissen bietet Startpage auch.

Bei Ixquick.com und Startpage ist standardmäßig ein Family-Filter aktiv. Wer etwas Anstößiges sucht, erhält keinen Hinweis auf den Filter sondern nur die Antwort:

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

Dann muss eine andere Suchmaschine nutzen.

- **Metager.de** (<https://www.metager.de/>) ist ein deutscher Klassiker vom Suma e.V. Neben klassischen Suchdiensten wird auch die Peer-2-Peer Suche Yacy einbezogen. Dadurch verzögert sich die Anzeige der Ergebnisse etwas. Mit Javascript sieht die Seite etwas besser aus, funktioniert aber auch ohne Javascript. Metager.de kann auch als Tor Hidden Service unter folgender Adresse genutzt werden: <http://b7cxf4dkdsko6ah2.onion/tor/>

Metager bietet wie Ixquick und Startpage einen Proxy, um Ergebnisse aus der Suchliste anonym aufzurufen.

**Privacy-Handbuch**  
<https://privacy-handbuch.de/> <  [anonym öffnen](#)  
 Privacy-Handbuch. Wir sind die Vielen. Einleitung Privacy-Levels Nachdenken Spurenarm Surfen  
 Bezahlen im Netz E-Mails (allgm.)  
 gefunden von: [yandex.com](https://yandex.com)

- **UnBubble.eu** (<https://unbubble.eu>) ist eine weitere europäische Metasuchmaschine. Im Gegensatz zu Startpage.com werden die Suchanfragen nicht an Google weitergereicht und keine Google Ergebnisse angezeigt. Der Name ist eine Anspielung auf die FilterBubble, in der wir gefangen sind, wenn wir nur personalisierte Suchergebnisse angezeigt bekommen.

### 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 LEO nutzen. Der Translator kennt neben Englisch und Deutsch weitere Sprachen.

### Peer-2-Peer Suchmaschine

Yacy<sup>6</sup> 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 Oracle<sup>7</sup> 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 Repository<sup>8</sup> mit fertigen Paketen.

Nach dem Start von Yacy kann man im sich öffnenden Browserfenster 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.awxcnx.de/handbuch.htm`

wird im Moment des Klick eine Google-URL:

`http://www.google.de/url?q=https://www.awxcnx.de/.....`

---

<sup>6</sup> <http://yacy.net>

<sup>7</sup> <http://java.sun.com>

<sup>8</sup> <http://www.yacy-websuche.de/wiki/index.php/De:DebianInstall>

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

Diese Umschreibung der Links gibt es auch bei Bing, Facebook, Youtube und anderen Datensammlern. Das Firefox Add-on Google Privacy kann diese Umschreibung verhindern. Das Add-on ist noch im Beta Status. Die Entwicklung von *Google Privacy* ist ein Wettlauf zwischen Hase und Igel. Einfacher und sicherer ist es, privacy freundliche Suchmaschinen zu nutzen.

**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 Panopticklick 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. Sie ist mit dem Datenschutzsiegel EuroPriSe zertifiziert. Andere Suchmaschinen bieten eine andere Sicht auf das Netz - auch nicht schlecht, erfordert aber etwas Umgewöhnung.

### Firefox konfigurieren

Die Suchmaschinen kann man in Firefox in den *Einstellungen* in der Sektion *Suche* konfigurieren.

Die standardmäßig im Firefox installierten Suchmaschinen verraten überflüssige Informationen über die Installation. Wenn man z.B. unter Ubuntu den

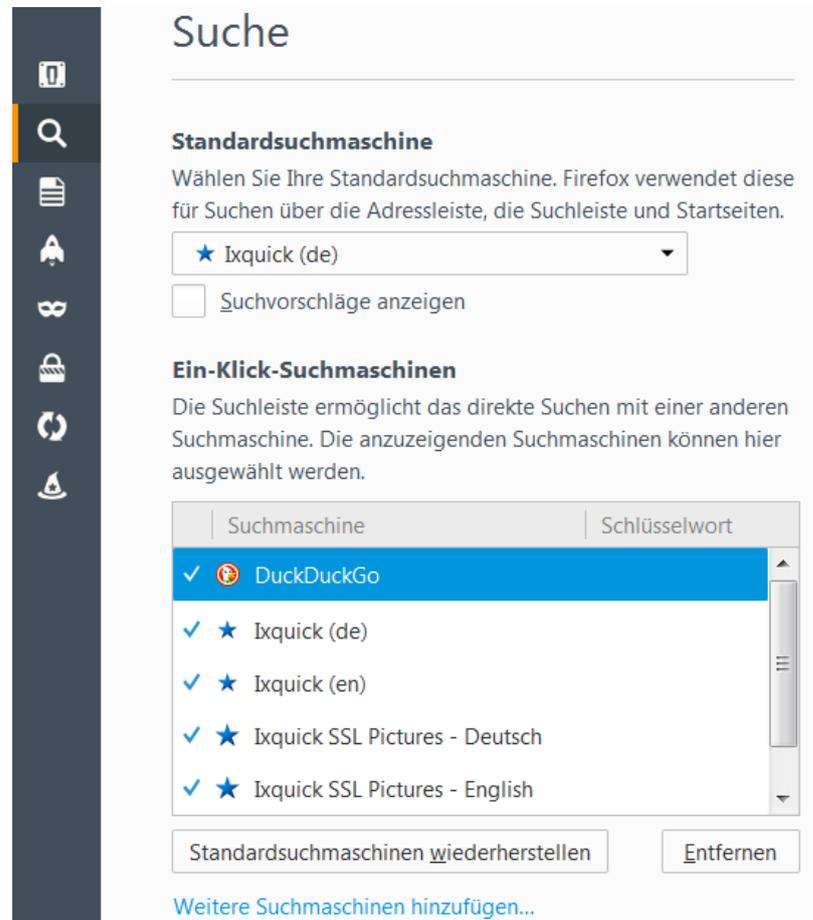


Abbildung 4.2: Suchmaschinen verwalten

Firefox aus dem Repository nutzt, wird bei jeder Suchanfrage irgendwie ein Hinweis auf Ubuntu angehängt:

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

```
https://duckduckgo.com/?...&t=canonical
```

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

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

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

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

Diese Parameter in der Suchanfrage können einen User-Agent Fake entlarven. Die standardmäßig installierten Suchmaschinen sollte man deaktivieren

und statt dessen privacy-freundlichere Plug-ins von [mycroft.mozdev.org](http://mycroft.mozdev.org) installieren.<sup>9</sup> zu installieren. In einem Suchformular auf der Webseite gibt man den Namen der Suchmaschine ein und findet schnell eine umfangreiche Liste von Varianten. Für viele Suchmaschinen wie DuckDuckGo, Ixquick, Google, Wikipedia, Startpage u.a.m. gibt es eine lokalisierte Variante (DE) mit SSL-Verschlüsselung und evtl. ohne Javascript. Diese Variante sollte bevorzugt werden. Ein Klick in der Liste der Ergebnisse installiert das Plug-in. Die Webseite funktioniert nur mit JavaScript.

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

Die Generierung von Suchvorschlägen kann man deaktivieren. Die Vorschläge kommen von der gewählten Standardsuchmaschine, sobald man mit der Eingabe im Suchfeld beginnt. Es verlangsamt aber die Reaktion auf Eingaben deutlich.

#### GeoIP-spezifische Standardsuchmaschine deaktivieren

Aus kommerziellen Gründen verwendet Firefox die Suche von Yahoo! als Standardsuchmaschine für US-amerikanische Nutzer. Um den eigenen Standort und damit das Land zu bestimmen, kontaktiert Firefox bei jedem Start den Server *location.services.mozilla.com*. Damit wird die externe IP-Adresse ermittelt und via Geolocation der aktuelle Standort bestimmt.

Um diese überflüssige Verbindungsaufnahme zu unterbinden, kann man unter der Adresse *about:config* folgende Variablen setzen:

```
browser.search.countryCode      = DE
browser.search.geoSpecificDefaults = false
browser.search.geoip.url        = ""    (leerer String)
```

## 4.3 Cookies

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 überwiegend 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<sup>10</sup> hat 2011 beim Surfen auf den TOP100 Webseiten 5.675 Cookies gefunden (ohne Login oder Bestellung). 4.914 Cookies wurden von Dritten gesetzt, also nicht von der aufgerufenen Webseite. Die

<sup>9</sup> <http://mycroft.mozdev.org/>

<sup>10</sup> <http://heise.de/-1288914>

Daten wurden an mehr als 600 Server übermittelt. Spitzenreiter unter den Datensammlern ist Google. 97% der populären Webseiten setzen Google-Cookies.

Immer mehr Tracking Dienste gehen dazu über, die Cookies im First-Party Context zu setzen, da Cookies von Drittsiten recht einfach blockiert werden können. Eine empirische Studie der Universität Leuven von 2014 zeigt, dass 44 verschiedene Tracking Dienste mehr als 40% des Surfverhaltens mit Hilfe von Cookies verfolgen können, auch wenn man Cookies für Drittsiten blockiert und nur First-Party Cookies erlaubt. Die Cookies werden mit Javascript geschrieben oder der Tracking Dienst erschleicht sich mit einem DNS-Alias als Subdomain der besuchten Webseite First-Party Status.<sup>11</sup>

Die Tracking-Cookies werden auch von der NSA und GCHQ im Rahmen der globalen Überwachung genutzt. Die Geheimdienste beobachten den Datenstrom im Internet und identifizieren Surfern anhand langlebiger Cookies, insbesondere das Google PREF Cookie wird von den Überwachern gern genutzt. Zielpersonen werden anhand dieser Cookies verfolgt und bei Bedarf mit *Foxit Acid* gezielt angegriffen, wenn die Identifikation für mindestens 2 Wochen stabil möglich ist.<sup>12</sup>

Sinnvoll ist ein **Whitelisting** für die Behandlung von Cookies:

1. Standardmäßig wird die Annahme von Cookies verweigert.
2. Für vertrauenswürdige Websites, welche die Nutzung von Cookies zur vollen Funktion benötigen, werden Ausnahmen zugelassen.
3. Alle gespeicherten Cookies werden beim Schließen des Browsers automatisch gelöscht.

Fast alle Login-Seiten, welche Cookies zur Identifizierung des Surfers verwenden, weisen mit einem kleinen Satz auf die notwendigen Freigaben hin. Treten beim Login seltsame Fehler auf, z.B. ständig die Fehlermeldung *FALSCHES PASSWORT*, verweigert der Browser wahrscheinlich die Annahme von Cookies. Die Website sollte in die Liste der vertrauenswürdigen Websites aufgenommen werden oder man muss Cookies temporär erlauben.

### Mozilla Firefox konfigurieren

Mozilla Firefox bietet bereits standardmäßig die Möglichkeit, die meisten Cookies ohne Einbußen am Surf-Erlebnis loszuwerden. Im Bild 4.4 gezeigte Dialog *Einstellungen* Sektion *Datenschutz* kann die Annahme von Cookies standardmäßig deaktiviert werden.

Mit einem Klick auf den Button *Ausnahmen* kann man Webseiten konfigurieren, die Cookies setzen dürfen. In der Regel sind das alle Webseiten, die einen Login erfordern.

<sup>11</sup> [https://securehomes.esat.kuleuven.be/gacar/persistent/the\\_web\\_never\\_forgets.pdf](https://securehomes.esat.kuleuven.be/gacar/persistent/the_web_never_forgets.pdf)

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

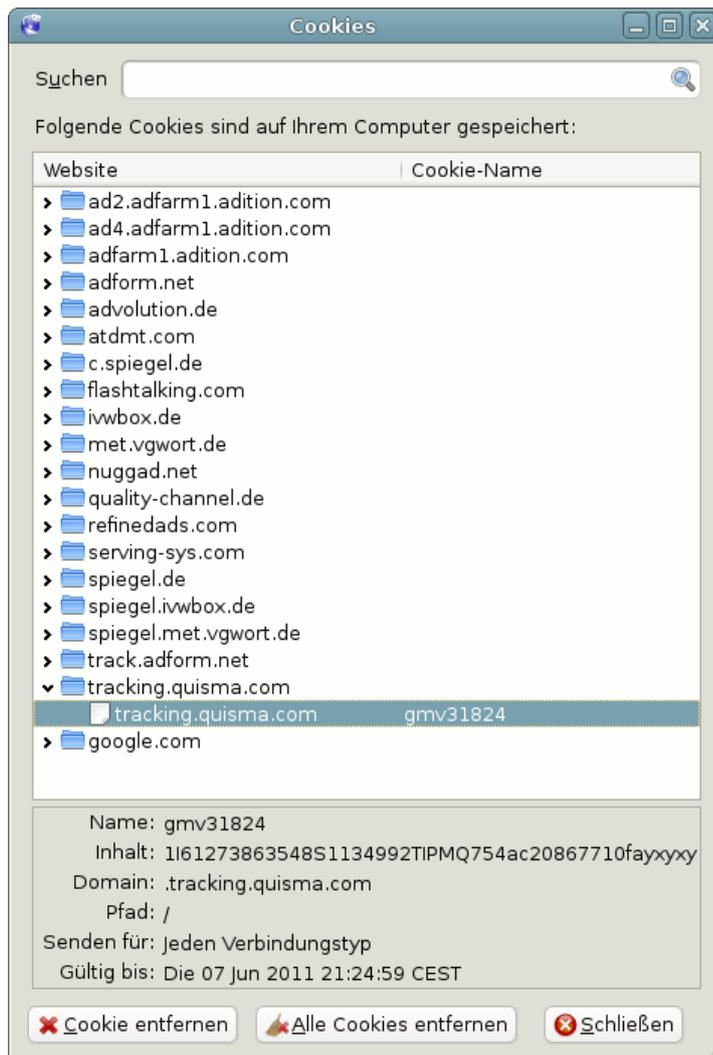


Abbildung 4.3: Liste der Cookies beim Besuch von Spiegel-Online

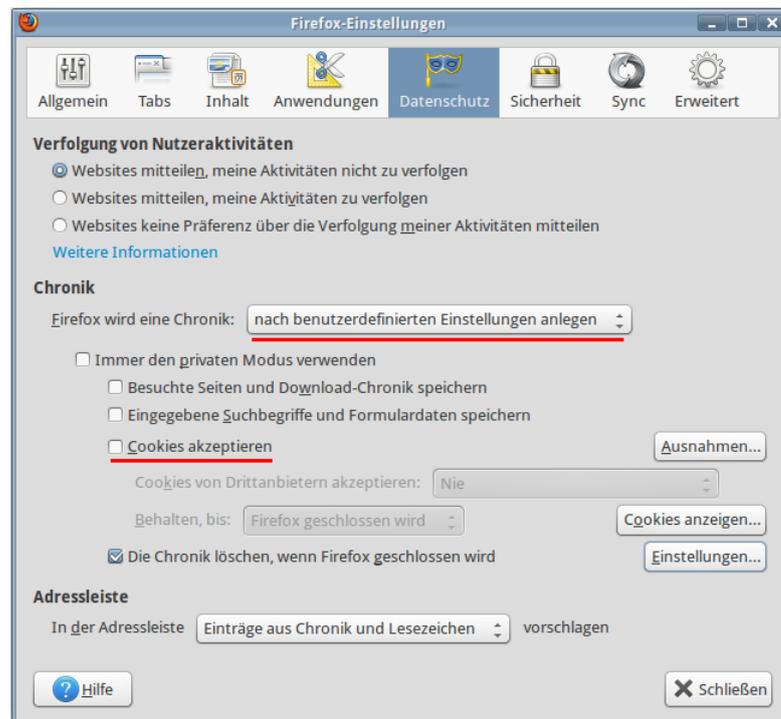


Abbildung 4.4: Cookies-Einstellungen in Firefox

Außerdem sollte man die Option *Chronik löschen, wenn Firefox geschlossen wird* aktivieren und in den Einstellungen für diese Funktion das Löschen der Cookies aktivieren.

Das Add-on **Cookie Controller**<sup>13</sup> ist empfehlenswert. Es erlaubt die site-spezifische Verwaltung von Cookies. Ein einfacher Klick auf das Install-Symbol der Website startet den Download der Erweiterung und installiert sie.

### DOMStorage in Firefox

Mozilla Firefox bietet auch die clientseitige HTML5 Datenspeicherung. Dieser DOMStorage oder Web-Storage wird gelegentlich auch als Super-Cookie bezeichnet, da bis zu 5 MB große Datenmengen mit Hilfe von Javascript abgelegt werden können.

Aktuelle Versionen von Firefox wenden die Beschränkungen für Cookies auch auf den DOMStorage an. Es reicht aus, die Cookies zu deaktivieren. Damit ist auch die clientseitige Datenspeicherung deaktiviert. Der DOMStorage wird auch zusammen mit den Cookies gelöscht. Diese parallele Anwendung der Einstellung für Cookies auf DOMStorage gilt nur für Firefox. Andere Browser verhalten sich bezüglich der clientseitigen Datenspeicherung anders!

<sup>13</sup> <https://addons.mozilla.org/en-US/firefox/addon/cookie-controller/>

### Indexed Database API

Am 08.01.2015 hat das W3C die *Indexed Database API* als Standard verabschiedet. Dabei handelt es sich um eine hierarchische Datenbank im Browser, die mit Javascript genutzt werden kann. Im Unterschied zum DOM-Storage können nicht nur Key-Value-Paare gespeichert werden, sondern mittels SQL auch komplexe Abfragen realisiert werden.

Wie jede Technologie, die Daten im Browser speichert, kann die Indexed Database ähnlich wie Cookies für die Markierung von Surfern für Trackingzwecke genutzt werden. Forscher der KU Leuven (Belgien) haben darauf hingewiesen, dass diese Technik bereits genutzt wird und näher untersucht werden sollte.

Um die Indexed Database API im Firefox abzuschalten, ist unter *about:config* folgender Wert zu setzen:

```
dom.indexedDB.enabled = false
```

### Flash-Cookies

Aus Sicherheitsgründen empfehle ich, keinen Flash Player zu nutzen. Wenn man auf Flash absolut nicht verzichten kann, dann findet man die privacy-freundliche Konfiguration des Adobe Flash-Players in einem gesonderten Abschnitt für Plug-ins.

## 4.4 EverCookies

80% der Internetnutzer lehnen das Tracking ihres Surfverhaltens ab. Viele Surfer ergreifen einfache Maßnahmen gegen Tracking Cookies. Nach einer Untersuchung von AdTiger blockieren 52,5% der Surfer die Annahme von Cookies, die nicht von der aufgerufenen Website stammen (sogenannte Third-Party-Cookies). Andere Studien<sup>14</sup> kommen auf 15%...35% Cookie-Verweigerer unter den Surfern (was mir seriöser erscheint). Dabei handelt es meist um Surfer, die regelmäßig auf dem Datenhighway unterwegs sind und somit die Erstellung präziser Profile ermöglichen könnten. Von Gelegenheits-Surfern kann man kaum umfassenden Interessen-Profilen erstellen.

Die Tracking-Branche reagiert auf diese Entwicklung mit erweiterten Markierungen, die unter der Bezeichnung *EverCookie* zusammengefasst werden. Zusätzlich zum Tracking-Cookie werden weitere Markierungen im Browser gespeichert. Später kann ein gelöscht Tracking-Cookie anhand dieser Markierungen wiederhergestellt werden.

---

<sup>14</sup> <http://smorgasbork.com/component/content/article/84-a-study-of-internet-users-cookie-and-javascript-settings>

Nach empirischen Untersuchungen der University of California <sup>15</sup> nutzen viele Trackingdienste EverCookie Techniken. Häufig werden seit 2005 Flash-Cookies bzw. LSOs parallel zu normalen Cookies eingesetzt, wobei diese Technik auf dem absteigenden Ast ist. 2011 nutzen 37% der TOP100 Webseiten diese Technik, 2012 nur noch 17%. Die Flash-Cookies werden durch HTML5-Techniken wie DOMStorage und ETags ersetzt. 31% der TOP100 Webseiten nutzen moderne HTML5-Techniken zur Markierung der Surfer (Stand 2012).

- Die *Google-Suche* nutzt DOMStorage, was eine Markierung von Nutzern auch bei deaktivierten Cookies ermöglichen soll.
- Die Firma *Clearspring* protzt damit, präzise Daten von 250 Mio. Internetsurfern zu haben. Sie setzte bis 2010 Flash-Cookies ein, um gelöschte Cookies wiederherzustellen.
- *Ebay.de* verwendet Flash-Cookies, um den Browser zu markieren.
- *AdTiger.de* bietet umfangreiche Angebote zur gezielten Ansprache von Surfern und protzt damit, 98% der Zugriffe über einen Zeitraum von deutlich länger als 24h eindeutig einzelnen Nutzern zuordnen zu können. Nach einer eigenen Studie kann AdTiger aber nur bei 47,5% der Surfer normale Cookies setzen.
- Die Firma *KISSmetrics* (*“a revolutionary person-based analytics platform“*) setzte zusätzlich zu Cookies und Flash-Cookies noch ETags aus dem Cache, DOMStorage und IE-userData ein, um Surfer zu markieren. Aufgrund der negativen Schlagzeilen wird seit Sommer 2011 auf den Einsatz von ETags verzichtet.

#### EverCookies - never forget

Der polnische Informatiker Samy Kamkar hat eine Demonstration <sup>16</sup> von EverCookie Techniken erstellt, die verschiedene technische Möglichkeiten basierend auf HTML5 zeigen:

- Local Shared Objects (Flash Cookies)
- Silverlight Isolated Storage
- Cookies in RGB Werten von automatisch generierten Bildern speichern
- Cookies in der History speichern
- Cookies in HTTP ETags speichern
- Cookies in Browser Cache speichern
- window.name auswerten
- Internet Explorer userData Storage
- HTML5 DOMStorage
- HTML5 Database Storage (IndexedDB)
- HTTP-Auth speichern

<sup>15</sup> <http://www.law.berkeley.edu/privacysurvey.htm>

<sup>16</sup> <http://samy.pl/evercookie/>

### Verteidigungsstrategien

Zur Verteidigung gibt es drei Möglichkeiten:

1. Die Verbindung zu Tracking-Diensten kann mit **AdBlockern** komplett verhindert werden. Es sind Filterlisten zu nutzen, die in der Regel als Privacy Listen bezeichnet werden.
2. Viele EverCookie Techniken nutzen Javascript. Die Freigabe von Javascript nur auf wenigen, vertrauenswürdigen Seiten schützt ebenfalls. HTML5 DOMStorage folgt den Freigaben für Cookies und Hinweise zur Configuration des Cache zur Vermeidung langfristiger Markierungen mit ETags findet man weiter unter.
3. Die Verwendung von HTML5 IndexedDB zur Wiederherstellung gelöschter Tracking Cookies wurde von Forschern der Universität Leuven (Belgien) erstmals im Sommer 2014 in the wild nachgewiesen. Als Schutz gegen diese EverCookies kann man die IndexedDB in Firefox deaktivieren:

```
dom.indexedDB.enabled = false
```

Einen EverCookie-sicherer Browser kann nur mit Konfigurationseinstellungen nicht erreichen. Der Datenverkehr ist durch zusätzliche Maßnahmen zu reinigen. Bisher kann nur der **JonDoFox** und der **JonDoBrowser** alle von Samy Kamkar vorgestellten Techniken während des Surfens blockieren.

Der **TorBrowser** blockiert EverCookies beim Surfen nicht sondern beseitigt alle Markierungen beim Beenden der Surf-Session (Schließen des Browsers oder *Neue Identität* im TorButton wählen). Während der Session ist man anhand von EverCookies wiedererkennbar. Dieses Verhalten entspricht der Zielstellung der Tor-Entwickler.

## 4.5 JavaScript

JavaScript ist eine der Kerntechniken des modernen Internet, birgt aber auch einige Sicherheitsrisiken.

1. Mit Hilfe von Javascript kann man ein Vielzahl von Informationen über den Browser und das Betriebssystem auslesen. Bildschirmgröße, Farbeinstellungen, installierte Schriftarten... Diese Informationen können zu einem individuellen Fingerabdruck des Browsers verrechnet werden (siehe: Kapitel *Tracking Techniken* in der Einleitung).
2. EverCookie Techniken nutzen Javascript, um zusätzliche Markierungen im Browser zu hinterlegen und gelöschte Tracking Cookies wiederherzustellen.
3. Bösartiger Javascript Code kann aktiv Sicherheitslücken im Browser ausnutzen und den Rechner kompromittieren. Alle bisher bekannten Exploits von NSA/FBI gegen den TorBrowser nutzten bösartiges Javascript.

4. Forscher der Columbia University haben eine side-channel attack vorgestellt, die komplett als Javascript im Browser läuft: *The Spy in the Sandbox – Practical Cache Attacks in Javascript*<sup>17</sup>. Mit dem Angriff können beliebige Prozesse außerhalb des Browsers analysiert werden ohne den Rechner zu kompromittieren (spurenfrei). Seitenkanalangriffe sind ein moderner Angriff gegen Kryptografie.
5. Bösartiger Javascript Code kann sich auch gegen Dritte richten, ohne das der Nutzer es bemerkt. Chinas Great Cannon<sup>18</sup> injiziert Javascript Code beim Aufruf chinesischer Webseiten, um die PCs der Nutzer als Botnet für DDoS-Attacken zu nutzen.

Das Einschleusen von bösartigem Javascript Code kann auch über vertrauenswürdige Webseiten erfolgen (wenn die Webseiten nachlässig programmiert wurden). Werbefbanner können ebenfalls bösartigen Javascriptcode transportieren. 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.<sup>19</sup>

### Prinzip Whitelisting

Ein generelles Abschalten ist heutzutage nicht sinnvoll. Ähnlich dem Cookie-Management benötigt man ein Whitelisting, 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 deutliche Einschränkung der Funktionalität zu erwarten ist.



Um unsere Seiten komfortabel zu nutzen, empfehlen wir, Javascript zu aktivieren!

#### 4.5.1 NoScript für Mozilla Firefox

Die Einstellungen für JavaScript lassen sich mit dem Add-on *NoScript* komfortabel verwalten. Die Erweiterung kann von der Website<sup>20</sup> installiert werden. Ein Klick auf das Install-Symbol der Website installiert die Erweiterung.

Nach dem Neustart von Firefox ist in der Toolbar ein zusätzliches Symbol vorhanden, das den Status der Freigabe für Javascript anzeigt. Ein Klick auf das Symbol öffnet das im Bild 4.5 gezeigte Menü, welches Javascript für die aktuell relevanten Webseiten generell oder temporär für die laufende Sitzung freigibt.

Skripte von Drittanbietern (googletagmanager, ioam...) werden üblicherweise nur zum Spionieren verwendet und sind für die Funktionalität selten notwendig. Einige Webseiten verwenden *Captchas* als Spamschutz. Die Captchas werden von Drittseiten eingebunden (Recaptcha.com, Nucaptcha.com...)

<sup>17</sup> <http://arxiv.org/pdf/1502.07373v2.pdf>

<sup>18</sup> <https://citizenlab.org/2015/04/chinas-great-cannon/>

<sup>19</sup> <http://heise.de/-1787511>

<sup>20</sup> <https://addons.mozilla.org/de/firefox/addon/noscript>

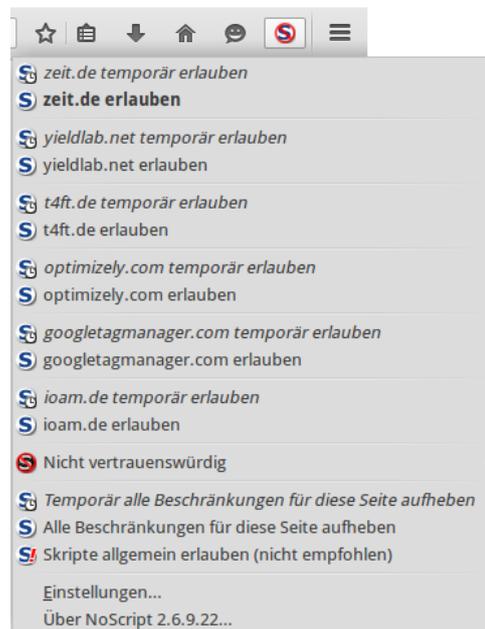


Abbildung 4.5: NoScript-Button und Menü in der Toolbar

und funktionieren nur, wenn Javascript für den Captcha-Provider freigegeben ist. Wenn das Captcha auf einer Webseite nicht funktioniert, schaut man in der NoScript-Liste nach, ob evtl. ein Captcha-Provider dabei ist und gibt Javascript temporär für diese Domain frei.

Wählt man den Punkt *Einstellungen* im NoScript-Menü, öffnet sich der Einstellungsdialog (Bild 4.6), der auf dem Reiter *Positivliste* eine Liste der Websites zeigt, für die Javascript freigegeben wurde. Als Erstes sollte man aus der Positivliste alles entfernen, was man nicht braucht (z.B. google.com). Damit diese Positivliste nicht von NoScript durch Updates modifiziert wird, ist unter *about:config* folgende Variable zu setzen:

```
noscript.allowWhitelistUpdates = false
```

Auf dem Reiter *Benachrichtigungen* lässt sich beispielsweise konfigurieren, ob NoScript den Surfer mit einem Sound oder mit einem Info-Balken darüber informiert, dass Scripte auf der aktuellen Webseite blockiert wurden. Der Sound nervt mich, diese Option habe ich deaktiviert. Wenn eine Webseite jedoch nicht wie erwartet funktioniert, kann die kurze Einblendung eines Info-Balkens hilfreich bei der Suche nach den Ursachen sein.

### Sicherheitsfunktionen

NoScript dient nicht nur der Steuerung von Javascript, es bieten **Schutz gegen vielfältige Angriffe** aus dem Netz. (XSS-Angriffe, Webbugs, Click-

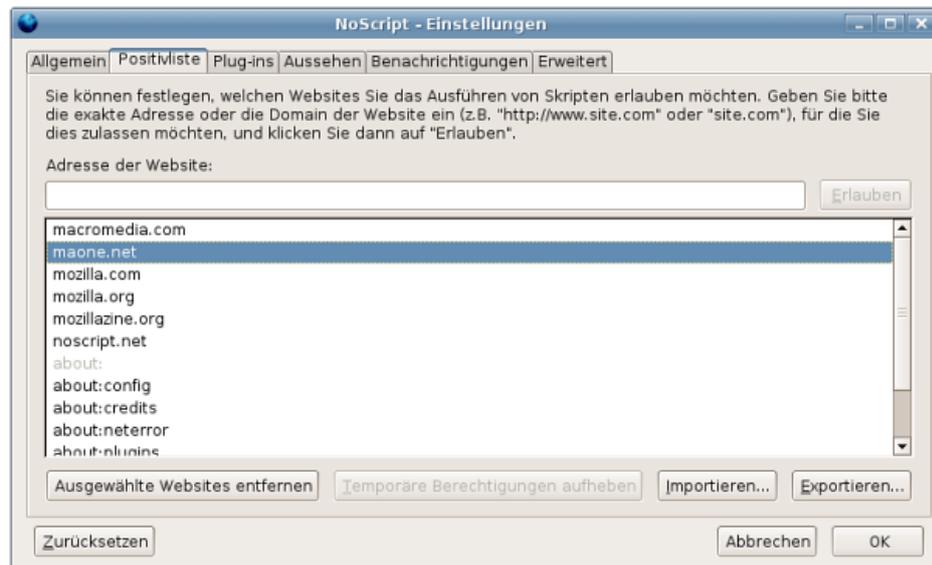


Abbildung 4.6: Einstellungen für NoScript

Hijacking...).

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<sup>21</sup>.

Bösartiger Javascript Code könnte lokale Dienste wie CUPS oder andere Rechner im LAN angreifen. Im Mai 2015 wurde ein Exploit-Kit entdeckt, der als bösartiges Javascript auf Webseiten platziert wird und beim Aufruf der Webseite den Router angreift um die DNS Einstellungen zu ändern und damit den Internetzugriff beliebig zu manipulieren<sup>22</sup>.

NoScript bietet mit dem *Application Boundary Enforcer* (ABE) einen Schutz gegen diesen Angriff. Unter *Erweitert* auf dem Reiter *ABE* kann man dieses Feature konfigurieren. Die Option *WAN-IP als LOCAL* sollte man deaktivieren, weil NoScript sonst bei jedem Start des Browsers einen externen Server kontaktiert, um die externe IP-Adresse zu ermitteln.

### Javascript Security Einstellungen

Mit kleinen Anpassungen der Einstellungen unter der Adresse `about:config` kann man die Robustheit von Javascript gegen Exploits wie z.B CVE-2015-0817

<sup>21</sup> <https://mailman.boum.org/pipermail/tails-dev/2015-April/008607.html>

<sup>22</sup> <http://heise.de/-2665387>

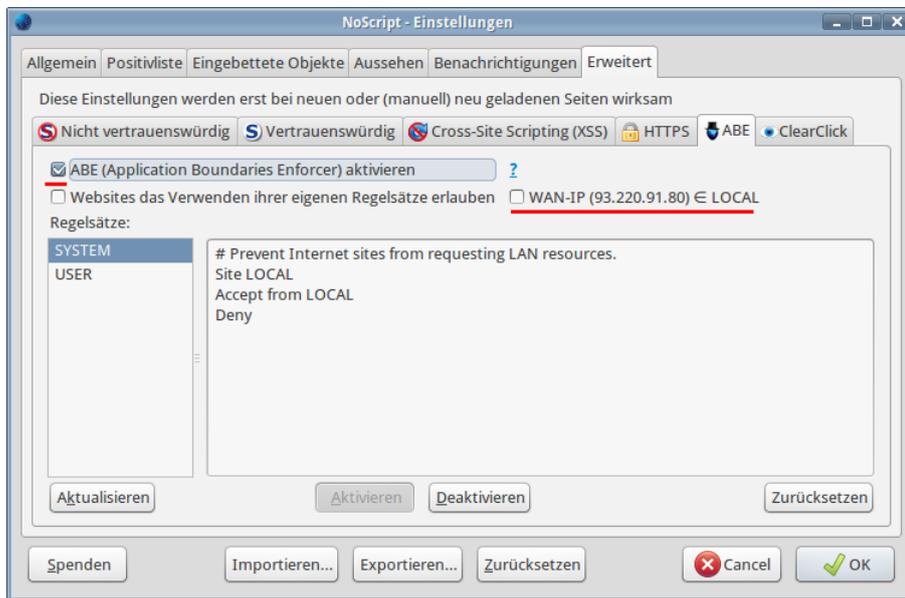


Abbildung 4.7: Einstellungen für NoScript

<sup>23</sup> verbessern. Diese Vorschläge verringern die Performance von Javascript geringfügig aber nicht signifikant:

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

Die Javascript SharedWorker erlauben den Datenaustausch zwischen den IFrames in Webseiten, die in unterschiedlichen Tabs geöffnet sind, auch wenn die Webseiten nicht zur selben Domain gehören. Dieses Feature sollte deaktiviert werden, da es z.B. Trackingdiensten Synchronisierungen von Daten über unterschiedliche Domains ermöglicht.

```
dom.workers.sharedWorkers.enabled = false
```

## 4.6 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>
```

<sup>23</sup> <https://www.mozilla.org/en-US/security/advisories/mfsa2015-29/>

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>
```

Für Webdesigner sind iFrames eine Technik aus dem vergangenen Jahrhundert und werden kaum noch verwendet. Man kann iFrames generell mit NoScript blockieren ohne wesentliche Einschränkungen beim Surfen (Bild 4.8). An Stelle des blockierten iFrames zeigt NoScript einen Platzhalter an. Bei Bedarf kann man den blockierten iFrame mit einem Klick auf das Platzhaltersymbol laden.

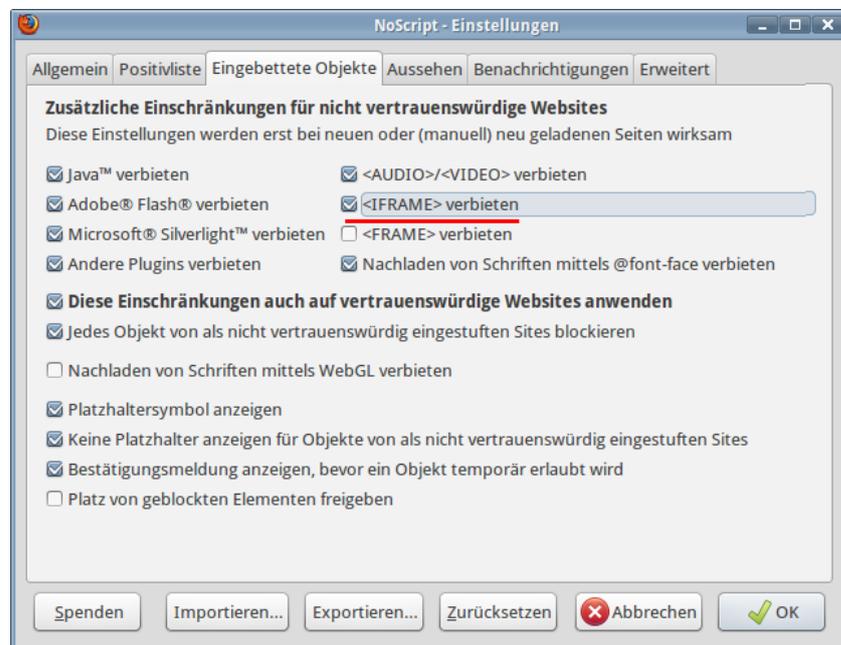


Abbildung 4.8: iFrames mit NoScript blockieren

## 4.7 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. Mit Hilfe von listen- und musterbasiert Filtern kann der Zugriff auf Werbung sowie die von diesen Servern genutzten Cookies unterbunden werden.

Hinweis: Viele Angebote im Web werden über Werbung finanziert, da die Nutzer meist nicht bereit sind, für diese Angebote zu bezahlen. Die Redaktion von Heise.de hat ein kurzes Statement<sup>24</sup> zu Werbung auf Heise online veröffentlicht und erklärt, wie sie einzelne Webangebote durch Freigaben im Werbeblocker unterstützen können.

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.

Hinweis: das System METIS<sup>25</sup> der VG Wort verwendet HTML-Wanzen, um die Besucher von Online-Angeboten zu zählen und anhand der Ergebnisse Tantiemen an Autoren auszuzahlen.

Facebook und andere Sociale Netze verwenden sogenannte **Like Buttons**, um Daten zu sammeln. Die Verwendung der Like Buttons ist nach Ansicht von Thilo Weichert (ULD) nicht mit deutschem Datenschutzrecht vereinbar. Deutsche Webseitenbetreiber sind aufgefordert, die Facebook Buttons von ihren Seiten zu entfernen<sup>26</sup>. Mit dem Aufruf einer Webseite, die den Like Button enthält, werden Daten an Facebook übertragen und dort ausgewertet.

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 vorher-sagen<sup>27</sup>. Man verrät mit einem Klick auf einen Like Button möglicherweise Informationen, die man nicht im Netz veröffentlichen möchte.

### 4.7.1 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 verglichen<sup>28</sup>. Die Ergebnisse in Bild 4.9 zeigen: keine Lösung ist perfekt.

---

<sup>24</sup> <http://www.heise.de/Adblocker-auf-heise-online-1164703.html>

<sup>25</sup> <http://www.vgwort.de/metis.php>

<sup>26</sup> <https://www.datenschutzzentrum.de/facebook>

<sup>27</sup> <http://heise.de/-1820638>

<sup>28</sup> <https://cyberlaw.stanford.edu/node/6730>

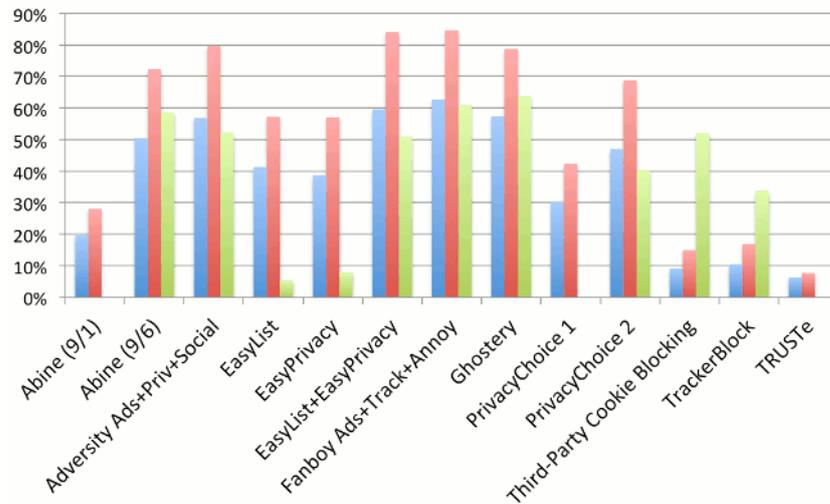


Abbildung 4.9: Effektivität verschiedener Tracking-Filter

Aufgrund der Flexibilität bei der Einbindung verschiedener Filterlisten empfehle ich *AdBlock Plus*. Mit den Easylist Filterlisten erreichten das Add-on bei dem Test mit die besten Ergebnisse. Die Listen werden ständig weiterentwickelt. Es gibt als Zusatz eine spezielle Filterliste für deutsche Webseiten.usätzlich zur den Blocklisten gegen Werbung und Tracking gibt es auch Listen, die die Social Media Buttons blockieren.

*Ghostery* schneidet im Test auch gut ab und wird oft empfohlen. Es gibt aber immer wieder Probleme mit *Ghostery* auf einigen Webseiten, da das Add-on kein Whitelisting kennt. Außerdem arbeitet es mit einer festen Blockliste, die nicht flexibel erweitert oder kombiniert werden kann.

#### 4.7.2 Adblock für Mozilla Firefox

Für Mozilla Firefox steht mit **Adblock Plus**<sup>29</sup> ein Add-on für das listenbasierte Blockieren von Werbung zur Verfügung. Für Adblock Plus gibt es viele Listen zum Blockieren von Werbung (länderspezifisch), Tracking-Diensten und der Social Media Like-Buttons. Ein einfacher Klick auf das Install-Symbol der Website startet den Download der Erweiterungen und installiert sie.

Nach dem Neustart ist mindestens eine Filterliste zu abonnieren (Bild 4.10). Standardmäßig wird für deutsche Benutzer die Liste *EasyList Germany* + *EasyList* vorgeschlagen. *EasyList* ist eine gute Wahl, die man akzeptieren kann.

Weitere Filterlisten können im Einstellungen von Adblock Plus unter dem Menüpunkt *Filter Preferences* abonniert werden. Hier ist der Menüpunkt *Filter* -> *Abonnement hinzufügen* zu wählen. Aus der Liste der angebotenen Filter kön-

<sup>29</sup> <https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/>

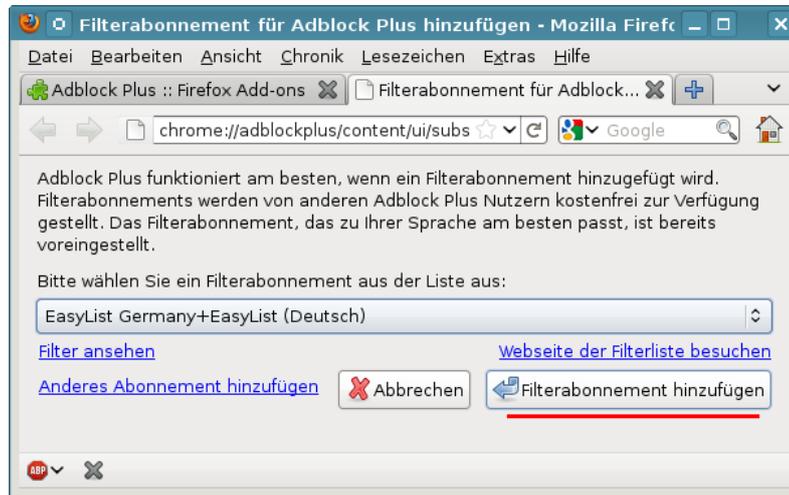


Abbildung 4.10: Auswahl einer Liste nach der Installation von Adblock Plus

nen regional passende Listen gewählt werden. Folgende Filter-Listen sind als Ergänzung zur EasyList passend:

- **EasyPrivacy** blockiert meist unsichtbare Tracking-Elemente zum Auspähen ihres Verhaltens im Internet mit HTML-Wanzen. Die Liste ist eine sinnvolle Ergänzung zur EasyList (Germany). Bei der Installation von *EasyPrivacy* kann die zusätzliche empfohlene EasyList deaktiviert werden, das sie bereits vorhanden ist.
- **Fanboy's Social Blocking List** ist eine Liste zum Blockieren der verschiedenen Social Media Tracking Features wie Facebook Like Buttons u.ä. Zur Installation kopiert man folgende URL in die Adressleiste von Firefox: <abp:subscribe?location=https://easylist-downloads.adblockplus.org/fanboy-social.txt>.

Mit der Version 2.0 hat AdBlock Plus eine Whitelist für unaufdringliche Werbung eingeführt. Die Filterung wird auf den Webseiten in der Whitelist abgeschaltet, so dass diese Webseiten Werbung einblenden können. Wer auch keine unaufdringliche Werbung sehen möchte, hat folgende Optionen:

1. Man kann dieses Feature wie in Bild 4.11 in der Übersicht der Filterlisten abschalten, indem man die Option *Nicht aufdringliche Werbung zulassen* deaktiviert.
2. Alternativ kann man auch das Add-on **AbBlock Edge** statt AdBlock Plus verwenden. Es ist 100% kompatibel mit AdBlock Plus, das Whitelisting ist jedoch nicht vorhanden.

Statt dessen kann man selbst entscheiden, welchen Webseiten man das Anzeigen von Werbung gestatten möchte. Mit einem gelegentlichen Klick auf Werbung kann man gute Webseiten bei der Finanzierung unterstützen. Wenn Sie eine Webseite im Browser geöffnet haben, können Sie in den Menü von AdBlock die aktuelle Webseite zu einer eigenen Whitelist hinzufügen.

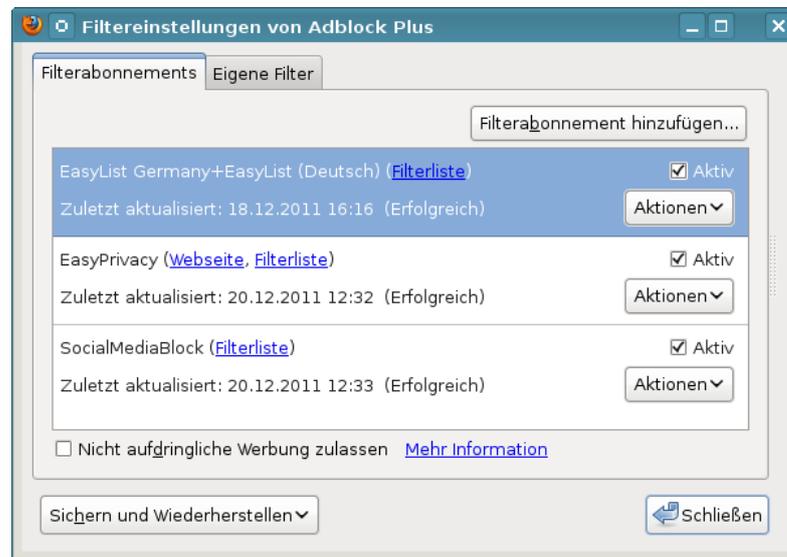


Abbildung 4.11: Whitelisting in AdBlock Plus deaktivieren

### Anti-AdBlock

Anti-AdBlock ist ein Script für Webmaster, die den Besucher der Webseite zur Deaktivierung von AdBlock Plus zwingen wollen. Bei aktivem Werbeblocker sieht man beim Besuch einer präparierten Webseite nur folgenden Hinweis:

**Please disable your ad blocker!**  
**Bitte deaktiviere Deinen Werbeblocker!**  
**— Veuillez désactiver votre bloqueur de publicité!**  
**Por favor, desactive el bloqueador de anuncios!**  
[antiblock.org](http://antiblock.org) v2.2.2

Wer sich nicht gängeln lassen will, kann das Firefox Add-on **Disable Anti-Adblock**<sup>30</sup> installieren. Dann kann man die Webseite wieder werbefrei betrachten.

### Werbung auf der NewTab Page

Mozilla möchte die NewTab Seite für die Einblendung von Werbung nutzen. Diese Seite erscheint standardmäßig, wenn man einen neuen Tab öffnet. Sie soll Thumbnails der häufig genutzten Webseiten zeigen. Bei einem frisch installierten Browser oder wenn man die Speicherung der History deaktiviert, bleibt diese Seite allerdings leer.

Mozilla Chefin Mitchell Baker ist der Meinung<sup>31</sup>, dass die Mehrzahl der Nutzer es gut finden oder es tolerieren werden, wenn die leeren Thumbnails

<sup>30</sup> <https://addons.mozilla.org/en-US/firefox/addon/disable-anti-adblock/>

<sup>31</sup> <http://heise.de/-2115431>

für Werbung genutzt werden. Mit Firefox 33.1 hat Mozilla die Pläne zur Werbung auf der NewTab Seite umgesetzt.

Man kann die Werbung abschalten indem man auf das kleine Zahnrad oben rechts in der NewTab Seite klickt und in dem sich öffnenden Menü Abb. 4.12 die Option *Leere Seite anzeigen* auswählt. Wer an der NewTab Seite Gefallen gefunden hat und sie weiterhin nutzen möchte, sollte zumindest die Option *Vorschläge einbeziehen* deaktivieren.

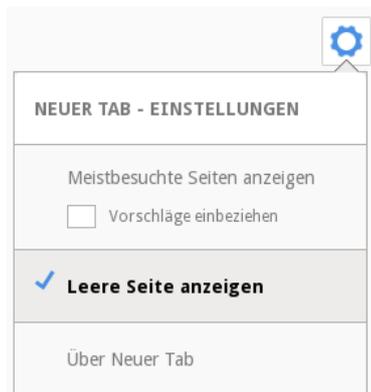


Abbildung 4.12: NewTab Seite konfigurieren

### Speicherung von Screenshots der besuchten Webseiten

Firefox speichert Screenshots von jeder besuchten Webseite auf der Festplatte, um sie später als Thumbnails auf der New Tab Page einzublenden. Diese Speicherung gefällt mir nicht, da ich mein Surfverhalten nicht protokollieren möchte, auch nicht auf dem eigenen Rechner. Um diese Speicherung abzuschalten, kann man eine neue Variable vom Typ Boolean unter *about:config* erstellen:

```
browser.pagethumbnails.capturing_disabled = true
```

### Mozillas Werbung nach einem Update

Nach jedem Update von Firefox wird eine Webseite 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"  
startup.homepage_welcome_url = " "  
startup.homepage_override_url = " "
```

## 4.8 History Sniffing

Browser speichern Informationen über besuchte Webseiten in einer Surf-History. Eine empirische Untersuchung der University of California <sup>32</sup> zeigt, dass ca. 1% der Top 50.000 Websites versuchen, diese Daten über zuvor besuchte Websites auszulesen. Daneben gibt es spezielle Anbieter wie Tealium oder Beencounter, die einem Webmaster in Echtzeit eine Liste der Websites liefern, die ein Surfer zuvor besucht hat. Die dabei übermittelten Informationen erlauben ein ähnlich detailliertes Interessenprofil zu erstellen, wie das Tracking über viele Websites. In der Regel werden die Informationen für die Auswahl passender Werbung genutzt.

Ein Experiment des Isec Forschungslabors für IT-Sicherheit <sup>33</sup> zeigt, dass diese History-Daten auch zur Deanonymisierung genutzt werden können. Anhand der Browser History wurde ermittelt, welche Gruppen bei Xing der Surfer bisher 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 konnten ohne Mithilfe der Surfer ermittelt werden.

Die derzeit einzig wirksame Verteidigung besteht in der Deaktivierung der Surf-History. Im Dialog "Einstellungen" kann man auf dem Reiter "Datenschutz" die Speicherung besuchter Webseiten deaktivieren.

Außerdem können Webseiten in einem Tab die Anzahl der zuvor besucht Webseiten auslesen. Um das zu verhindern, kann man unter *about:config* folgenden Wert setzen:

```
browser.sessionhistory.max_entries = 2
```

Damit kann man aber mit dem Back-Button nur noch eine Seite zurück gehen. :-)

## 4.9 Browsercache

Mit jeder aufgerufenen Webseite wird ein ETag gesendet, welches der Browser im Cache speichert. Wird die Webseite erneut aufgerufen, sendet der Browser zuerst das ETag, um zu erfragen, ob die Seite sich geändert hat. Dieses Tag kann eine eindeutige User-ID enthalten. KISSmetrics<sup>34</sup> verwendete diese Technik, um gelöschte Tracking-Cookies wieder herzustellen.

Ein vollständiges Abschalten des Cache ist nicht empfehlenswert. Man sollte den Cache des Browsers beim Schließen automatisch bereinigen. Außerdem kann man während des Surfens den Cache usw. mit einer Tastenkombination gelegentlich löschen.

---

<sup>32</sup> <http://cseweb.ucsd.edu/users/lerner/papers/ccs10-jsc.pdf>

<sup>33</sup> <http://www.iseclab.org/papers/sonda-TR.pdf>

<sup>34</sup> <http://heise.de/-1288914>

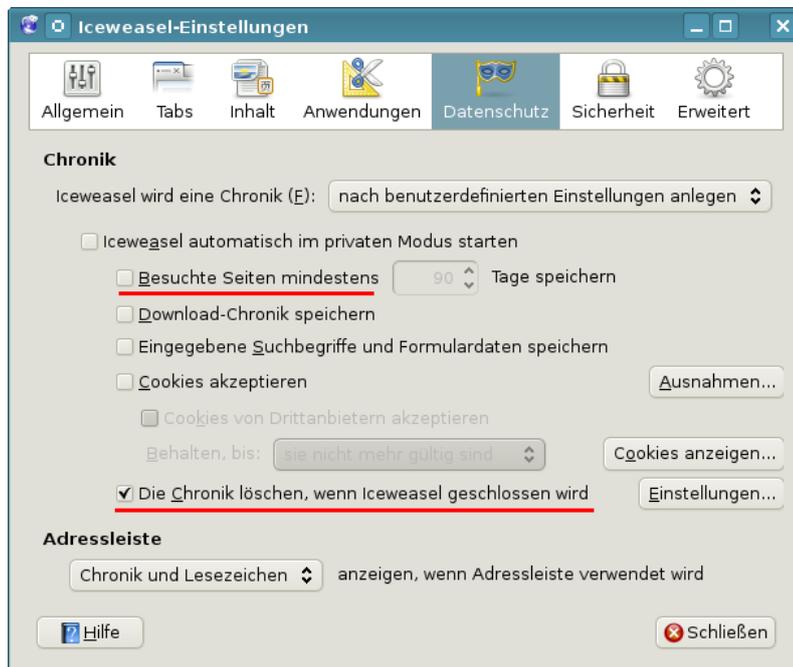


Abbildung 4.13: Speichern der Surf-Chronik deaktivieren

Im Firefox wird der Cache mit weiteren temporären Daten in der *Chronik* zusammengefasst. Die Einstellungen zum Löschen der Chronik findet man unter *Einstellungen* auf dem Reiter *Datenschutz*. Klicken Sie auf den Button *Einstellungen* hinter der Option *Die Chronik löschen, wenn Firefox geschlossen wird*. In dem sich öffnenden Dialog kann man detailliert festlegen, welche Daten beim Schließen des Browsers gelöscht werden sollen.

Während des Surfens kann man die Chronik mit der Tastenkombination STRG-SHIFT-ENTF reinigen oder über den Menüpunkt *Extra - Neueste Chronik löschen*.

Firefox verwendet einen Cache im Hauptspeicher und einen Disk-Cache auf der Festplatte. Der Cache im Hauptspeicher ist mit 64 MB groß genug für eine Surf-Session. Den Disk-Cache kann man deaktivieren und damit auch überflüssige Spuren auf dem Rechner vermeiden, die forensisch sichtbar gemacht werden könnten. Unter *about:config* sind dafür folgende Variablen zu setzen:

```
browser.cache.disk.enable      false
browser.cache.disk_cache_ssl  false
browser.cache.offline.enable  false
media.cache_size               0
```

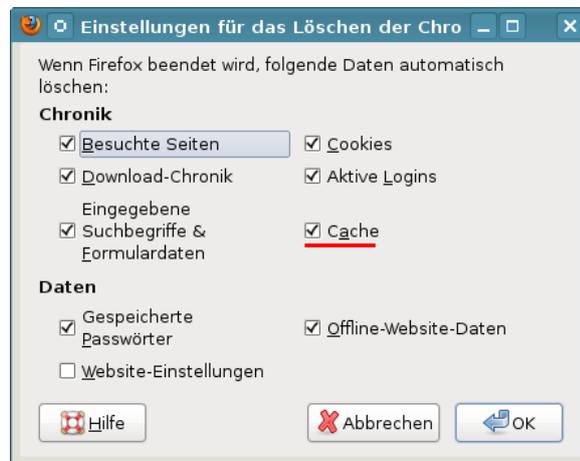


Abbildung 4.14: Cache löschen beim Beenden

## 4.10 Referer

Ein Referer liefert die Information, von welcher Seite der Surfer zu der aufgerufenen Webseite gekommen ist, oder bei der Einblendung von Werbung durch Dritte die Information, welche Seite er gerade betrachtet. Es ist ein sehr gut geeignetes Merkmal für das Tracking mit Werbung, HTML-Wanzen und Like-Button - die Schleimspur im Web.

Die Studie *Privacy leakage vs. Protection measures*<sup>35</sup> 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.

Firefox bietet die Möglichkeit, das Senden des Referers and Drittseiten zu blockieren. Dafür setzt man unter `about:config` folgende Option:

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

Wenn man den Wert auf 2 setzt, dann werden Subdomains als Drittseiten behandelt und es wird auch an Subdomains kein Referer gesendet. Das bringt

<sup>35</sup> <http://w2spconf.com/2011/papers/privacyVsProtection.pdf>

allerdings Probleme bei einigen Websites mit sich. Andererseits schützt es auch gegen Trackingdienste, die sich mit einem DNS-Alias als Subdomain der besuchten Website einschleichen wollen (z.B. WebTrek).

Alternativ kann man die Add-ons **Smart Referer** oder **Referrer Control** installieren. Mit diesen Add-ons können Ausnahmen vom Standardverhalten definiert und spezifische Einstellungen für einzelne Websites konfiguriert werden. Nach der Installation der Add-ons kann man in den Einstellungen das Verhalten anpassen.

Technisch hochentwickelte Datensammler können den Schutz teilweise aushebeln. Google+ und einige Werbenetzwerke übertragen den Referer zusätzlich in URL-Parametern.

## 4.11 Risiko Plugins

Für die Darstellung von Inhalten, die nicht im HTML-Standard definiert sind, kann Firefox Plug-ins nutzen. Populär sind Plug-ins für die Anzeige von PDF-Dokumenten im Browser oder Flash Videos. Die Nutzung dieser Plug-ins ist jedoch ein Sicherheitsrisiko. Firefox bietet eine einfache Möglichkeit, die Gefahr durch Plug-ins zu reduzieren. Man kann unter der Adresse *about:config* die folgende Variable setzen (seit Firefox 19.0 standardmäßig aktiviert):

```
plugins.click_to_play = true
```

Dann werden externe Plug-ins nur aktiviert, wenn der Nutzer es wirklich per Mausklick erlaubt und Drive-By-Download Angriffe sind nicht mehr möglich. Nur Flash-Applets werden weiterhin sofort ausgeführt. Diese Applets können mit dem Add-on NoScript blockiert und individuell mit einem Mausklick freigegeben werden.

### 4.11.1 PDF Reader Plugins

Anwender sind relativ unkritisch gegenüber PDF-Dokumenten. Was soll beim Anschauen schon passieren? Nur wenige Surfer wissen, dass es mit präparierten PDFs möglich ist, den *Zeus-Bot* zu installieren und den Rechner zu übernehmen <sup>36</sup>. 2008 gelang es dem *Ghostnet*, die Rechnersysteme westlicher Regierungen, der US-Regierung und des Dalai Lama mit böartigen PDFs zu infizieren <sup>37</sup>. 2012 gelang es dem Trojaner *MiniDuke*<sup>38</sup>, mit böartigen PDFs in die Computer von Regierungsorganisationen in Deutschland, Israel, Russland, Großbritannien, Belgien, Irland, Portugal, Rumänien, Tschechien und der Ukraine einzudringen. Über eine von Adobe als *nicht kritisch* eingestufte Sicherheitslücke einer überflüssigen PDF-Funktion wurde der Wurm *Win32/Auraax* verteilt <sup>39</sup> ...

---

<sup>36</sup> <http://heise.de/-979037>

<sup>37</sup> <http://www.linux-magazin.de/Heft-Abo/Ausgaben/2010/01/Geisterstunde>

<sup>38</sup> <http://heise.de/-1812971>

<sup>39</sup> <http://heise.de/-990544>

Nach Beobachtung des Sicherheitsdienstleisters Symantec<sup>40</sup> und Scan-Safe<sup>41</sup> erfolgen die meisten Angriffe aus dem Web mit bösartigen PDF-Dokumenten. 2009 wurden für ca. 50% der Angriffe präparierten PDF-Dokumente genutzt (mit steigender Tendenz).

Schutzmaßnahmen:

1. Statt funktionsüberladener Monster-Applikationen kann man einfache PDF-Reader nutzen, die sich auf die wesentliche Funktion des Anzeigens von PDF-Dokumenten beschränken. Die FSFE stellt auf [PDFreaders.org](http://PDFreaders.org)<sup>42</sup> Open Source Alternativen vor.
  - Für Windows werden *Evince* und *Sumatra PDF* empfohlen.
  - Für Linux gibt es *Okular* (KDE) und *Evince* (GNOME, XFCE, Unity).
  - Für MacOS wird *Vindaloo* empfohlen.
2. Wenn die PDF Reader Plugins nicht deinstallierbar sind (keine Administrator-Rechte), können sie im Browser deaktiviert werden. Diese Funktion finden Sie im Addon-Manager unter *Extras* -> *Add-ons*. PDF-Dokumente sollte man vor dem Öffnen zu speichern und nicht im Kontext des Browsers zu betrachten.
3. Außerdem sollte man PDF Dokumenten aus unbekannter Quelle ein ähnliches Misstrauen entgegen bringen, wie ausführbaren EXE- oder PAF-Dateien. Man kann einen Online-PDF-Viewer<sup>43</sup> nutzen, um PDF-Dokumente aus dem Internet zu betrachten ohne den eigenen Rechner zu gefährden.

### 4.11.2 Java-Applets

Es gibt eine Vielzahl von sinnvollen Java-Anwendungen. Im Internet spielt Java aber keine Rolle mehr (im Gegensatz zu Javascript, bitte nicht verwechseln). Trotzdem installiert Oracles Java unter Windows ohne Nachfrage ein Browser-Plugin zum Ausführen von Java-Applets, die in Webseiten eingebettet sein können. Dieses Plug-in ist in erster Linie ein Sicherheitsrisiko und kann zur unbemerkten Installation von Trojanern genutzt werden.<sup>44 45 46</sup>

Der (Staats-) Trojaner der italienischen Firma *HackingTeam*<sup>47</sup> wird beispielsweise mit einer sauber signierten JAR-Datei auf dem Zielsystem installiert. Der Trojaner belauscht Skype, fängt Tastatureingaben ab, kann die Webcam zur Raumüberwachung aktivieren und den Standort des Nutzers ermitteln.

---

<sup>40</sup> <http://heise.de/-981631>

<sup>41</sup> [http://www.scansafe.com/downloads/gtr/2009\\_AGTR.pdf](http://www.scansafe.com/downloads/gtr/2009_AGTR.pdf)

<sup>42</sup> <http://www.pdfreaders.org/index.de.html>

<sup>43</sup> <http://view.samurajdata.se>

<sup>44</sup> <http://heise.de/-1485195>

<sup>45</sup> <http://heise.de/-1677249>

<sup>46</sup> <http://heise.de/-1780850>

<sup>47</sup> <http://heise.de/-1671203>

Als Schutz wird häufig die komplette Deinstallation von Java empfohlen (BSI<sup>48</sup>, DHS<sup>49</sup>, Fefe<sup>50</sup>). Das ist Bullshit und nur sinnvoll, wenn man keine Java-Programme nutzt. Anderenfalls ist die komplette Deinstallation von Java eine unnötige Einschränkung für sinnvolle Anwendungen.

- Aktuelle **Linux** Distributionen verwenden in der Regel OpenJDK-6/7. Diese Java-JRE installiert KEIN Browser Plug-in. Es besteht also auch keine Gefahr, durch bösartige Java-Applets aus dem Internet den Rechner zu verseuchen.
- Unter **Windows** bietet die aktuelle Version von Oracles Java die Möglichkeit, die Plug-ins für alle Browser unter *Systemsteuerung - Programme - Java* zu deaktivieren (Bild 4.15).

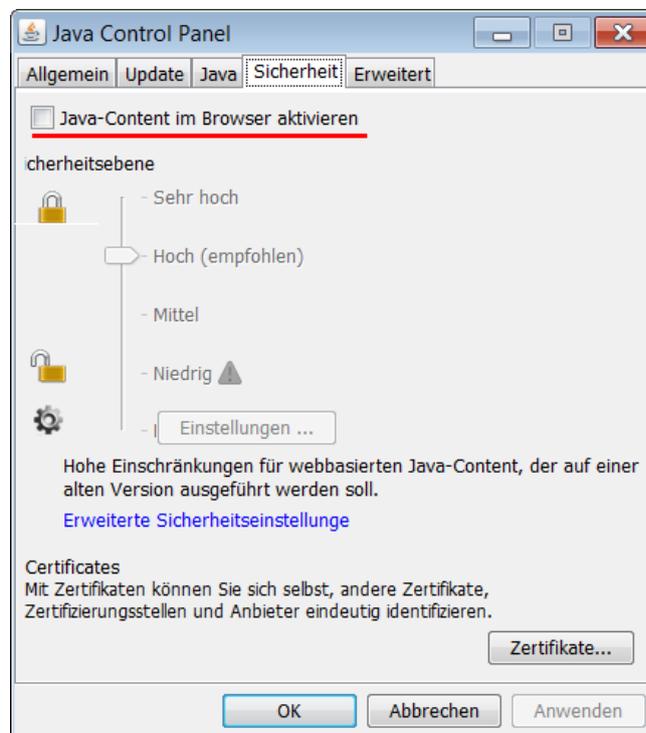


Abbildung 4.15: Java Plug-in für alle Browser deaktivieren

### 4.11.3 Flash-Applets und Flash-Videos

Flash Applets sind ein Sicherheits- und Privacyrisiko. Diese Applets können umfangreiche Informationen über den Browser auslesen (installierte Schrift-

<sup>48</sup> [https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2013/Krit\\_Schwachstelle\\_Java-7-10\\_11012013.html](https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2013/Krit_Schwachstelle_Java-7-10_11012013.html)

<sup>49</sup> <http://www.nbcnews.com/technology/technology/us-warns-java-software-security-concerns-escalate-1B7938755>

<sup>50</sup> <https://blog.fefe.de/?ts=ae0f1f75>

arten, Betriebssystem, Kernelversion) und daraus einen genauen Fingerprint zum Tracking berechnen. Die Studie *Dusting the Web for Fingerprinters* der KU Leuven (Belgien) hat bei 1% der TOP 10.000 Webseiten Flash-basiertes Fingerprinting des Browsers nachgewiesen.

Die italienische Firma Hacking Team verwendete mindestens drei Bugs im Flash Player für 0day Exploits<sup>51</sup>, um ihre Spionage Software als Drive-by-Download auf den Computern der Opfer zu installieren. Auch andere staatliche und kriminelle Trojaner nutzen mit Sicherheit Bugs im Flash Player.

### Verwendung von Flash vermeiden

1. Das Firefox Add-on **VideoDownloadHelper**<sup>52</sup> kann man Videos von vielen Websites herunter laden und in ein gebräuchlicheres Format für Mediaplayer konvertieren. Wer noch keinen passenden Mediaplayer installiert hat, kann den VideoLAN Player nutzen (VLC-Player), der für alle Betriebssysteme zur Verfügung steht.

Für die volle Funktionalität benötigt das Add-on die Bibliothek *Libav* für die Konvertierung von Videos. Diese Bibliothek ist zusätzlich zu installieren:

- Für Windows findet man ein Installationspaket auf der Webseite <http://www.downloadhelper.net/install-converter3.php>
- Debian Nutzer können *Libav* aus dem Repository installieren:

```
sudo aptitude install libav-tools libavcodec-extra
libavcodec55 libavformat55
```

Nutzer von Debian *wheezy* können die Backports nutzen:

```
sudo aptitude install -t wheezy-backports libav-tools
libavcodec-extra libavcodec55 libavformat55
```

- Für Ubuntu installiert man die nötigen Pakete mit:

```
sudo apt-get install libav-tools libavcodec-extra
libavformat-extra-54
```

- Unter MacOS ist ein Terminal zu öffnen, um mit Homebrew die *Libav* zu installieren:

```
brew install libav
```

2. Web Videos können mit Hilfe von Download Sites wie KeepVid<sup>53</sup> oder ShareTube<sup>54</sup> gespeichert und mit einem Mediaplayer abgespielt werden.

<sup>51</sup> <http://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flash-player-flaws-more-pocs-found-in-hacking-team-leak/>

<sup>52</sup> <https://addons.mozilla.org/de/firefox/addon/video-downloadhelper>

<sup>53</sup> <http://keepvid.com>

<sup>54</sup> <http://www.share-tube.de/flvdownload.php>

### Privacy-freundliche Konfiguration für Adobe Flash-Player

Wenn man auf Flash nicht verzichten möchte, kann man mit der Konfigurationsdatei *mms.cfg* ein privacy-freundlicheres Verhalten für den Adobe Flash-Player erzwingen und einige Trackingfeatures deaktivieren. Die Datei ist in folgenden Verzeichnissen zu speichern:

```
Windows (32Bit): %Windir%\System32\Macromed\Flash\  
Windows (64Bit): C:\Windows\SysWOW64\Macromed\Flash\  
MacOS:          /Library/Application Support/Macromedia/  
Linux:          /etc/adobe/
```

Folgende Optionen empfehle ich für die Konfigurationsdatei *mms.cfg*:

- Deaktivierung von Mikrophon und Lautsprecher sowie Abschaltung des Auslesens der Schriftarten erschweren Fingerprinting des Browsers:

```
AVHardwareDisable=1  
DisableDeviceFontEnumeration=1
```

- Blockierung der Speicherung von Cookies und Drittseiten-Content verhindert Tracking:

```
ThirdPartyStorage=0  
LocalStorageLimit=1  
AssetCacheSize=0
```

- Up- und Download von Dateien mit der Scripting API wird blockiert:

```
FileDownloadDisable=1  
FileUploadDisable=1  
LocalFileReadDisable=1
```

- Für die gemeinsame Nutzung von SWF-Dateien in einer Sandboxen wird die exakte Übereinstimmung der Domains erzwungen und die lockeren Einstellungen von Flash Player Version 6.0 werden verboten:

```
LegacyDomainMatching=0
```

- Deaktivierung von Sockets verhindert die Deanonymisierung durch Umgehung der Proxy-Einstellungen des Browsers bei der Nutzung von Anonymisierungsdiensten wie JonDonym oder Tor:

```
DisableSockets=1
```

Damit werden nicht alle Fingerprinting-Features deaktiviert. Betriebssystem, Kernel, Bildschirm und Systemzeit sind weiterhin auslesbar, aber es ist eine deutliche Verbesserung.

#### 4.11.4 Weitere Anwendungen

Neben PDF-Dokumenten können auch alle anderen Dokument-Typen für Drive-by-Donwload Angriffe verwendet werden. Um diese zu unterbinden, sollte man externe Anwendungen für Dateien nur nach Bestätigung durch den Anwender öffnen lassen. Anderenfalls können Bugs in diesen Anwendungen automatisiert genutzt werden.

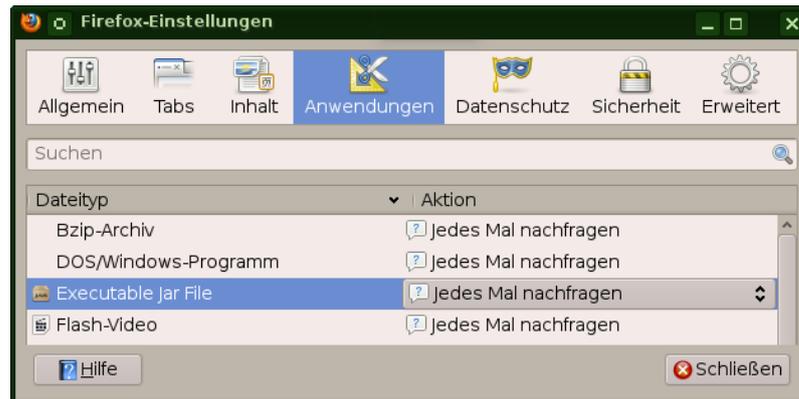


Abbildung 4.16: Externe Anwendungen nur auf Nachfrage öffnen

Auf dem Reiter *Anwendungen* im Dialog *Einstellungen* können die Helper-Applications wie im Bild 4.16 für jeden Dateityp auf *„Jedes Mal nachfragen“* gesetzt werden. Diese Einstellungen sind natürlich nur sinnvoll, wenn der Surfer kritisch hinterfragt, ob die Aktion wirklich dem entspricht, was er erwartet. Wer unkritisch bei jeder Nachfrage auf *Öffnen* klickt, muss sich nicht wundern, wenn sein Computer infiziert wird.

#### 4.11.5 H.264 Plug-in und Adobe Primetime deaktivieren

Der H.264-Codec für WebRTC und HTML5 Videos wird als Closed Source Plug-in von Cisco herunter geladen und automatisch installiert. Man kann die automatische Installation des Plug-in verhindern, wenn man unter *about:config* folgende Werte auf *false* setzt:

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

Adobe Primetime ist ein Plug-in zur Wiedergabe von DRM-geschützten Inhalten. Es ist im Firefox 38.0 für Windows standardmäßig enthalten. Ein Plug-in von Adobe ist etwas, was ich aus Sicherheitsgründen auf keinen Fall in meinem Browser haben möchte. Mozilla beschreibt in einem Artikel <sup>55</sup>, wie man das Plug-in entfernt. Unter *Einstellungen* in der Sektion *Inhalt* ist die Option *Inhalte mit DRM-Kopierschutz wiedergeben* zu deaktivieren.

<sup>55</sup> <https://support.mozilla.org/de/kb/drm-inhalte-in-firefox-ansehen>

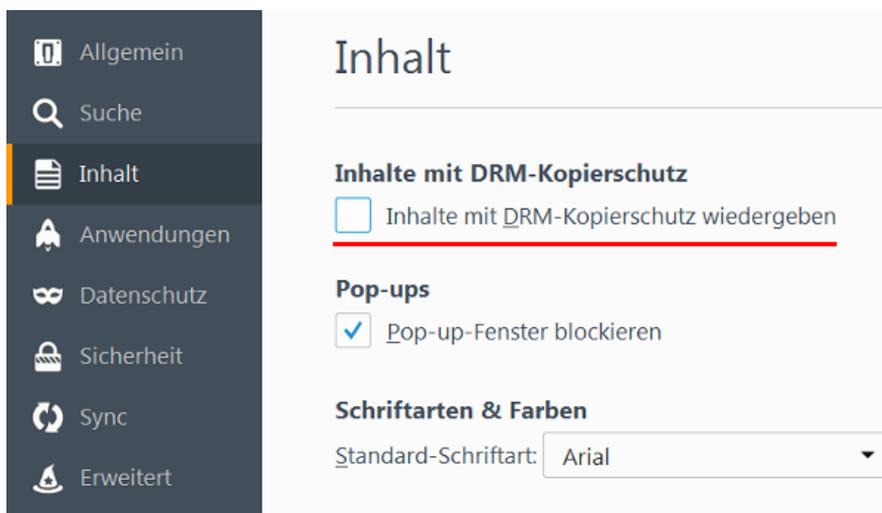


Abbildung 4.17: Adobe Primetime deinstallieren

## 4.12 HTTPS-Verschlüsselung nutzen

Viele Websites bieten HTTPS-Verschlüsselung an. Diese sichere Datenübertragung wird häufig nicht genutzt. Mit wenig Konfigurationsaufwand lässt sich die Nutzung von HTTPS für eine definierte Liste von Websites erzwingen.

Firefox enthält eine *HSTS preload list*<sup>56</sup> mit mehr als 1200 Domains, für die HTTPS ohne weitere Konfiguration erzwungen wird. Webmaster können ihre Websites auf der Seite HSTS Preload Submission<sup>57</sup> eintragen, wenn sie die Voraussetzungen erfüllen.

### NoScript Enforce HTTPS

NoScript Enforce HTTPS ist einfach konfigurierbar, kann aber nur *http://* durch *https://* für eine Liste von Websites ersetzen. Die Liste muss man per Hand erstellen. Im Dialog *Einstellungen* findet man auf dem Reiter *Erweitert* unter *HTTPS* eine editierbare Liste von Websites.

Standardmäßig ist die Liste leer. Wer das Webinterface eines E-Mail Providers nutzt, sollte die Domain hier eintragen. Außerdem sollte man die Webseite der Bank eintragen, wenn man Online-Banking nutzt und die Webseite nicht in HTTPSEverywhere oder der *HSTS preload list* enthalten ist.

<sup>56</sup> <https://mxr.mozilla.org/mozilla-central/source/security/manager/boot/src/nsSTSPreloadList.inc>

<sup>57</sup> <https://hstspreload.appspot.com/>

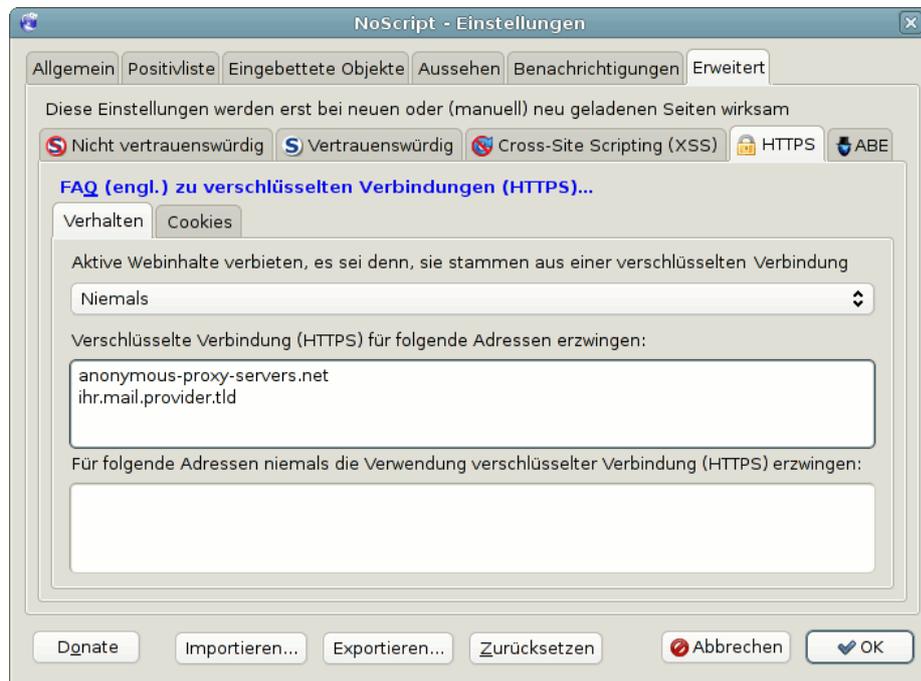


Abbildung 4.18: Einstellungen für NoScript STS

### HTTPS-Everywhere

Das Firefox Add-on HTTPS-Everywhere<sup>58</sup> der EFF.org kann auch komplexe Umschreibungen der URLs realisieren, wie es beispw. für Wikipedia notwendig ist. Das Add-on bringt bereits über 2500 Regeln für häufig genutzte Webseiten mit. Die Konfiguration eigener Regeln ist aufwendiger als bei NoScript und erfolgt über XML-Dateien.

Bei HTTPS-Everywhere sind Regeln standardmäßig deaktiviert, wenn der Server ein SSL-Zertifikat von CAcert.org nutzt (z.B. www.ccc.de) Wenn Sie das Root-Zertifikat von CAcert.org im Browser importiert haben, dann können Sie diese Regeln in den Einstellungen von HTTPS-Everywhere mit Klick auf das Kreuz aktivieren (Bild 4.19).

## 4.13 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 routinemäßig ausgeführt werden, schreibt die<sup>59</sup>

<sup>58</sup> <https://www.eff.org/https-everywhere>

<sup>59</sup> <https://eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl>

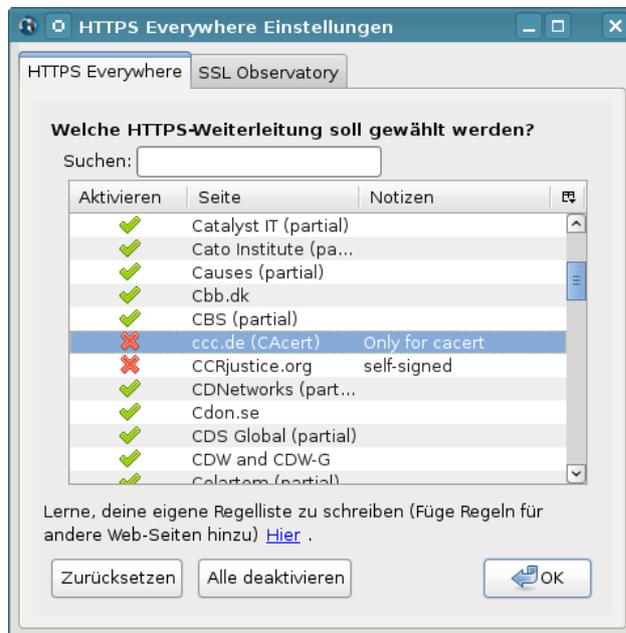


Abbildung 4.19: Einstellungen für Https-Everywhere

*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, z.B. die Firma ClearTrail oder die deutsche Firma Utimaco. Einen Auszug aus dem Datenblatt *Utimaco LIMS* zeigt Bild 4.20.

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 von Adi Shamir:

*I think you will see more and more events like this, where a CA under*

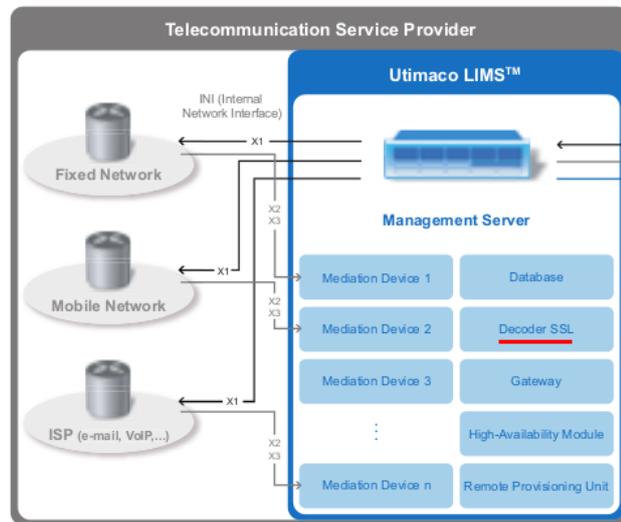


Abbildung 4.20: Datenblatt Ultimaco LIMS

*pressure from a government will behave in strange ways.*

Im Juni 2014 signierte die staatliche indische Certification Authority (NIC) gefälschte SSL-Zertifikate für Google Dienste und Yahoo!. 45 gefälschte Zertifikate wurden nachgewiesen. Ob es um eine staatliche Überwachung, einen Hackerangriff oder einen Konfigurationsfehler(?) handelt, ist unklar.<sup>60</sup>

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 SSL Interception.

Kriminelle Subjekte haben ebenfalls nachgewiesen, dass sie für man-in-the-middle Angriffe auf die SSL-Verschlüsselung gültige Zertifikate verwenden können (bspw. beim Angriff auf das Bitcoin Forum). Man kann sich so einfach als Unberechtigter ein gültiges SSL-Zertifikat für einen Server ausstellen zu lassen, wenn man die richtigen Mail-Account kontrolliert. Für die Ausstellung Domain-validierte SSL-Zertifikate werden die E-Mail Adressen *webmaster-domain.tld*, *postmasterdomain.tld*, *ssladmindomain.tld*, *ssladministratoromain.tld* u.a.m. u.a. akzeptiert. Eine unverschlüsselte E-Mail mit einem Verification Link an eine der genannten E-Mail Adressen ist die einzige Prüfung auf

<sup>60</sup> <http://heise.de/-2255992>

Rechtmäßigkeit durch die CAs.

Die Software für einen man-in-the-middle Angriff mit den gefälschten Zertifikaten gibt es auch als Open Source, z.B. den mitm-proxy<sup>61</sup> der Stanford University oder dsniff<sup>62</sup>.

#### 4.13.1 Verbesserung der Vertrauenswürdigkeit von HTTPS

Es gibt einige Möglichkeiten, die Vertrauenswürdigkeit der HTTPS-Verschlüsselung zu verbessern und Angriffe mit falschen Zertifikaten zu erschweren.

- **Zertifikate speichern:** Beim ersten Besuch der Webseite wird das SSL-Zertifikat gespeichert. Bei späteren Besuchen wird das aktuelle Zertifikat mit dem gespeicherten Zertifikat verglichen. Bei seltsamen Abweichungen wird eine Warnung angezeigt, die der Surfer allerdings bewerten muss.
- **Vergleich mit Anderen:** Beim Besuch einer HTTPS-verschlüsselten Webseite wird das Zertifikat mit den Ergebnissen an anderen Punkten der Welt verglichen. Wenn alle Teilnehmer des Netzes das gleiche Zertifikat sehen, ist es wahrscheinlich Ok. Dieser Vergleich kann mit einer zeitlich begrenzten Speicherung kombiniert werden.

Obwohl die Idee auf den ersten Blick einleuchtend ist, gibt es einige Probleme bei großen Serverfarmen wie Google, Facebook, Amazon, PayPal... Diese Serverfarmen verwenden nicht immer ein einheitliches Zertifikat. Das führt zu Verwirrung bei einem externen Beobachter und zu inkonsistenten Ergebnissen der Notary Server.

- **Certificate Pinning:** Nur der Betreiber einer Webseite kann wirklich wissen, welche Zertifikate gültig sind. Diese Information muss unabhängig vom Webserver verteilt und durch die Browser ausgewertet werden. Das ist ein besserer Weg, als der Vergleich mit externen Beobachtern oder der Speicherung in einer lokalen Datenbank.
  - Nur der Betreiber einer Webseite kann wirklich wissen, welche Zertifikate gültig sind. Diese Information muss unabhängig vom Webserver verteilt und durch die Browser ausgewertet werden. Das ist ein besserer Weg, als der Vergleich mit externen Beobachtern oder der Speicherung in einer lokalen Datenbank.
  - DANE ist ein Standard, der im Januar 2014 verabschiedet wurde. Die Fingerprints der SSL-Zertifikate werden vom Webmaster im TLSA-Record via DNSSEC verteilt. Inzwischen gibt es einige Webseiten, die DANE anbieten. Um die Zertifikate zu verifizieren benötigt man ein zusätzliches Browser Add-on (z.B. den DNSSEV/TLSA-Validator), da die aktuellen Webbrowser das (noch) nicht selbst können.

<sup>61</sup> <http://crypto.stanford.edu/ssl-mitm/>

<sup>62</sup> <http://www.monkey.org/~dugsong/dsniff/>

### 4.13.2 Firefox Add-ons

Ein paar kleine Erweiterungen für Firefox, welche die Vertrauenswürdigkeit der Zertifikate bei der Nutzung von HTTPS-verschlüsselten Verbindungen deutlich erhöhen können.

#### DNSSEC/TLSA-Validator

DNSSEC/TLSA-Validator<sup>63</sup> überprüft die Zertifikate einer Webseite anhand der Fingerprints, die vom Webmaster im TLSA-Record in DNSSEC hinterlegt wurden. Der verwendete Standard DANE wurde im Januar 2014 verabschiedet und die ersten Anbieter unterstützen diese Verifikation, die unabhängig von einer kompromittierbaren Certification Authority arbeitet.

Es werden zwei zusätzliche Icons in der Adresszeile angezeigt. Normalerweise wird man folgendes Bild mit zwei grauen Icons sehen, weil die Webseite DANE noch nicht für die Validierung der Zertifikate unterstützt:



Wenn ein TLSA-Record im DNSSEC vom Webmaster hinterlegt wurde, dann sieht man zwei grüne Icons, wenn alles Ok ist:



Wenn eines der beiden Icons orange ist, dann läuft etwas schief und man sollte dem SSL-Zertifikat NICHT vertrauen.

Hinweis: dieses Add-on funktioniert (noch) nicht mit dem TorBrowser oder JonDoFox!

#### HTTPSEverywhere

HTTPS-Everywhere<sup>64</sup> kann das SSL-Observatory der EFF.org nutzen. Wenn man diese Funktion in den Einstellungen des Add-on aktiviert, werden die SSL-Zertifikate der besuchten Webseiten an das SSL-Observatory gesendet. Ist das Zertifikat nicht ok, erhält man eine Warnung. Es wird eine Datenbasis von weltweit verteilten Nutzern genutzt.

HTTPSEverywhere ignoriert die Proxy-Einstellungen von Firefox. Wenn man einen Proxy konfiguriert hat, dann muss man unter *about:config* auch die folgenden Einstellungen für HTTPSEverywhere per Hand anpassen:

```
extensions.https_everywhere._observatory.proxy_type = direct | socks | http
extensions.https_everywhere._observatory.proxy_host = <IP oder Hostname>
extensions.https_everywhere._observatory.proxy_host = <Port des Proxy>
```

Hinweis: Im TorBrowser und beim JonDoFox muss man sich nicht darum kümmern, da das Add-on fester Bestandteil dieser beider Browser ist und die Proxy-Einstellungen vom TorBrowser bzw. JonDoFox mit verwaltet werden.

<sup>63</sup> <https://www.dnssec-validator.cz/pages/download.html>

<sup>64</sup> <https://www.eff.org/https-everywhere>

## Perspectives

Perspectives<sup>65</sup> vergleicht SSL-Zertifikate mit den bei Notary Servern bekannten Zertifikaten. Wenn alle Notary-Server das gleiche Zertifikat über einen längeren Zeitraum sehen, ist es wahrscheinlich gültig. Leider gibt es noch nicht viele, international verteilte Notary Server. Alle standardmäßig im Add-on enthaltenen Server werden vom MIT bereit gestellt.

Aufgrund der nicht immer eindeutigen Resultate und der Performance der Notary Server ist Perspectives nicht unbedingt für eine ständige Validierung aller SSL-Zertifikate geeignet. Der Server awxcnx.de ist im Moment nur bei der Hälfte der Notary Server bekannt. Das führt zu einem Fehler bei Perspectives, obwohl eigentlich alles Ok ist.

Ich empfehle daher die Abfrage der Notarys bei Bedarf (wenn man ein Zertifikat genauer prüfen möchte). Dafür sind die Einstellungen in den Preferences wie im Bild 4.21 zu setzen.

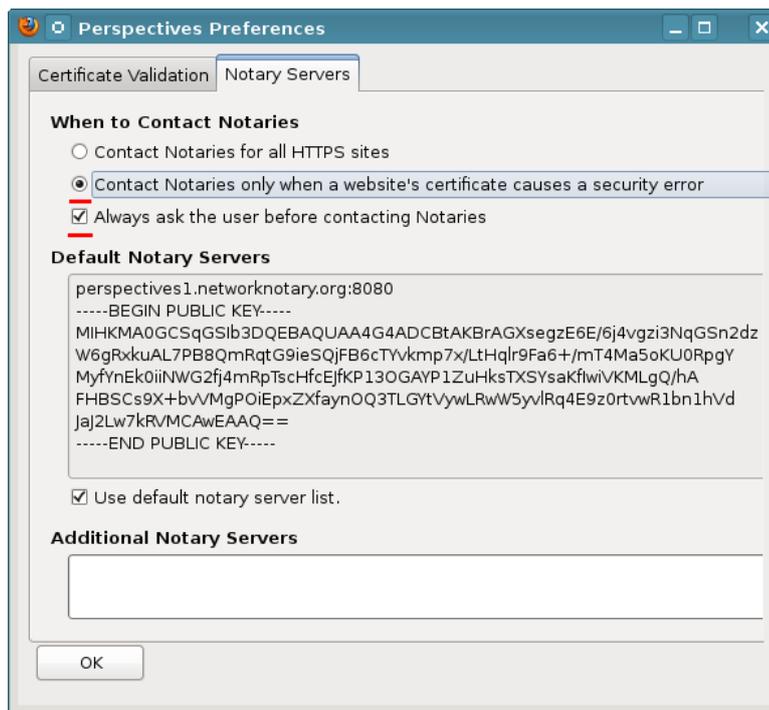


Abbildung 4.21: Perspectives Konfiguration

Zukünftig kann man mit einem Klick der rechten Maustaste auf das Perspectives-Symbol in der Statusleiste einen Check des Zertifikates der Webseite erzwingen und sich die Notary Results anzeigen lassen.

<sup>65</sup> <https://addons.mozilla.org/en-US/firefox/addon/perspectives/>

### 4.13.3 OCSP abschalten

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.

OCSP ist 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` können das automatisiert ausführen. OCSP bringt also kaum Sicherheitsgewinn.<sup>66</sup>

Einige CAs nutzen die OCSP-Anfragen zum Tracking des Surfers mit Cookies, wie der folgende Mitschnitt eines OCSP-Request zeigt:

```
POST http://ocsp2.globalsign.com/gsorganizationvalg2 HTTP/1.1
Host: ocsp2.globalsign.com
User-Agent: Mozilla/5.0 (...) Gecko/20130626 Firefox/17.0 Icedragon/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
```

(Aktuelle Firefox Versionen akzeptieren keine OCSP-Cookies mehr, sind für das Tracking also nicht mehr anfällig. Bei anderen Browsern ist das Thema noch relevant.)

Mit der OCSP-Anfrage erhält die CA außerdem die Information, von welcher IP-Adresse die SSL-geschützte Webseite bzw. Mailserver aufgerufen wurde. Da die OCSP-Anfrage und Antworten unverschlüsselt übertragen werden, kann auch ein *Lauscher am Draht* diese Informationen abgreifen.

Im Gegensatz zu anderen Browsern wie Google Chrome ist OCSP in Firefox standardmäßig aktiviert. In den Einstellungen kann man in der Sektion *Erweitert* auf dem Reiter *Zertifikate* die überflüssige Validierung von SSL-Zertifikaten mit OCSP abschalten.

### 4.13.4 Tracking via SSL 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 diese Session eindeutig ist, kann sie für das Tracking genutzt werden. Das Verfahren ist im

<sup>66</sup> <http://www.thoughtcrime.org/papers/ocsp-attack.pdf>

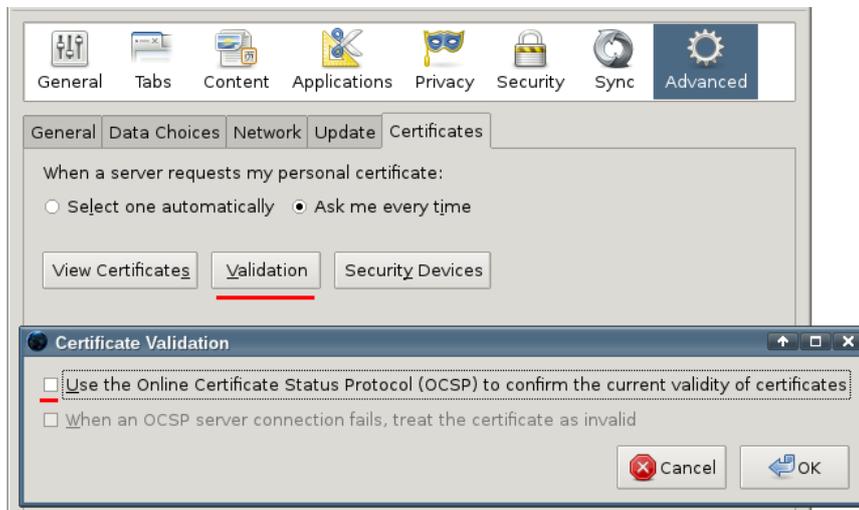


Abbildung 4.22: OCSP deaktivieren

RFC 5077<sup>67</sup> beschrieben.

Die SSL-Session-ID kann von nahezu allen Webservern für das Tracking der Zugriffe genutzt werden. IBM WebSphere, Apache und andere bieten eine API für den Zugriff auf die SSL Session-ID. Einige Webshops sind für das Tracking via SSL Session-ID vorbereitet (z.B. die *xtcModified eCommerce Shopsoftware*<sup>68</sup>). Dieses Tracking-Verfahren ist so gut wie nicht nachweisbar, da es vollständig durch den Webserver realisiert wird und keine Spuren im Browser hinterlässt.

Gegen das Tracking via SSL Session Identifiers kann man sich ab **Firefox 36.0** schützen, indem man unter *about:config* eine neue Variable vom Type *Boolean* anlegt:

```
security.ssl.disable_session_identifiers = true
```

#### 4.13.5 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. Das verhindert ein Downgrade auf unverschlüsselte HTTP-Verbindungen.

<sup>67</sup> <https://tools.ietf.org/html/rfc5077>

<sup>68</sup> [http://www.modified-shop.org/wiki/SESSION\\_CHECK\\_SSL\\_SESSION\\_ID](http://www.modified-shop.org/wiki/SESSION_CHECK_SSL_SESSION_ID)

S. Greenhalgh hat ein Verfahren publiziert, wie man HSTS für das Tracking von Surfern verwenden kann<sup>69</sup>. Es steht eine Testseite für HSTS Super-Cookies bereit, die dieses Verfahren demonstriert. Ob man HSTS im Browser deaktiviert, um sich gegen ein bisher nur theoretisch relevantes Trackingverfahren zu schützen, oder ob man HSTS aktiviert, um sich gegen *ssl-stripe* Angriffe zu schützen (Standard im Firefox), ist also eine Wahl zwischen Skylla und Charybdis.

Meine Überlegungen dazu:

- In der Regel nutzt man nur eine begrenzte Anzahl von Websites regelmäßig, bei denen sensitive Informationen durch SSL-Verschlüsselung wirklich geschützt werden müssen (E-Mail Provider, Website der Bank, Diskussionsforen, bevorzugte Suchmaschine....). Mit der HSTS preload list, NoScript oder HTTPSEverywhere kann man SSL-Verschlüsselung für diese Websites erzwingen und ist damit auch ohne HSTS gegen *ssl-stripe* Angriffe geschützt.
- Unter der Adresse *about:config* kann man folgende Variable setzen:

```
privacy.clearOnShutdown.siteSettings = true
```

Damit werden beim Schließen des Browsers alle gespeicherten HSTS-Werte gelöscht und ein langfristiges Tracking wird verhindert. Während einer Surf-Session ist der HSTS-Schutz aktiv.

- Innerhalb einer Surf-Session kann man HSTS-Cookies mit der Tastenkombination STRG-SHIFT-ENTF löschen. Zum Löschen der HSTS-Werte ist unter Details die Option *Website-Einstellungen* zu aktivieren.

#### 4.13.6 Schwache SSL-Cipher deaktivieren

Die SSL-Verschlüsselung ist ein komplexer Standard, der über Jahre gewachsen ist. Neben aktuell starken Algorithmen sind auch schwache kryptografische Verfahren enthalten, die aus Kompatibilitätsgründen unterstützt werden:

1. Das Protokoll SSLv3 ist geknackt. Mozilla hat SSLv3 in Firefox 34 standardmäßig abgeschaltet.
2. Die RC4-Cipher sind schwach und genügen aktuellen Anforderungen nicht mehr. Laut aktuellen Empfehlungen der IETF dürfen RC4-Cipher nicht mehr genutzt werden. Nach Ansicht von J. Appelbaum ist die NSA in der Lage, RC4 zu knacken.<sup>70</sup>. Aufgrund der Performance wird die RC4-Verschlüsselung von 1/3 der großen Webseiten bevorzugt genutzt (z.B. Twitter und EBay), wenn der Browser es unterstützt. Starke Alternativen werden nur genutzt, wenn RC4 im Browser deaktiviert wurde.
3. Schlüsseltausch mit DSS kann höchstens 1024 Bit DH-Keys nutzen. Das ist nach aktueller Einschätzung nicht mehr ausreichend sicher.

<sup>69</sup> <http://heise.de/-2511258>

<sup>70</sup> <http://heise.de/-2041383>

4. Schlüsseltausch mit DHE ist anfällig für die Logjam Attack<sup>71</sup>. Dieser TLS Downgrade Angriff ist nur möglich, wenn der HTTPS-Server schlecht konfiguriert ist, das betrifft aber immerhin 8,4% der SSL-Webseiten.
5. Insecure Renegotiation wird seit 2009 als schwiegender Bug des SSL-Protokoll eingestuft. Tools zum Ausnutzen der Insecure Renegotiation gibt es auch als OpenSource (z.B. dsniff). Ein Angreifer kann Login Credentials stehlen ohne die SSL-Verschlüsselung knacken zu müssen.<sup>72</sup>
6. Eine SSL-verschlüsselte Webseite sollte nur SSL-verschlüsselte Inhalte darstellen. Unverschlüsselte Elemente sollten nicht geladen werden, um die Sicherheit nicht zu kompromittieren. Firefox blockiert unverschlüsselte aktive Inhalte, lässt Bilder aber zu.
7. FIPS-kompatible Cipher sind per Design schwach ausgelegt und in Firefox standardmäßig deaktiviert.
8. Mit einer TLS Downgrade Attack <sup>73</sup> kann ein Angreifer als man-in-the-middle die Verwendung starker Algorithmen verhindern und eine schwache Verschlüsselung erzwingen (z.B. SSLv3 mit RC4), wenn Browser und Webserver diese schwachen Algorithmen als Alternative unterstützen. Dieser Angriff ist schwer erkennbar.

Zur Verbesserung der Sicherheit kann man unter der Adresse *about:config* folgende Variablen anpassen. Das Ergebnis kann man im Browser Test von Qualsys SSL Labs überprüfen.<sup>74</sup>

- SSLv3 deaktivieren (seit Firefox 34.0 standardmäßig deaktiviert)

```
security.tls.version.min = 1
```

- RC4-Cipher deaktivieren:

```
security.ssl3.ecdhe_ecdsa_rc4_128_sha = false
security.ssl3.ecdhe_rsa_rc4_128_sha   = false
security.ssl3.rsa_rc4_128_md5         = false
security.ssl3.rsa_rc4_128_sha         = false
```

- 3DES-Cipher deaktivieren (in Firefox 36.0 teilweise deaktiviert):

```
security.ssl3.dhe_rsa_des_ede3_sha   = false
security.ssl3.ecdhe_rsa_des_ede3_sha = false
security.ssl3.rsa_des_ede3_sha       = false
```

- Cipher mit DSS Schlüsseltausch deaktivieren:

```
security.ssl3.dhe_dss_aes_128_sha    = false
security.ssl3.dhe_dss_aes_256_sha    = false
```

<sup>71</sup> <https://weakdh.org>

<sup>72</sup> <https://www.verbraucher-sicher-online.de/news/fehlerhaftes-design-im-wichtigsten-verschlusselungsprotokoll-fuer-angriffe-nutzbar>

<sup>73</sup> <http://jbp.io/2013/07/07/tls-downgrade/>

<sup>74</sup> <https://www.ssllabs.com/ssltest/viewMyClient.html>

- Cipher mit DHE Schlüsseltausch deaktivieren:

```
security.ssl3.dhe_rsa_aes_128_sha      = false
security.ssl3.dhe_rsa_aes_256_sha     = false
```

- Insecure Renegotiation verbieten (PayPal.com, EBay.de u.a. funktionieren dann nicht mehr):

```
security.ssl.require_safe_negotiation  = true
security.ssl.treat_unsafe_negotiation_as_broken = true
```

- Mixed Content verbieten (keine unverschlüsselten Inhalte in HTTPS-Webseiten):

```
security.mixed_content.block_display_content = true
security.mixed_content.block_active_content = true
```

Hinweis: Für Nutzer von Anonymisierungsdiensten (Tor, JonDonym) empfehle ich NICHT, die Einstellungen zur SSL-Verschlüsselung zu verändern, da individuelle Einstellungen beim SSL-Handshake die Anonymität gefährden können.

### Probleme mit sicheren SSL-Einstellungen

Einige Webseiten lassen sich mit diesen Einstellungen nicht via HTTPS aufrufen. Man erhält nur eine leere Seite mit einer Fehlermeldung:

Fehlercode: `ssl_error_no_cypher_overlap`

Wenn man diesen Fehler erhält, kann man als erstes kann man RC4 Cipher zulassen (2). Wenn es nicht reicht, dann kann man SSLv3 freigeben (1).

Fehlercode: `ssl_error_unsafe_negotiation`

Wenn dieser Fehler auftritt, dann müsste man Insecure Renegotiation zulassen (5) oder darauf verzichten, die Webseite zu nutzen.

Wenn man unsichere SSL-Einstellungen zulassen muss, dann sollte man sich darüber im klaren sein, dass die Verschlüsselung nicht mehr sicher ist (nach dem Stand der zivilen Forschung). Man sollte sich überlegen, welche privaten Daten man dieser schwachen Verschlüsselung anvertrauen will.

In diesem Zusammenhang möchte ich ohne weiteren Kommentar auf die Antwort der Bundesregierung auf eine Anfrage zu den technischen Möglichkeiten des BND vom Mai 2012 verweisen:

*Frage: Ist die eingesetzte Technik auch in der Lage, verschlüsselte Kommunikation (etwa per SSH oder PGP) zumindest teilweise zu entschlüsseln und auszuwerten?*

*Antwort: Ja, die eingesetzte Technik ist grundsätzlich hierzu in der Lage, je nach Art und Qualität der Verschlüsselung.*

## 4.14 Starke Passwörter nutzen

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 unter der Tastatur "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 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 0,16 Euro. Eine 8-stellige Kombination hat man mit 400 Euro wahrscheinlich und mit 850 Euro sicher geknackt. Man sollte mindestens 10...12 Zeichen verwenden. (Stand: 2011)
- Warum sollte man nicht das gleiche Passwort für viele Logins verwenden? Diese Frage beantwortet der Hack von Anonymous gegen HBGary. Den Aktivisten von Anonymous gelang es, Zugang zur User-Datenbank des Content Management Systems der Website zu erlangen. Die Passwörter konnten geknackt werden. Die Passwörter wurden vom Führungspersonal für weiterer Dienste genutzt: E-Mail, Twitter und Linked-In. Die veröffentlichten 60.000 E-Mails waren sehr peinlich für HBGary <sup>75</sup>.

Das Add-on **PwdHash**<sup>76</sup> vereinfacht den Umgang mit Passwörtern. Wenn man vor der Eingabe des Passwortes die Taste F2 drückt oder mit einem doppelten @@ beginnt, wird es in einen Hash aus dem Master Passwort und der Domain umgerechnet. Das Ergebnis der Berechnung ist eine 10-stellige zufällige Kombination von Buchstaben und Zahlen und wird als Passwort gesendet. Damit ist es möglich, ein merkbares Master-Passwort für alle Sites zu nutzen, bei denen PwdHash funktioniert. Wichtig ist, dass die Domains der Webseiten für die Eingabe und die Änderung der Passwörter identisch sind.

PwdHash schützt auch vor Phishing-Angriffen. Da die Seite des Phishers von einer anderen Domain geliefert wird, als die originale Website, wird ein falscher Hash generiert, der für den Angreifer wertlos ist.

Sollte man unterwegs auf einem Rechner das Add-on nicht installiert haben, ist das Login-Passwort natürlich nicht zu erraten. Auf der Website des Projektes <sup>77</sup> steht der Algorithmus auch als Javascript Applet zur Verfügung. Man kann sein Master Passwort und die Domain eingeben und erhält das generierte Login Passwort. Das kann man mit Copy & Paste in das Passwort Eingabefeld übernehmen.

<sup>75</sup> <http://www.heise.de/ct/artikel/Ausgelacht-1195082.html>

<sup>76</sup> <https://addons.mozilla.org/de/firefox/addon/pwdhash/>

<sup>77</sup> <https://www.pwdhash.com>

## 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 (z.B. LUKS oder Truecrypt).
- 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 Bezahlern.
- 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.

Mir gefällt *Keypass*<sup>78</sup> (Windows) bzw. *KeepassX* (Linux) sehr gut. Die Bedienung ist übersichtlich. Man kann Einträge gruppieren, komplizierte Passwörter können über die Zwischenablage in die Eingabefelder kopiert werden und müssen nicht (fehlerhaft) abgetippt werden. Um kryptoanalytische Angriffe zu erschweren, kann man die Datenbank mehrere 10.000x mit AES256 verschlüsseln.

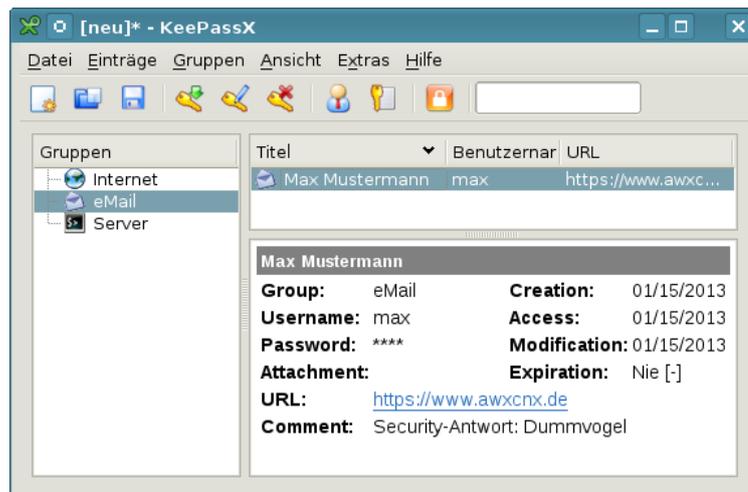


Abbildung 4.23: KeePassX Hauptfenster

<sup>78</sup> <http://keypass.en.softonic.com>

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.

## 4.15 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.

**OTP:** Bei der Zwei-Faktor-Authentifizierung mit zusätzlichem One-Time-Passwort besteht das Passwort aus zwei Komponenten, die hintereinander in das 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 geliefert und ist nur einmalig verwendbar.

Wenn ein Angreifer dieses zusammengesetzte Zwei-Faktor-Passwort erbeutet (mit einem Keylogger in einem unsicheren Internet Cafe', durch erfolgreiche Angriffe auf den Datenverkehr), dann ist es wertlos. Außerdem schützt OTP gegen Beobachtung der Passworteingabe durch die ausufernde Videoüberwachung öffentlicher Bereiche und in Internet Cafes.

OTP schützt aber 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 erfolgreichem Einbruch die Parameter auslesen und clonen.

Es gibt mehrere Verfahren für die Zwei-Faktor-Authentifizierung:

- **FreeOTP** nutzt One-Time-Passwörter, die von einer App auf dem Smartphone generiert werden. Sie werden auf dem Smartphone angezeigt und müssen per Hand innerhalb von 60s in das Login Formular abgetippt werden. Die Smartphone App *FreeOTP* gibt es im F-Droid Store und im GooglePlay Store (für Android) sowie im AppleStore (für iPhone).

Wenn man FreeOTP Login bei einem Webdienst aktiviert, dann wird ein ORCode angezeigt, den man mit dem Smartphone scannt. Mit diesem Scan ist FreeOTP auf dem Smartphone für den Webdienst konfiguriert.

- **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-

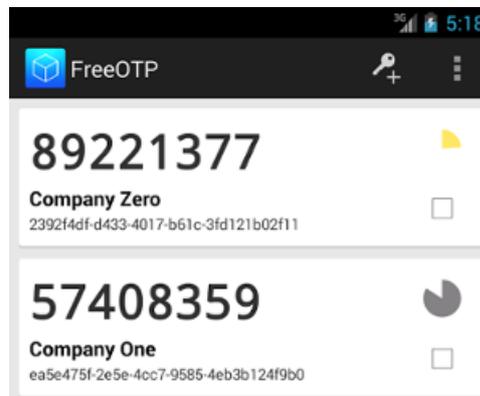


Abbildung 4.24: FreeOTP auf einem Smartphone

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 neuerdings auch als U2F SecurityStick.

**U2F:** ist ein kryptografisches Privat/Public Key Verfahren zur Authentifizierung mit einem kleinen Security USB-Stick, das im Okt. 2014 standardisiert wurde. Es schützt im Gegensatz zu OTP auch bei Einbrüchen auf dem Server und vor der Eingabe von gültigen Login Credentials auf Phishingseiten. Das Verfahren läuft im Hintergrund automatisch ab, man muss nur den SecurityStick vor dem Login anschließen. Der Server sendet ein zufälliges Challenge an den Client (Browser), der Browser gibt diesen Input zusammen mit der URL an den SecurityStick weiter, der mit einem geheimen Schlüssel eine Signatur über diese Daten berechnet. Diese Signatur wird als Response an den Server zurück gesendet und kann dort mit dem passenden public Key verifiziert werden.

U2F muss vom Browser und vom Webdienst unterstützt werden. Bisher bietet nur Google Chrome Support für U2F. Mozilla arbeitet daran. Im Gegensatz zu OTP wäre U2F auch mit E-Mail Clients sinnvoll einsetzbar, wenn Thunderbird und die E-Mail Provider es unterstützen würden. Das dauert aber noch ein einige Zeit.

**VerificationCode** nutzt SMS. Der Webdienst sendet eine SMS mit einem Code an eine Handynummer, die der Nutzer beim Webdienst hinterlegt hat. Der Code ist dann abzutippen. Ich mag es nicht, einem Webdienst wie Google (PRISM-Partner) meine Handynummer zu geben, ich erwähne das Verfahren nur wegen der Vollständigkeit.

## 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 Firma *Bluecava* verwendet im Trackingscript BCAL5.js u.a. Informationen über installierte Schriftarten zur Identifikation der Surfer.

Um die installierten Schriftarten zu verstecken, deaktiviert man in den Einstellungen die Option *Webseiten das verwenden von eigenen Schriften erlauben*. Man findet die Option in den Firefox *Einstellungen* auf dem Reiter *Inhalt*. Klicken Sie auf den Button *Erweitert*, um im folgenden Dialog Bild 4.25 die Option zu deaktivieren.

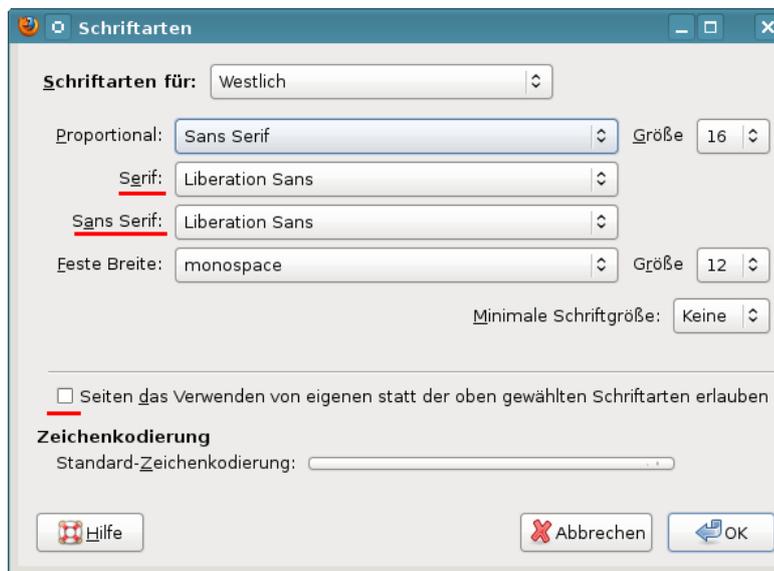


Abbildung 4.25: Schriftarten

Damit kann man nur "3" Schriftarten auslesen. Der Browser verwendet aber auch nur die drei Standardschriften zur Darstellung der Webseiten. Damit sehen nicht alle Webseiten exakt so aus, wie es sich der Designer wünscht. Um die Lesbarkeit zu verbessern, sollten man außerdem gut lesbare Standardschriften verwenden. Unter Windows eignet sich *Arial*, unter Linux nutzt man am besten *Liberation Sans*.

Außerdem können auf dem Rechner nicht vorhandene Schriftarten aus dem Web nachgeladen werden. Das ist ein Sicherheitsrisiko, weil damit Angriffe direkt auf das Betriebssystem möglich werden. Bugs in den Font Rendering Bibliotheken, die Remote Code Execution durch Laden von bösartigen Schriften erlaubten, gab es für Windows (ms11-087), Linux (CVE-2010-3855) oder OpenBSD (CVE-2013-6462).

Das Laden von Schriften aus dem Web mittels *@font-face* Attribute in CSS3 kann man mit dem Add-on NoScript blockieren. Außerdem können Schriften mit WebGL geladen werden. Das Nachladen von Schriftarten mit WebGL

kann man ebenfalls mit NoScript blockieren (siehe Bild 4.26) oder man schaltet WebGL unter *about:config* komplett ab.

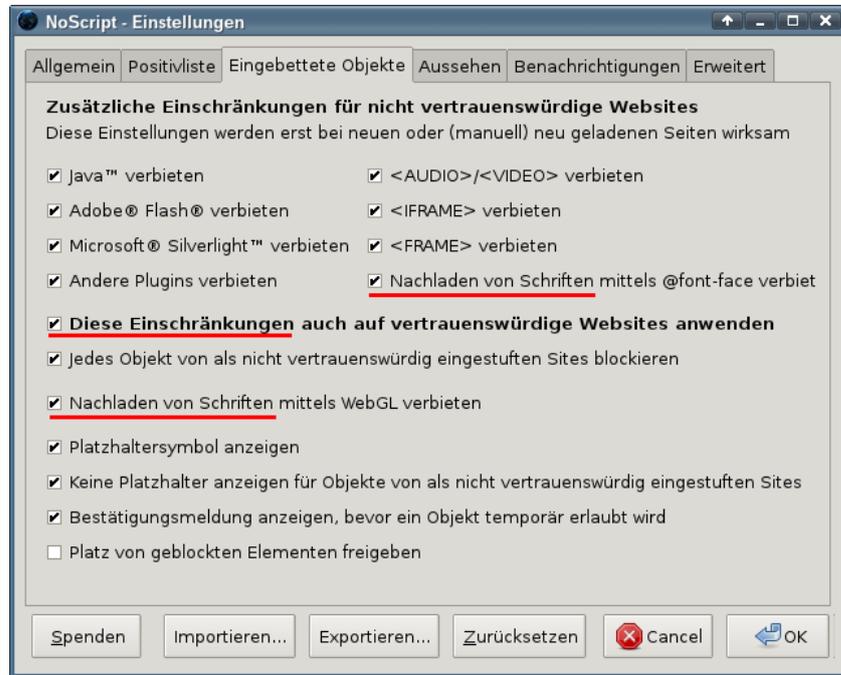


Abbildung 4.26: Nachladen von Schriften deaktivieren

## 4.17 HTML5 Canvas Elemente

Wie man das HTML5 Canvas Element zur Berechnung eines individuellen Fingerprint nutzen kann, wurde 2012 in dem Paper Perfect Pixel<sup>79</sup> (PDF) beschrieben. Mit Javascript kann z.B. ein Text in das Bildelement geschrieben werden. Danach wird das Ergebnis als Grafik ausgelesen und ein Hash berechnet. Das Ergebnis unterscheidet sich on Browser zu Browser aufgrund installierter Schriften, Software für das Rendering usw.

Der Canvastest auf Browserleaks.com<sup>80</sup> demonstriert das Verfahren und kann Schlussfolgerungen über den verwendeten Browser und das verwendete Betriebssystem ableiten (und damit einen User-Agent Fake enttarnen).

Your Fingerprint :

|                    |   |
|--------------------|---|
| Signature          | 1CC7FA60  |
| Found in DB        | ✓ True  |
| General Conclusion | <b>It is very likely that you are using [Firefox] on [Ubuntu]</b> |

<sup>79</sup> <http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf>

<sup>80</sup> <http://www.browserleaks.com/canvas>

Das Add-on **CanvasBlocker**<sup>81</sup> kann Zugriffe auf Canvas Elemente blockieren. In den Einstellungen des Add-on aktiviert man am besten die Option: *alle lesenden Zugriffe auf Canvas Elemente blockieren*. Dann wird man nicht mit seltsamen Fragen belästigt.

## 4.18 User-Agent modifizieren für Firefox

Die meisten Browser senden Informationen über den verwendeten Browser und das Betriebssystem. Ein Beispiel zeigt, wie detailliert der Browser Auskunft gibt:

```
Mozilla/5.0 (Macintosh; U; PPC Mac OS X; de-DE) AppleWebKit/419.3  
(KHTML, like Gecko) Safari/419.3
```

Beim US-Reiseportal Orbitz werden Surfern mit MacOS (am User-Agent erkennbar) die Hotelzimmer 20-30 Dollar teurer angeboten, als anderen Kunden<sup>82</sup>. Außerdem können anhand der Informationen gezielt Lücken in der verwendeten Software für Angriffe zur Installation von Trojanern ausgenutzt werden.

Es ist nicht so einfach, den User Agent plausibel zu faken. Um durch unsachgemäße Änderung keine eindeutige Kennung zu generieren, sollte man nachdenken, bevor man etwas ändert. Man kann für einen Firefox nur eine andere Firefox-Kennung verwenden. Da die verschiedenen Browser durch individuelle HTTP-Header erkennbar sind, ist eine Tarnung mit dem User-Agent eines anderen Browsers leicht als Fake zu identifizieren und man ist eindeutig identifizierbar. Einige Firefox Versionen unterscheiden sich nicht nur im User-Agent, sondern auch sehr subtil in einigen anderen HTTP-Headern. Man beachte das Leerzeichen nach dem Komma bei FF 10.0:

```
ACCEPT-ENCODING "gzip,deflate"      (Firefox 3.6.x)  
ACCEPT-ENCODING "gzip, deflate"    (Firefox 10.0.x)
```

Deshalb muss man auch eine ähnliche Firefox-Version für den Fake nutzen, die sich in den übrigen HTTP-Headern nicht unterscheidet. Die meisten Firefox-User nutzen Windows als Betriebssystem. Für diese Nutzergruppe empfehle ich den Firefox ESR für Linux als Fake, um die Gefahr automatisierter Angriffe zu reduzieren. Die Nutzer anderer Betriebssysteme können als Fake einen Firefox für Windows verwenden, um in einer möglichst großen Anonymitätsgruppe einzutauchen.

Um die User-Agent Kennung zu ändern, gibt man in der Adresszeile *about:config* ein und setzt die angegebenen Variablen auf die Werte. Falls eine Variable noch nicht existiert, ist sie neu anzulegen. Alle Werte sind vom Typ String. Der Wert für *general.buildID.override* ändert sich alle 6 Wochen mit einem neuen Firefox Release.

User-Agent Fake für einen Firefox 38.2.0 esr (Linux):

<sup>81</sup> <https://addons.mozilla.org/de/firefox/addon/canvasblocker/>

<sup>82</sup> <http://heise.de/-1626368>

| Variable                    | Wert  |
|-----------------------------|---|
| general.useragent.override  | Mozilla/5.0 (X11; Linux i686; rv:38.0)<br>Gecko/20100101 Firefox/38.0 |
| general.appname.override    | Netscape  |
| general.appversion.override | 5.0 (X11)   |
| general.oscpu.override      | Linux i686  |
| general.platform.override   | Linux i686  |
| general.productSub.override | 20100101  |
| general.buildID.override    | 20150806103657  |
| general.useragent.vendor    |   |
| general.useragent.vendorSub |   |

User-Agent Fake für einen Firefox 40.0 (Windows 7):

| Variable                    | Wert   |
|-----------------------------|--|
| general.useragent.override  | Mozilla/5.0 (Windows NT 6.1; rv:40.0)<br>Gecko/20100101 Firefox/40.0 |
| general.appname.override    | Netscape   |
| general.appversion.override | 5.0 (Windows)  |
| general.oscpu.override      | Windows NT 6.1   |
| general.platform.override   | Win32  |
| general.productSub.override | 20100101   |
| general.buildID.override    | 20150807085045   |
| general.useragent.vendor    |  |
| general.useragent.vendorSub |  |

## 4.19 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.

**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.

Firefox bietet keine Möglichkeiten, um diese Werte zu faken. Als Verteidigung gibt es folgende zwei Möglichkeiten:

1. Trackingscripte können listenbasiert mit Werbeblockern wie *Ad-Block Plus* oder *uBlock Origin* blockiert werden.
2. Da das Auslesen der Daten mit Javascript erfolgt, kann man Javascript blockieren, wenn man es nicht benötigt.

**Batterie-API:** Aus unbekannten Gründen ist im HTML5-Standard eine API für den Zugriff auf den Status des Laptop Akku vorgesehen. Damit ist es möglich, den Ladezustand des Akku sowie den Status des Stromanschlusses abzufragen. Um zu verhindern, dass der Ladezustand der Batterie als Tracking Feature genutzt wird oder dass das Vorhandensein eines Akku im Browser Fingerprint genutzt wird, sollte man die API unter *about:config* deaktivieren:

```
dom.battery.enabled = false
```

**Gamepad-API:** Die Gamepad-API liefert Informationen über einen angeschlossenen Gamepad. Das ist ein überwiegend sinnloses Feature und kann ebenfalls unter *about:config* deaktiviert werden:

```
dom.gamepad.enabled = false
```

**Keyboard-API:** Erste Funktionen der Keyboard-API wurden in Firefox 38.0 standardmäßig aktiviert. Durch Auswertung der Keyboard Events beim Schreiben in Formularen kann ein Trackingscript z.B. ermitteln, ob eine deutsche oder englische Tastatur verwendet wird. Die Keyboard Events können unter *about:config* deaktiviert werden:

```
dom.keyboardevent.code.enabled = false
dom.beforeAfterKeyboardEvent.enabled = false
dom.keyboardevent.dispatch_during_composition = false
```

**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
```

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

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

## 4.20 Sonstige Maßnahmen

Am Schluss der Konfiguration gibt es noch ein paar kleine Maßnahmen, die überflüssige Features im Browser deaktivieren, die Informationen preisgeben.

### Geolocation-API deaktivieren

Mit Hilfe der Geolocation-API kann die geografische Position des Surfer relativ genau bestimmt werden. Zur Ortsbestimmung können je nach vorhandener Hardware im Rechner die WLANs in der Umgebung genutzt werden, GPS-Hardware oder ... Im ungünstigsten Fall kann der Standort nur anhand der IP-Adresse bestimmt werden. Aktuelle Firefox Versionen fragen nach, bevor der

Zugriff auf die Geolocation API erlaubt wird. Trotzdem habe ich ein besseres Gefühl, wenn man es komplett deaktiviert. Dafür muss man unter *about:config* die folgende Variable setzen:

```
geo.enabled = false
geo.wifi.uri = "" (leerer String)
```

Diese Einstellung ist wichtig, wenn man die eigene IP-Adresse mit VPNs oder Anonymisierungsdiensten versteckt.

### WebGL deaktivieren

WebGL stellt eine Javascript-API für das Rendering von 3D-Objekten bereit. Es kann für das Fingerprinting der Performance der Grafikkhardware und OpenGL Implementierung genutzt werden, wie die Studie *Perfect Pixel: Fingerprinting Canvas in HTML5*<sup>83</sup> zeigt. Außerdem können mit WebGL Schriftarten aus dem Web nachgeladen werden. Das ist ein Sicherheitsrisiko, weil damit Angriffe auf das Betriebssystem möglich werden. Bugs, die eine Remote Code Execution mit böartigen Schriftarten erlaubten, gab es für Windows (ms11-087), Linux (CVE-2010-3855) oder OpenBSD (CVE-2013-6462).

Bei Firefox kann man WebGL unter *about:config* deaktivieren:

```
webgl.disabled = true
```

### WebRTC deaktivieren

WebRTC ist eine Technologie, die direkte Telefonie und Videochats zwischen Surfern im Browser ermöglichen soll. Derzeit gibt es wenig sinnvolle Anwendungen für diese Technologie und ich würde ein spezialisiertes Programm wie Jitsi bevorzugen. Wer es einmal ausprobieren möchte, kann sich <https://palava.tv> oder <http://browsermeeting.com> anschauen.

Mit WebRTC kann die lokale IP Adresse des Rechners im LAN und die öffentliche IP Adresse ermittelt werden. Bei IPv4 Adressen ist es in der Regel nicht öffentliche IP-Adresse sondern die Adresse im internen LAN, trotzdem ist es ein Identifikationsmerkmal. Bei Firefox kann man WebRTC unter *about:config* deaktivieren:

```
media.peerconnection.enabled = false
```

### Timing APIs deaktivieren

Die hochgenauen Timing APIs können von Webanwendungen zur Analyse des Ladens von Ressourcen oder des Nutzerverhaltens missbraucht werden, siehe: *Timing Attacks on Web Privacy*<sup>84</sup>. Wenn man seinen Browser zum Lesen von Webseiten und nicht vorrangig für Games verwendet, sollte man die APIs deaktivieren:

<sup>83</sup> <http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf>

<sup>84</sup> <http://sip.cs.princeton.edu/pub/webtiming.pdf>

```
dom.enable_resource_timing = false
dom.enable_user_timing     = false
dom.enable_performance     = false
```

### 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
```

### WebIDE deaktivieren

TorProject.org empfiehlt für Firefox 38.0 ff. aus Sicherheitsgründen, die WebIDE unter *about:config* zu deaktivieren:

```
devtools.webide.enabled = false
devtools.webide.autoinstallADBHelper = false
devtools.webide.autoinstallFxdtdAdapters = false
```

### Kill Switch für Add-ons abschalten

Die Extension blocklist<sup>85</sup> 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
```

<sup>85</sup> <https://addons.mozilla.org/en-US/firefox/blocked>

### Download der Safebrowsing Datenbank deaktivieren

Ab Firefox 34.0 reicht es nicht mehr, die Nutzung von Googles Safebrowsing Datenbank im Einstellungsdialog zu deaktivieren. Zusätzlich muss man den Download der Datenbank unter *about:config* abschalten, wenn man keine Verbindungen zu Google herstellen will:

```
browser.safebrowsing.downloads.enabled = false
```

### Healthreport deaktivieren

Der Healthreport wird an Mozilla gesendet, kann man unter *about:config* deaktivieren:

```
datareporting.healthreport.service.enabled = false  
datareporting.healthreport.uploadEnabled = false  
datareporting.policy.dataSubmissionEnabled = false
```

### Heartbeat User Rating deaktivieren

Mit Firefox 37.0 hat Mozilla das heartbeat user rating system eingeführt. Der User soll Firefox bewerten und wird gelegentlich zur Teilnahme an der Community eingeladen. Mozilla hat selbst erkannt, dass dieses Feature nerven könnte:

*We understand that any interruption of your time on the internet can be annoying.*

Unter *about:config* kann man das Feature deaktivieren, indem man die folgende URL auf einen leeren String setzt:

```
browser.selfsupport.url =
```

## 4.21 Snakeoil für Firefox (überflüssiges)

Auf der Mozilla-Website für Add-ons findet man tausende von Erweiterungen. Man kann nicht alle vorstellen. Ich bekomme immer wieder Hinweise auf dieses oder jenes privacyfreundliche Add-on und habe ein paar Dinge zusammengestellt, die ich nicht in die Empfehlungen aufnehmen.

Als Grundsicherung empfehle ich die Kombination von *CookieController* + *NoScript* + *AdBlock Plus* (o.ä.) + *HTTPSEverywhere* + *CanvasBlocker* und evtl. *RefControl*. Viele Add-ons bieten Funktionen, die von dieser Kombination bereits abgedeckt werden. Andere sind einfach nur überflüssig.

### PrivacyBadger der EFF.org

Das Add-on lernt anhand der Verteilung der Cookies beim Surfen selbständig, welche Domains das Surfverhalten tracken. Das ist ein interessantes Konzept. Wir teilen aber die Vorbehalte von TorProject.org gegen dieses Konzept.

- Es entstehen dabei individuelle Blocklisten, die für das Fingerprinting genutzt werden können. Es ist bekannt, dass man Seiteneffekte von Add-ons (NoScript Whitelist, Adblock Filterlisten) für das Fingerprinting des Browsers nutzen kann. PrivacyBadger liefert einen dynamischen, aber sehr individuellen Fingerprint.
- Es werden Informationen über das Surfverhalten auf der Festplatte gespeichert (unerwünscht) und außerdem werden durch die individuelle Blockliste indirekt Informationen über die Surf-History an die Webseiten geliefert.

### Google Analytics Opt-Out

Das Add-on von Google verhindert die Ausführung der zu Google-Analytics gehörenden Scripte. 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 (via Referer). Außerdem gibt es über hundert weitere Surftracker, die ignoriert werden.

Die Add-ons NoScript und Adblock erledigen diese Aufgabe besser.

### GoogleSharing

Das Add-on verteilt 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 unserer Meinung verbessert man seine Privatsphäre nicht, indem die Daten einem weiteren Dienst zur Verfügung stellt. Das 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 breitwillig an Behörden und Geheimdienste weiter. So kann man unschuldig in Verwicklungen geraten, die man lieber vermeiden möchte. Bei [daten-speicherung.de](http://daten-speicherung.de) findet man aktuelle Zahlen zur Datenweitergabe von Google an Behörden und Geheimdienste:

- 3x täglich an deutsche Stellen
- 20x täglich an US-amerikanische Stellen
- 6x täglich an britische Stellen

Statt GoogleSharing sollte man lieber privacy-freundliche Alternativen nutzen: die Suchmaschine [Ixquick.com](http://Ixquick.com) oder [Startingpage.com](http://Startingpage.com), für E-Mails einen Provider nutzen, der den Inhalt der Nachrichten nicht indiziert, [openstreetmap.org](http://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 Trackingdienste blockiert, die auch Adblock Plus mit der *EasyPrivacy Liste* sehr gut blockiert. Außerdem gibt es immer wieder Probleme mit *Ghostery* auf einigen Webseiten, da das Add-on kein Whitelisting kennt.
- *No FB Tracking* blockiert die Facebook Like Buttons. Auch das kann Adblock Plus besser. Die *SocialMediaBlock Liste* von MontzA blockieren nicht nur Facebook Like Buttons sondern andere Social Networks.
- 

Wer meint, es nutzen zu müssen - Ok.

## Kapitel 5

# Bezahlen im Netz

Der bekannteste Bezahl Dienstleister im Internet ist zweifellos **PayPal.com**. 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 gesperrt <sup>1</sup>, 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. 35.000 PayPal-Nutzer sollen dem Aufruf umgehend gefolgt sein.

Zukünftig möchte PayPal.com auch in der realen Welt präsent sein. Das Bezahl system 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.*

---

<sup>1</sup> <http://heise.de/-1320630>

## 5.1 Kreditkarten

Die Kreditkarte ist ein ungeeignetes Zahlungsmittel im Internet. Es ermöglicht das Tracking aller Einkäufe im Web. Außerdem kann die Kreditkarte durch Datenverluste beim Online-Händler kompromittiert werden. Das passiert öfters:

- 400.000 Kunden beim Internetkonzern Unister betroffen (Dez. 2012).<sup>2</sup>
- 1,5 Millionen Kunden bei Global Payments betroffen (Juni 2012).<sup>3</sup>
- Tausenden Nutzer der israelischen Sport-Webseite One.co.il betroffen (Jan. 2012).<sup>4</sup>
- 24 Millionen Kunden der Amazon-Tochter Zappos betroffen (Jan. 2012).<sup>5</sup>
- 40 Millionen Kreditkarten vom bei US-Shoppingriesen Target kopiert (Dez. 2013).<sup>6</sup>

In Carder-Foren kann man diese Kreditkarten für 3-10 Euro kaufen.

### Prepaid-Kreditkarten

Eine Alternative sind Prepaid-Kreditkarten. An Tankstellen usw. kann man Prepaid-Karten von *mywirecard.com* kaufen. Die Karte kostet ca. 10 Euro und kann bis zu 100,- Euro mit Bargeld beim Kauf aufgeladen werden. Man zahlt also 10% Security-Bonus.

Die Prepaid-Karte muss anschließend im Internet aktiviert werden. Dabei wird ein Code per SMS an eine Handynummer gesendet, der auf der Internetseite einzugeben ist. Die Anonymität hängt also davon ab, ob man ein anonymes Prepaid-Handy nutzt. Man braucht nicht immer die große, richtige Anonymität. Wenn ich ein SSL-Zertifikat für den Webserver *awxcnx.de* kaufe, dann ist mehr oder weniger eindeutig klar, wer dahinter steckt. Vergleichbare Anwendungsbeispiele lassen sich für den Leser sicher leicht finden.

Mit einer Prepaid-Karte kann man einen anonymen PayPal-Account mit fiktiven Daten anlegen. Das eröffnet Möglichkeiten zur anonymen Nutzung von kommerziellen Angeboten im Internet wie Wuala oder Cilent Circle, die nur Bezahlung via PayPal.com oder Kreditkarte anbieten.

Hinweis: Tor Onion Router kann nicht als Anonymisierungsdienst für PayPal.com genutzt werden. Paypal.com prüft anhand der IP-Adresse den Standort des Nutzers und sperrt den Account, wenn etwas seltsames passiert. Wenn man sich bspw. mit einer deutschen IP-Adresse einloggt und 10min später mit einer amerikanischen IP-Adresse auf den Account zugreifen möchte, dann geht PayPal.com von einem Hacker-Angriff aus und sperrt den Account. Mit JonDonym gibt es keine Probleme, wenn man immer die gleiche Mix-Kasakde nutzt.

<sup>2</sup> <http://www.mdr.de/nachrichten/unister130.html>

<sup>3</sup> <http://heise.de/-1617091>

<sup>4</sup> <http://heise.de/-1403584>

<sup>5</sup> <http://www.golem.de/1201/89081.html>

<sup>6</sup> <http://heise.de/-2070721>

## 5.2 Bezahlssysteme der Deutschen Bahn

Am 28. September 2011 veröffentlichte die Leaking Plattform Cryptom.org in der Liste der *Online Spying Guides* einen *Leitfaden zum Datenzugriff* der Generalstaatsanwaltschaft München.

Das Dokument zeigt auch, wie das Bezahlssystem der Deutschen Bahn in die Überwachung eingebunden wird. Für das e-Ticketing der Deutschen Bahn gibt es ein konkretes Überwachungsszenario. Durch die Abrechnung übers Mobiltelefon verfüge die Deutsche Bahn über die Daten sämtlicher Funkzellen, die der Nutzer durchfahren hat. Diese Daten werden langfristig gespeichert und können von den Behörden auf Grundlage von §100g StPO abgerufen werden. Der Zugriff auf die Reisepprofile ist damit nicht nur bei schweren Straftaten möglich, sondern auch bei allen Straftaten, die mittels Telekommunikationstechnik begangen wurden.

Das Beispiel zeigt, wie bei Nutzung Handy-basierter Bezahlmethoden neue Datenbestände anhäufen. Teilweise können diese Daten auch als Rechnungsdaten abgerufen werden ohne die juristischen Hürden des Zugriffs auf Kommunikationsdaten.

Als Konsequenz kann man Reisenden mit der Deutschen Bahn nur zu anonymen Bargeldzahlungen raten. Wie schnell man plötzlich ein *Terrorist* wird, zeigte das Beispiel *Andrej Holm*.

## 5.3 Paysafecard, UKash, Pecunix

Bei der Nutzung von Alternativen ist man abhängig von den Angeboten der Online-Händler. Man kann nicht bei allen Händlern mit allen Varianten bezahlen und muss als Kunde etwas flexibel sein.

- **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. Es ist nicht notwendig, dass man einen Gutscheincode genau mit dem geforderten Betrag vorweisen kann. Man kann mehrere Gutscheine für eine Bezahlung verwenden oder nur einen Teilbetrag von Gutscheinen einlösen. Der Restbetrag bleibt erhalten und kann später verwendet werden.

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 Gutscheincodes.

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 im April 2012 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.

- **UKash:** funktioniert ähnlich wie Paysafecard, bietet aber nicht ganz so viele Verkaufsstellen in Deutschland. Im Gegensatz zu Paysafecard sind keine Probleme mit gesperrten Gutscheincodes bekannt. Außerdem wird man bei UKash nicht zur Einrichtung eines Accounts gedrängt. Die Nutzung ist damit anonymer, als mit Paysafecard.

UKash akzeptiert keine Anonymisierungsdienste und VPN-Dienstleister als Partner, hat aber mit (illegalen) Webseiten zu (Sport-) Wetten kein Problem:

*Ukash will not under any circumstances knowingly approve Merchants associated directly or indirectly with the following products or services:*

.....

*1. IP anonymisers or private VPNs or any similar service which has the intention of hiding the true identity of a computer or device.*

- **Pecunix:** wickelt Bezahlungen in Gold ab. Die Geldbeträge werden automatisch in Gold konvertiert. Um mit Pecunix zu bezahlen, ist ein Account zu erstellen, bei dem ebenfalls lediglich die E-Mail Adresse gültig sein muss. Als einziger Bezahlendienstleister kann Pecunix den gesamten E-Mail Verkehr zu den Nutzern mit OpenPGP verschlüsseln. Man kann seinen eigenen OpenPGP-Schlüssel im Account hochladen und die Option zur Verschlüsselung aktivieren.

Um mit Pecunix bezahlen zu können, muss man eGold kaufen. Auf der Webseite von Pecunix findet man eine Liste von Exchangern.

- **cashU:** ist ein Bezahlservice, der hauptsächlich in der arabischen Welt verwendet wird. Registrieren kann man sich *wie man will* und die Konten bleiben unüberprüft bestehen. Die cashU Währung lässt sich auf der Webseite durch UKash Codes aufladen, wenn man sich mit einer Kopie des Ausweises identifiziert. Einen anderen Weg habe ich von Deutschland aus noch nicht gefunden.

## 5.4 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.<sup>7</sup>

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:

---

<sup>7</sup> <http://heise.de/-1269409>

*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.*

## 5.5 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.

In Deutschland sind bereits kleine Schritte in diese Richtung sichtbar. Einige Banken haben die Verfügbarkeit von Bargeld von 2.000 Euro pro Tag auf 1.000 Euro pro Tag reduziert. Außerdem werden zusätzlich zu Tageslimits auch Wochenlimits eingeführt.

Der Wirtschaftsweiser 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 Bargeld einsetzen soll. Dafür wurden folgende Gründe genannt:<sup>8</sup>, die ich nur kurz kommentieren will:

<sup>8</sup> <http://www.manager-magazin.de/finanzen/artikel/bofinger-und-rogoff-fordern-abschaffung-des-bargelds-a-1034135.html>

**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.

### **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.<sup>9</sup>*

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.<sup>10</sup>*

<sup>9</sup> <http://bitcoinblog.de/2015/05/18/bargeld-ist-macht>

<sup>10</sup> <http://www.heise.de/tp/artikel/45/45089/1.html>

### Weitere Entwicklung

In Deutschland werden lt. einer Studie der Bundesbank<sup>11</sup> noch 53% der Umsätze im Einzelhandel in Bargeld abgewickelt. Außerdem steht eine Mehrheit der Deutschen Experimenten mit Zahlungssystemen eher skeptisch gegenüber. Nach Einschätzung der Bundesbank ist derzeit eine Abschaffung von Bargeld nicht möglich. Diese Zahlen zeigen auch, wie man sich gegen diese Bestrebungen wehren kann:

#### Verwendet Bargeld, wo es möglich ist.

Das österreichisch-deutschen Unternehmen EDAQS hat mit Hilfe von RFID-Geldscheine entwickelt, die ferngesteuert entwertet werden können<sup>12</sup>. Das ist eine weitere, beunruhigende Entwicklung. Neben der ferngesteuerten Entwertung von Geldscheinen nach einem Bankraub soll damit auch die Finanzierung von *Terrorgruppen* verhindert werden können (ok - das scheint sich zum Universalargument zu entwickeln). Außerdem wäre es damit möglich, Sparguthaben unter der Matraze (außerhalb des Zugriffs der Banken) bei Bedarf und natürlich nur auf Basis gesetzlicher Grundlagen zu entwerten.

## 5.6 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 kann Bitcoin als Bezahlmethode verwendet werden. Bitcoins lassen sich in reale Währungen hin- und zurücktauschen. Der Kurswert

<sup>11</sup> [http://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Bericht\\_Studie/zahlungsverhalten\\_in\\_de](http://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Bericht_Studie/zahlungsverhalten_in_de)

<sup>12</sup> [http://www.t-online.de/wirtschaft/boerse/devisen/id\\_74134666/geldscheine-koennen-bald-per-funk-entwertet-werden.html](http://www.t-online.de/wirtschaft/boerse/devisen/id_74134666/geldscheine-koennen-bald-per-funk-entwertet-werden.html)

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.

Viele Dienste im Netz akzeptieren Bitcoins als Bezahlung. Eine Übersicht findet man im Bitcoin Wiki<sup>13</sup>. Man kann Musik, E-Books, Web- und Mailhosting oder Anonymisierungsdienste / VPN-Anbieter mit Bitcoins bezahlen. Der Kurs wird dabei von jedem Anbieter selbst festgelegt. Dabei kann es vorkommen, dass Anbieter vom mittleren Tauschkurs abweichen. Die schnelle, unkomplizierte Bezahlung bei Webdiensten, die die Privatsphäre ihrer Kunden respektieren, ist für mich die Hauptanwendung von Bitcoin. Es ist praktisch, wenn man immer ein paar Bitcoins im Wallet hat und unkompliziert bezahlen kann.

Um mit Bitcoins zu bezahlen, braucht man selbst ein paar Bitcoins. Diese kann man auf verschiedenen Marktplätzen gegen reale Währung kaufen oder man bietet selbst Dienstleistungen gegen Bitcoins als Bezahlung an. Verschiedene Marktplätze dienen dabei nur zur Anbahnung der Transaktionen *Geld gegen Bitcoin*. Der Austausch des reales Geldes erfolgt in der Regel auf direktem Weg zwischen den Beteiligten.

### 5.6.1 Exchanger / Marktplätze

Man kann Bitcoin komplett ohne Installation einer Software nutzen. Es gibt Webdienste (die sogenannten Exchanger oder Marktplätze), die den Handel mit Bitcoins zwischen den Personen einleiten und eine Bitcoin Brieftasche (eWallet) für Nutzer bereitstellen. Das vereinfacht die Nutzung von Bitcoin als Zahlungsmittel, da eine Installation von Software nicht zwingend nötig ist. Die erworbenen Bitcoins können aber auch auf den eigenen PC transferiert und mit einem Bitcoin Client verwaltet werden.

Die Exchanger verifizieren die Identität der Nutzer. Eine anonyme Nutzung ist nicht möglich. Hinweise zum anonymen Kauf von Bitcoins gibt es weiter unten im Abschnitt *Anonymität von Bitcoin*.

*Warnung:* viele Marktplätze haben sich als unsicher erweisen. Das prominenteste Beispiel ist die Insolvenz von *MtGox* nachdem Bitcoins im Wert von 368,4 Millionen Euro verloren gingen. Viele Kunden, die mit Bitcoin als Spekulationsobjekt das große Geld gewinnen wollten, haben ihr Geld dort verloren. Weitere Beispiele sind die Bitcoin Börsen *Flexcoin* (die nach virtuellem Bankraub geschlossen wurde) oder *Poloniex*. Man sollte also gut überlegen, wem man seine Bitcoin Brieftasche anvertraut oder ob man sie lieber selbst verwaltet.

Für den Einstieg gefällt mir [www.bitcoin.de](http://www.bitcoin.de) sehr gut. Im Gegensatz zu anderen Marktplätzen ist der Handel bei *Bitcoin.de* durch Kooperation mit der

<sup>13</sup> <https://en.bitcoin.it/wiki/Trade>

Fidor-Bank<sup>14</sup> abgesichert. Die Webseite wird professionell betreut, bietet in einer übersichtlichen Struktur alle nötigen Informationen für Kaufen, Verkaufen und die Verwaltung der eigenen Bitcoins und ist für die ersten Schritte gut geeignet. Allerdings ist der Dienst nicht ganz kostenfrei. Es wird eine Gebühr von 1% für den Handel mit Bitcoins erhoben.

Die Anmeldung bei Bitcoin.de erfordert die Angabe einer E-Mail Adresse und einer Bankverbindung. Die Bankverbindung wird durch eine einmalige Überweisung von 1 Cent verifiziert. Vollständige Identifizierung erfordert PostIdent. Temporäre E-Mail Adressen sollten nicht genutzt werden, da bei jeder Transaktion Informationen per Mail ausgetauscht werden. Bitcoin.de kann die E-Mails mit OpenPGP verschlüsseln, wenn man einen Public Key zum Server hochlädt und die Funktion aktiviert. Der Service setzt hohe Sicherheitsstandards um und bietet 2-Faktor Authentifizierung mit FreeOTP oder Yubikey.

**Bitcoins kaufen:** Im Marktbereich stehen in einer Liste mehrerer Verkaufsangebote. Durch Klick auf den Link *Kaufen* kann man ein Kaufangebot annehmen. Sie erhalten ein E-Mail mit den Daten für die Bezahlung. Überweisen Sie dem Verkäufer das Geld und bestätigen Sie die Überweisung auf der Webseite innerhalb von 12h. Wenn der Verkäufer den Zahlungseingang bestätigt, erhalten Sie die Bitcoins. Wenn kein passendes Angebot zu finden ist, können Sie ein Kaufangebot einstellen und auf Angebote warten.

Der Käufer sendet dem Verkäufer den Kaufpreis abzüglich 0.5% und erhalten dafür Bitcoins abzüglich 1% des Kaufangebotes. Somit teilen sich Käufer und Verkäufer die Marktgebühr von 1% jeweils zur Hälfte. Ein Rechenbeispiel:

- Das Angebot lautet: 1 BTC für 40,00 Euro.
- Der Käufer überweist 39,80 Euro an den Verkäufer.
- Er erhält dafür 0,99 BTC auf seinem Konto.

Die für ihre Transaktion gültigen Zahlen werden jeweils bei Annahme des Kaufangebotes und in der E-Mail angezeigt. Die Kontodaten des Verkäufers erhalten Sie ebenfalls per E-Mail.

## 5.6.2 Bitcoin Software

Wenn man einem externen Webserver nicht vertraut, kann man seine Bitcoins lokal auf dem eigenen Rechner oder Smartphone verwalten. Dafür muss ein Bitcoin Client wie Bitcoin-Qt oder Electrum installiert werden.

**Bitcoin-Qt** ist der Standard Client des Bitcoin Projektes und steht zum Download unter <http://bitcoin.org/en/download> bereit. Er ist einfach bedienbar, bietet eine Übersicht über alle Transaktionen und kann

<sup>14</sup> <https://blog.bitcoin.de/en/bitcoin-de-und-fidor-bank-ag-vereinbaren-weitgehende-partnerschaft>

beliebig viele Adressen verwalten.

Ein Nachteil für Gelegenheitsnutzer ist der ständige Download der gesamten Blockchain. Die Downloadseite weist darauf hin, dass die erste Initialisierung bis zu einem Tag dauern kann. Wenn man nach 3-4 Wochen Pause wieder einmal mit Bitcoins bezahlen möchte, dann benötigt Bitcoin-Qt ein bis zwei Stunden für die Aktualisierung der Blockchain, um wieder arbeitsbereit zu werden.

**Electrum** ist eine leichtgewichtige Alternative für Gelegenheitsnutzer. Es überlässt die Hauptarbeit speziellen Servern im Netz und benötigt die komplette Blockchain nicht. Trotzdem ist sichergestellt, dass die privaten Schlüssel ausschließlich in der Verfügung des Anwenders liegen. Die Installation für unterschiedliche Betriebssysteme ist auf der Website <https://electrum.org> unter *Download* beschrieben.

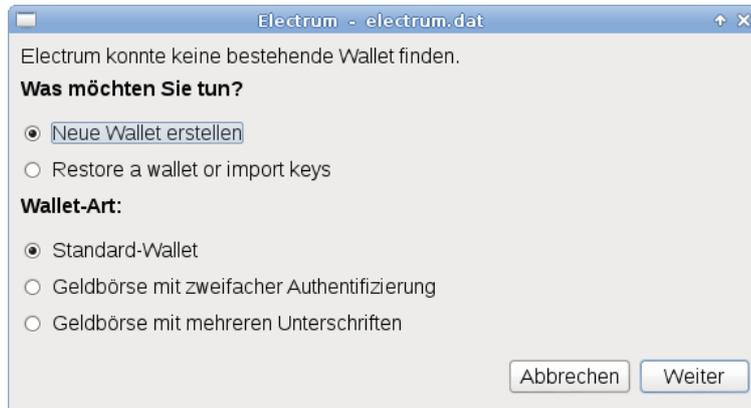


Abbildung 5.1: Neues eWallet in Electrum erstellen

Beim ersten Start fragt Electrum, ob ein neuer Account erstellt werden soll oder ob ein Wallet mit dem Backup eines vorhandenen Seed wieder hergestellt werden soll (Bild. 5.1). Ein Standard Wallet kann man mit einem Passwort schützen. Wenn man ein Wallet mit zweifacher Authentifizierung wählt, dann muss der Service TrustedCoin<sup>15</sup> alle Transaktionen unterschreiben. Gegenüber TrustedCoin authentifiziert man sich mit einem One-Time-Passwort.

Im nächsten Schritt wird bei der Erstellung eines neues eWallet der Seed angezeigt. Mit dem *Seed* kann das eWallet jederzeit auf einem anderen Rechner aus dem *ewigen Logfile* rekonstruiert werden. Ein vollständiges Backup der Konfiguration ist nicht nötig. Man benötigt nur den Seed, der wie eine lange Passphrase aus 25 Worten besteht. Der Seed ist unbedingt zu speichern (z.B. in einer verschlüsselten Passwortdatenbank

<sup>15</sup> <https://api.trustedcoin.com/>



Abbildung 5.2: Seed exportieren

wie KeePassX). Mit dem QR-Code könnte man den Seed schnell auf ein Smartphone übertragen, wenn man das gleiche Wallet auch unterwegs (in der realen Welt) nutzen möchte.

Die Oberfläche von Electrum ist einfach gehalten. Für die Übersicht der Transaktionen, zum Senden und Empfangen sowie eine einfache Adressliste gibt es Reiter im Hauptfenster (Bild 5.3).



Abbildung 5.3: Hauptfenster von Electrum

Die Netzwerkeinstellungen öffnet man mit einem Klick auf das rechte Icon in der Statusleiste im Hauptfenster, das üblicherweise ein grüner Punkt ist. Hier kann man festlegen, welchen Server man für die rechen-

intensiven Aufgaben nutzen möchte. Der Server kann aus der Liste frei gewählt werden, da keine Accountdaten auf dem Server gespeichert werden. Die Server werden durch Spenden finanziert und die Betreiber sind für eine kleine Spende in Bitcoins dankbar. Die Spendenadresse für den aktuell genutzten Server findet man auf dem Reiter *Console*.

Außerdem kann man in den Netzwerkeinstellungen den Proxy konfigurieren. Da Electrum nur geringen Datenverkehr verursacht, ist eine sinnvolle Kombination mit den Anonymisierungsdiensten Tor oder JonDonym möglich. Um den Datenverkehr von Electrum mit den Premiumdiensten von JonDonym zu anonymisieren, startet man das Programm mit folgenden Proxy-Parametern:

```
electrum --proxy=http:127.0.0.1:4001
```

Wenn man Tor Onion Router nutzen möchte (TorBrowserBundle) und sich außerdem nur mit Tor Hidden Services verbinden möchte, dann startet man das Programm mit folgenden Parametern:

```
electrum -s 56ck15obj37gypcu.onion:50001:t -p socks5:localhost:9150
```

```
electrum -s 4rwpmjwjfocguylj.onion:50001:t -p socks5:localhost:9150
```

```
electrum -s drp4pvejybx2ejdr.onion:50001:t -p socks5:localhost:9150
```

Die Installation von JonDo oder Tor ist im Kapitel *Anonymisierungsdienste* beschrieben.

### 5.6.3 Anonymität von Bitcoin

Über die Anonymität von Bitcoin gibt es viele Missverständnisse.

Alle Bitcoin Transaktionen werden in der öffentlich zugänglichen Blockchain protokolliert (ein *ewiges Logfiles*). Das ist kein Designfehler sondern notwendig, um double spending zu verhindern.

- Forscher der TU Darmstadt haben auf dem 28C3 eine Analyse des *ewigen Logfile* von Bitcoin vorgestellt <sup>16</sup>. Eine weitere Analyse wurde von D. Ron und A. Shamir publiziert <sup>17</sup>. Beide Analysen konnten scheinbar unabhängige Bitcoin Adressen zusammen führen und die IP-Adressen von Nutzern ermitteln. Dazu zählen beispielsweise Spender, die an Wikileaks via Bitcoin gespendet haben. Außerdem wurden Zahlen zur Bitcoin Nutzung von Wikileaks als Beispiel veröffentlicht. Bis März 2012 nutzte Wikileaks 83 Bitcoin Adressen und erhielt 2605.25 BTC von Unterstützern.

---

<sup>16</sup> <http://events.ccc.de/congress/2011/Fahrplan/events/4746.en.html>

<sup>17</sup> <http://eprint.iacr.org/2012/584>

- In dem wiss. Paper *Deanonymisation of clients in Bitcoin P2P network*<sup>18</sup> wird ein Angriff auf Netzwerkebene vorgestellt, der orthogonal zu den Angriffen durch Auswertung der Blockchain ist und zur Deanonymisierung von Bitcoin Usern im Tor Netzwerk verwendet werden kann.

Die Forscher kommen zu dem Schluss, dass die Anonymität von Bitcoin geringer ist, als eine einfache Banküberweisung.

Die CIA hatte Bitcoin als Zahlungsmittel *frühzeitig auf dem Radar*. Im Juni 2011 wurde Gavin Andresen (ein führender Bitcoin Entwickler) ins CIA-Hauptquartier zu einer Präsentation eingeladen. Das US-Militär suchte bereits 2012 einen Anti-Terror Finanzexperten mit Bitcoin Erfahrung. Die Europäische Zentralbank (EZB) sieht laut einem Bericht von Okt. 2012 in Bitcoin eine Gefahr, da es außerhalb der Kontrolle der Zentralbanken läuft und empfahl eine intensivere Beobachtung.

Die Firma Chainanalysis bietet Banken, Strafverfolgung, Geheimdiensten u.ä für \$500 pro Monat eine API mit Real-Time Informationen zur Beobachtung aktuellen Transaktionen in der Blockchain. Ziel der Firma ist es, compliance mit geltenden Gesetzen zur Überwachung von Finanzströmen herzustellen. Über die API ist es möglich, scheinbar unabhängigen Bitcoin Adressen auf einen Nutzer zurück zu führen, Nutzer zu identifizieren oder *known bad actors* gezielt zu überwachen. Die geleakte Roadmap von Chainanalysis zeigt, wie es weitergehen soll. Automatisiertes Profiling der Nutzer steht auf der Liste und eine Gruppierung der Payment Prozessoren in Gruppen wie *dark markets, gambling sites....*

Das sich Geheimdienste für Bitcoin Transaktionen interessieren, kann man auch dem Trojaner RCS der italienischen Firma Hacking Team sehen. Der Trojaner, der u.a. gegen politische Aktivisten und Dissidenten eingesetzt wurde, enthält ein *Money Module*, das alle Transaktionen von Bitcoin, Litecoin, Feathercoin und Namecoin analysieren kann.<sup>19</sup>

Bitcoin ist im Zeitalter der Überwachung angekommen. Man kann davon ausgehen, das Bitcoin zukünftig in gleichem Maße überwacht wird wie Kontobewegungen oder Kreditkarten.

#### 5.6.4 Bitcoin anonym nutzen

Da das gesamte System von Bitcoin auf Informationsaustausch im Internet basiert, ist es mit Anonymisierungsdiensten möglich, Bitcoin auch vollständig anonym zu nutzen. Dabei sind folgende Punkte zu beachten:

**Bitcoin-Brieftasche anonym verwalten:** Man kann einen Webservice verwenden und mit den Anonymisierungsdiensten *JonDo+JonDoFox* oder dem *TorBrowserBundle* das eWallet anonym auf den Servern verwalten.

<sup>18</sup> <http://arxiv.org/abs/1405.7418>

<sup>19</sup> <https://bitcoinmagazine.com/21246/italian-spyware-tracks-bitcoin-transactions-private-keys/>

- Blockchain.info<sup>20</sup> bietet die Verwaltung eines anonymen eWallet auf dem Webserver und erfordert keine persönlichen Angaben bei der Registrierung.
- StrongCoin.com<sup>21</sup> erfordert die Angabe einer E-Mail Adresse bei der Registrierung. Wegwerfadressen werden akzeptiert. Das Webinterface ist für Smartphones geeignet.
- OnionBC ist ein anonymes eWallet Service, der nur als Tor Hidden Service unter [6fgd4togcynxyc1b.onion](https://6fgd4togcynxyc1b.onion) erreichbar ist. (Ich bin immer etwas skeptisch bei Tor Hidden Services. Wenn man nicht weiss, wer den Dienst betreibt, kann es sich oft um Scam handeln. TORwallet hat sich z.B. als Scam herausgestellt.)

Wenn man einem Webdienst nicht vertrauen möchte, kann man den Bitcoin Client *Electrum* installieren und den Datenverkehr mit Tor oder JonDonym anonymisieren. Electrum überlässt die Hauptarbeit speziellen Servern und muss deshalb nicht das *ewige Logfile* ständig aktualisieren. Das reduziert den Datenverkehr und ermöglicht eine sinnvolle Kombination mit JonDonym oder Tor. Die privaten Schlüssel bleiben aber immer auf dem eigenen Rechner.

**Bitcoins anonym kaufen:** Man kann beim Kauf von Bitcoins die Angabe eines Bankkontos oder anderer identifizierender Informationen vermeiden.

- Auf der Webseite LocalBitcoins.com<sup>22</sup> findet man Anbieter in der Umgebung, die Bitcoins gegen Bargeld verkaufen.
- Im IRC Channel #bitcoin-otc im Freenode Netz kann man beliebige Formen der Geldübergabe mit dem Verkäufer vereinbaren.
- In Berlin trifft sich die Bitcoin Community an jedem ersten Donnerstag im Monat im *room 77* (Graefestr. 77, 10967 Berlin-Kreuzberg). Dort findet immer jemanden, der Bitcoins gegen Bargeld verkauft.
- Wer den Anonymisierungsdienst JonDonym nutzt, kann im Bitcoin Shop der JonDos GmbH<sup>23</sup> kaufen und mit Paysafecard bezahlen. Damit kann man auch Restbeträge von Paysafecards verwenden.

**Bitcoins als Zahlungsmittel verwenden:** Beim Einkauf virtueller Güter (z.B. JonDonym Premium Codes oder eBooks, die per E-Mail zugestellt werden) gibt es keine weiteren Probleme.

Muss man beim Kauf realer Güter eine Lieferadresse angeben, dann sollte man ein anderes Bitcoin eWallet verwenden als für die anonyme Bezahlung virtueller Güter. Anderenfalls könnten auch die anonymen Zahlungen deanonymisiert werden.

---

<sup>20</sup> <https://www.blockchain.info/wallet>

<sup>21</sup> <https://www.strongcoin.com>

<sup>22</sup> <https://localbitcoins.com/>

<sup>23</sup> <https://shop.anonymous-proxy-servers.net/bin/btc-shop>

**Mixing-Services?** Im Bitcoin-Wiki werden Mixing-Services wie Blockchain Mixing Service<sup>24</sup> oder Cleanbit.org<sup>25</sup> empfohlen, um die Spuren einer Transaktion zu verwischen. Die Analyse von D. Ron und A. Shamir lässt vermuten, dass diese Mixing-Services mit entsprechendem Aufwand analysiert werden könnten und zukünftig einen potenten Angreifer nicht von einer Verfolgung der Transaktionen abhalten können.

---

<sup>24</sup> <https://blockchain.info/wallet/send-anonymously>

<sup>25</sup> <http://www.cleanbit.org/>

## Kapitel 6

# E-Mail Kommunikation

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

Fast alle E-Mail Provider bieten die Möglichkeit, die E-Mail Kommunikation im Webinterface mit einem Browser zu verwalten. Aus mehreren Gründen empfehlen wir aber, die Nutzung eines E-Mail Clients wie z.B. Mozilla Thunderbird zu bevorzugen:

- 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 anbieten. Alle diese Lösungen haben gegenüber der lokalen Verschlüsselung im E-Mail Client verschiedene 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 kann man selbst dafür sorgen, dass man seine E-Mails unbeobachtet lesen kann.

### 6.1 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 genutzt 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 (siehe weiter unten).

Eine kleine Liste von E-Mail Providern abseits des Mainstream:

- **Mailbox.org** <sup>1</sup> (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, automatisch PGP-verschlüsselte Inbox und Mailversand nur über SSL/TLS aktivierbar, DANE, IP-Adressen der Nutzer werden aus dem E-Mail Header entfernt, anonyme Accounts möglich, anonyme Bezahlung per Brief oder Bitcoin, OTP-Login mit Yubikey für Webinterface)
- **Ownbay.net** <sup>2</sup> (Provider ist auf Malta registriert, Server stehen in Deutschland, Accounts ab 1,-Euro pro Monat, DANE, IP-Adressen der Nutzer werden aus dem E-Mail Header entfernt, anonyme Accounts möglich, anonyme Bezahlung per Brief oder Bitcoin, OTP-Login für Webinterface)
- **Posteo.de** <sup>3</sup> (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, S/MIME oder PGP verschlüsselte Inbox aktivierbar, DANE, IP-Adressen der Nutzer werden aus dem E-Mail Header entfernt, anonyme Accounts möglich, anonyme Bezahlung per Brief oder Bitcoin, OTP-Login mit FreeOTP für Webinterface)
- **KolabNow** <sup>4</sup> (Groupware Hosting in der Schweiz mit Adressbuch, Kalender und E-Mail, Mailaccounts für 4.41 CHF pro Monat, Groupware für 10 CHF pro Monat, DANE, IP-Adressen der Nutzer und User-Agent Info werden aus dem E-Mail Header entfernt)
- **neomailbox.com** <sup>5</sup> (anonymes E-Mail Hosting in der Schweiz, Accounts ab \$3,33 pro Monat, anonyme Bezahlung mit Pecunix, IP-Adressen der Nutzer werden aus E-Mails entfernt)
- **aikQ.de** <sup>6</sup> (deutsche Mailprovider, Accounts ab 1,- Euro pro Monat, anonyme Accounts möglich mit Bezahlung per Brief)

---

<sup>1</sup> <https://mailbox.org>

<sup>2</sup> <https://ownbay.net>

<sup>3</sup> <https://posteo.de>

<sup>4</sup> <https://kolabnow.com>

<sup>5</sup> <http://www.neomailbox.com/services/secure-email>

<sup>6</sup> <https://www.aikq.de>

- **ETHICmail** <sup>7</sup> (Offshore registrierte Firma (Seycellen), Betreiber in Gibraltar, Server verteilt in Japan, Schweiz und Zypern, zwei Accounts ab \$11,90 pro Monat, anonyme Bezahlung mit Bitcoin möglich, Emergency-Wipe des Account per SMS möglich, Backups abschaltbar, verschlüsseltes Postfach, Schwerpunkt: bestmöglicher Schutz gegen staatlichen Zugriff)
- **runbox.com** <sup>8</sup> (privacy-engagierter norwegischer E-Mail Provider, Server stehen ebenfalls in Norwegen, Accounts ab 1,66 Dollar pro Monat)
- **Private DE Mail** <sup>9</sup> (kostenfreie, anonyme Accounts, spendenfinanziert, kein Webinterface, Tor Hidden Services für alle Protokolle)
- **RuggedInbox** <sup>10</sup> (kostenfreie, anonyme Accounts, Webinterface Javascript-frei, als Tor Hidden Service erreichbar, Server in Bulgarien, privates Freizeit-Projekt)

Für politische Aktivisten gibt es Anbieter, die insbesondere den Schutz vor staatlichem Zugriff hervorheben. Diese Anbieter werden mit Spenden finanziert. Für einen Account muss man seine politischen Aktivitäten nachweisen, aber nicht unbedingt seine Identität offen legen. Neben E-Mail Accounts werden auch Blogs und Mailinglisten angeboten.

- **Associazione-Investici** <sup>11</sup> (italienischer Provider, Server stehen bei XS4ALL in Niederlande, verwendet eigene Certification Authority für SSL-Zertifikate)
- **Nadir.org** <sup>12</sup> (deutscher Provider, Server stehen ebenfalls bei XS4ALL)
- **Aktivix.org** <sup>13</sup> (deutscher Provider, Server stehen in Brasilien)

Hinweis: es kostet Geld, einen zuverlässigen Mailservice bereitzustellen. Es ist durchaus sinnvoll, die *alles kostenlos Mentalität* für einen vertrauenswürdigen Mailprovider fallen zu lassen.

### Sicherheit der SSL/TLS-Verschlüsselung

Die Webinterfaces kann man mit dem *SSL-Test von Qualys SSL Labs* <sup>14</sup> überprüfen. Die Mailserver (SMTP, POP, IMAP) können mit dem Mailserver Test von *ssl-tools.net* <sup>15</sup> geprüft werden oder mit *CheckTLS.com* <sup>16</sup>.

- Mailbox.org: sichere Verschlüsselung, DANE
- Ownbay.net: sichere Verschlüsselung, DANE
- Posteo.de: sichere Verschlüsselung, DANE

<sup>7</sup> <https://www.ethicmail.com/>

<sup>8</sup> <https://secure.runbox.com>

<sup>9</sup> <http://pvtdm.net/en/>

<sup>10</sup> <https://ruggedinbox.com>

<sup>11</sup> [http://www.autistici.org/de/get\\_service.html](http://www.autistici.org/de/get_service.html)

<sup>12</sup> <http://www.nadir.org>

<sup>13</sup> <https://www.aktivix.org>

<sup>14</sup> <https://www.ssllabs.com/ssltest>

<sup>15</sup> <https://de.ssl-tools.net/mailservers>

<sup>16</sup> <https://www.checktls.com/>

- KolabNow.com: sichere Verschlüsselung, DANE
- aikQ.de: sichere Verschlüsselung
- neomailbox.com: sichere Verschlüsselung
- ETHICmail: Zertifikate nur mit SHA1-Signaturen
- Runbox.com: sichere Verschlüsselung

### Nicht empfohlene E-Mail Provider

Einige Gründe, warum verschiedene E-Mail Provider mit gutem Ruf nicht in die Liste der Empfehlungen aufgenommen wurden:

- 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

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 Drittteilen ein. Die ID des Hushmail Account wird beim Besuch der Webseite nach dem Login an diese Drittteilen übermittelt. Für die Privacy-Policy dieser Drittteilen übernimmt Hushmail.com keine Verantwortung.

- In der EU-Studie *Fighting cyber crime and protecting privacy in the cloud*<sup>17</sup> warnen die Autoren in Kapitel 5.4 (S. 48) vor Risiken bei der Speicherung von Daten in den USA. Aufgrund des *US PATRIOT Act* (insbesondere S. 215ff) und der *4. Ergänzung des FISA Amendments Act* ist es für US-Behörden ohne juristische Kontrolle möglich, die Kommunikation von Nicht-US-Bürgern zu beschnüffeln. Dabei ist es unerheblich, ob der Cloud- bzw. E-Mail Provider eine US-Firma ist oder nicht. Es reicht nach Ansicht der Amerikaner, wenn die Server in den USA stehen.

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.<sup>18</sup>

<sup>17</sup> <http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050>

<sup>18</sup> [https://www.privacy-handbuch.de/handbuch\\_31.htm](https://www.privacy-handbuch.de/handbuch_31.htm)

## 6.2 Mozilla Thunderbird

Informationen und Downloadmöglichkeiten für Mozilla Thunderbird stehen auf der deutschsprachigen Website des Projektes <sup>19</sup> für Windows, Linux und MacOS zur Verfügung.

Linux Distributionen enthalten in der Regel Thunderbird. Mit der Paketverwaltung kann Thunderbird und die deutsche Lokalisierung komfortabel installiert und aktualisiert werden. Debian GNU/Linux bietet eine angepasste Version von Thunderbird unter dem Namen *Icedove*.

### 6.2.1 Account erstellen

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 6.1 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.

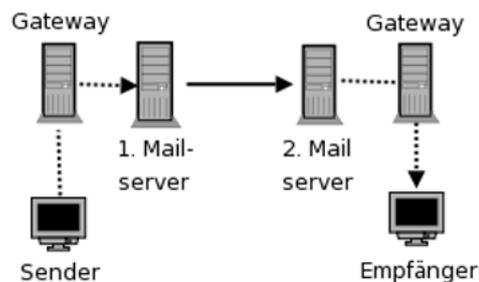


Abbildung 6.1: Der Weg einer E-Mail durch das Web

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. Aktuelle Versionen von Thunderbird aktivieren dieses Feature beim Einrichten eines

<sup>19</sup> <https://www.mozilla.org/de/thunderbird/>

Account standardmäßig.

Wie einfach es ist, unverschlüsselte Verbindungen zu belauschen, die Passwörter zu extrahieren und das Mail-Konto zu kompromittieren, wurde von T. Pritlove auf der re:publica 2007 demonstriert <sup>20</sup>.

Bewusst oder unbewusst können auch Provider die sichere Übertragung deaktivieren und damit den Traffic mitlesen. Es wird einfach die Meldung des Mail-Servers 250-STARTTLS gefiltert und überschrieben. Scheinbar verfügen alle DSL-Provider über die Möglichkeit, dieses Feature bei Bedarf für einzelne Nutzer zu aktivieren <sup>21</sup>. Die Standard-Einstellung der meisten E-Mail Clients ist *“TLS verwenden wenn möglich”*. Diese Einstellung ist genau in dem Moment wirkungslos, wenn man es braucht, weil der Traffic beschnüffelt werden soll.

Alle brauchbaren Mail-Server bieten Möglichkeit der verschlüsselten Kommunikation via SSL/TLS oder STARTTLS. Diese Option ist in Thunderbird bei der Einrichtung eines neuen Kontos zu aktivieren. Der Assistent erledigt das in der Regel automatisch.

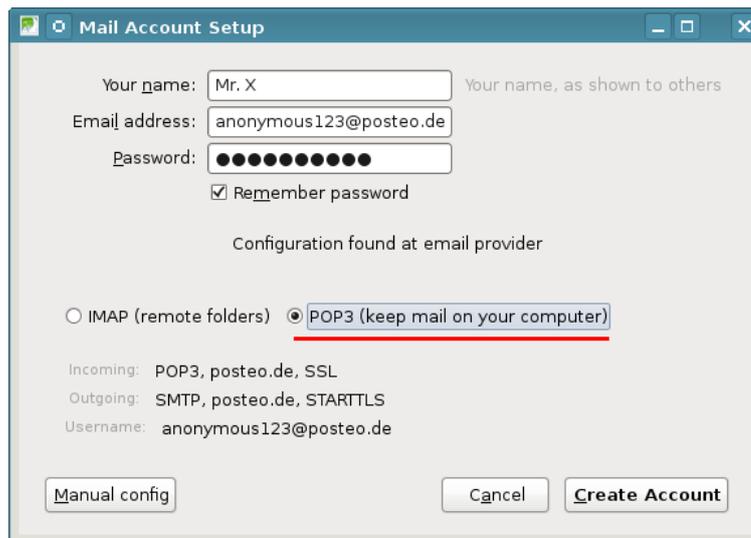


Abbildung 6.2: POP3-Account anlegen

SMTP, POP3 und IMAP sind für den Laien verwirrende Abkürzungen.

**SMTP** ist das Protokoll zum Versenden von E-Mails.

**POP3** ist das Protokoll zum Herunterladen von empfangenen E-Mails auf den lokalen Rechner. Dabei werden die E-Mails auf dem Server sofort oder einige Tage später gelöscht.

<sup>20</sup> <http://tim.geekheim.de/2007/04/24/netzwerksicherheit-auf-der-republica/>

<sup>21</sup> <http://heise.de/-206233>

Hinweis: bei POP3 wird nur der Ordner *Posteingang* vom Server geholt. Einige E-Mail Provider wie WEB.de oder GMX.de sind sich nicht sicher, ob sie Spam zuverlässig blockieren können. Sie sortieren einige Mails beim Empfang automatisch in einen Spamverdacht-Ordner, der nicht via POP3 abgerufen wird. Diese E-Mails gelten trotzdem als zugestellt, obwohl der Empfänger sie möglicherweise nie abgerufen und gelesen hat.

**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 Entwürfe werden bei der Nutzung von IMAP auf dem Mailserver des Providers gespeichert.

IMAP bietet damit die Möglichkeit, mit verschiedenen E-Mail Clients von unterschiedlichen Rechnern und Smartphones auf den Account zuzugreifen und stets Zugriff auf alle E-Mails zu haben. Die Möglichkeit des weltweiten Zugriffs auf seine Mails 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 <sup>22</sup>.

Mit der Reform der Telekommunikationsüberwachung im Dezember 2012 können Geheimdienste und Strafverfolger das Passwort für den Zugriff auf den Mail-Account ohne richterliche Prüfung vom Mail-Provider verlangen und damit Zugang zu dem Postfach erhalten. Es wäre un schön, wenn Sie dort die Kommunikation der letzten 5 Jahre vorfinden.

Deshalb empfehle ich die Nutzung von POP3 (SSL) statt IMAP (Bild 6.2).

Für viele E-Mail Provider werden automatisch sichere Einstellungen vom Assistenten vorgeschlagen (SSL bzw. STARTTLS). Wenn keine Vorschläge gefunden werden können, kann man auf *manuelle Konfiguration* klicken und in dem Dialog Bild 6.3 die Einstellungen per Hand anpassen. Die nötigen Daten für POP3- und SMTP-Server findet man auf der Webseite des Mail-Providers. Außerdem muss man in der Regel den Usernamen an die Vorgaben des Providers anpassen.

- Für den POP3-Server ist in der Regel Port 995 (SSL) passend.
- Viele SMTP-Server bieten neben STARTTLS für Port 25 auch auf den Ports 587 (STARTTLS) oder Port 465 (SSL) verschlüsselte Verbindungen zum Senden von E-Mails.

#### **Hinweis für Nutzer der Telekom-Router**

Die aktuellen Versionen der DSL-Router, die von der Telekom bereitgestellt werden, haben ein Feature, um Spambots das Versenden von E-Mails zu

<sup>22</sup> <https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-079.html>

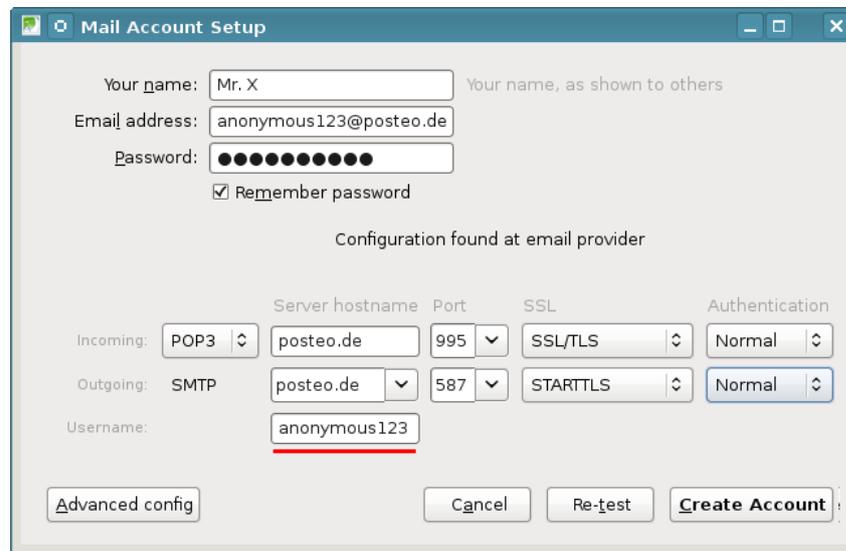


Abbildung 6.3: POP3-Account anpassen

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 eigenen 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.

## 6.2.2 Sichere Optionen für SSL/TLS-Verschlüsselung

Die IETF hat im Mai 2015 die Richtlinien für den Einsatz von TLS-Verschlüsselung überarbeitet. Es wird ausschließlich der Einsatz von TLS 1.2 empfohlen. SSLv3 darf nicht mehr genutzt werden, TLS 1.0 und TLS 1.1 sollen nicht mehr genutzt. Außerdem sollen folgende Cipher für die Transportverschlüsselung genutzt werden:

```
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
```

(Aufgrund des Logjam Angriff auf TLS empfehle ich nur die ersten beiden Cipher, da nicht sicher ist, ob der Mail-Server gute DH-Parameter nutzt.)

Die E-Mail Provider können diese Empfehlungen nicht vollständig umsetzen, da es noch zuviele E-Mail Clients gibt, die diese sicheren Cipher (noch) nicht unterstützen. Um IETF-konforme, sichere SSL/TLS-Verschlüsselung für den Transport vom/zum Mail-Server zu erzwingen, kann man in Thunderbird selbst Hand anlegen in den *Erweiterten Einstellungen* die folgenden Optionen setzen:

- TLS v1.2 erzwingen:

```
security.tls.version.min = 3
```

- Alle Cipher bis auf die als sicher eingestuft sind deaktivieren, da bleibt bei Thunderbird 31.x ESR nur ein Cipher übrig:

```
security.ssl3.ecdhe_rsa_aes_128_gcm_sha256 = true
security.ssl3.* = false
```

- Insecure Renegotiation verbieten:

```
security.ssl.require_safe_negotiation = true
security.ssl.treat_unsafe_negotiation_as_broken = true
```

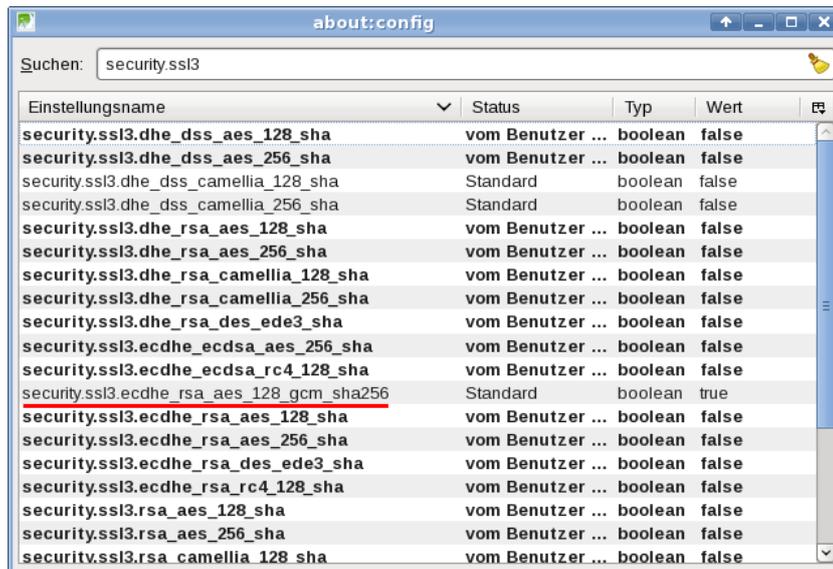


Abbildung 6.4: Konfiguration der SSL/TLS-Einstellungen für Thunderbird

### Add-on Installation

Die Installation und das automatische Update von Add-ons ist mit diesen SSL-Einstellungen im Thunderbird nicht mehr möglich, weil die Mozilla Server [services.addons.mozilla.org](http://services.addons.mozilla.org) und [versioncheck.addons.mozilla.org](http://versioncheck.addons.mozilla.org)

die aktuell empfohlenen SSL-Cipher nicht unterstützen und nur schwachen Parameter für den Diffie-Hellman Schlüsseltausch verwenden.

Man kann die gewünschten Add-on mit dem Browser von der Webseite [addons.mozilla.org](https://addons.mozilla.org) herunterladen und in der Add-on Verwaltung von Thunderbird aus der Datei installieren. Linux User finden viele nützliche Add-ons auch in den Repositories der Distribution. Die Pakete heißen meist *xul-ext-\**.

### Verbindungsprobleme

Wenn man die im Bild 6.5 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. Oft bietet der Mail-Server keine *Secure Renegotiation* beim Aufbau der verschlüsselten Verbindung an. Das Problem wird seit 2009 als schwebend eingestuft<sup>23</sup>. 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*).

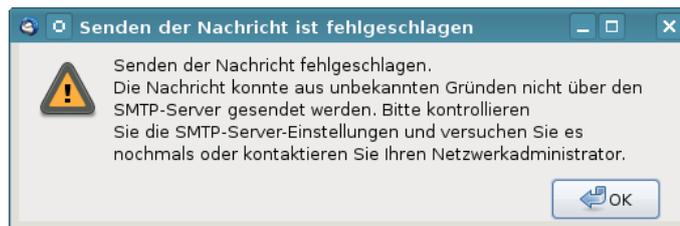


Abbildung 6.5: Fehlermeldung bei unsicherer Verbindung

### SSL-Zertifikate mit DANE/TLSA prüfen (Linux)

IT-Sicherheitsforscher der EFF.org kamen bereits 2009 in einer wiss. Arbeit zu dem Schluss, dass Geheimdienste schwer erkennbare man-in-the-middle Angriffe mit gültigen SSL-Zertifikaten durchführen können. Dieser Angriff wird als *Lawful SSL Interception* bezeichnet. Firmen für Überwachungstechnik wie die deutsche Firma Utimaco bieten fertige Appliances dafür.

Gute E-Mail Provider veröffentlichen die SHA2-Hashes der SSL-Zertifikate für SMTP-, POP3- und IMAP-Server im DNS via DANE/TLSA Record, um diese Angriffe zu verhindern. Leider kann Thunderbird die SSL-Zertifikate (noch) nicht via DANE/TLSA überprüfen.

Linuxer können mit Kommandozeilentools wie z.B. *danetool* von GnuTLS prüfen, ob beim Aufbau einer verschlüsselten Verbindung zu den Mailservern

<sup>23</sup> <https://www.verbraucher-sicher-online.de/news/fehlerhaftes-design-im-wichtigsten-verschluesselungsprotokoll-fuer-angriffe-nutzbar>

das richtige Zertifikat verwendet wird oder ob ein Angriff mit einem Fake-Zertifikate erfolgt.

Als erstes ist GnuTLS zu installieren. Dabei muss man die Software selbst compilieren, da die Linux Distributionen das Paket *gnutls-bin* ohne DANE-Support erstellen. Dafür benötigt man auch einige Entwickler-Pakete, die man mit dem bevorzugten Paketmanager isnatllieren kann. Für Debian/Ubuntu funktioniert das folgende Kommando:

```
> sudo aptitude install gcc make libgmp-dev libidn11-dev zlib1g-dev nettle-dev libunbound-dev
```

Debian 7.x *wheezy* ist etwas älter und benötigt die letzten beiden Pakete in einer aktuelleren Version aus den Backports:

```
> sudo aptitude install -t wheezy-backports nettle-dev libunbound-dev
```

Nach dem Download der aktuellen Sourcen von der Webseite [gnutls.org](http://gnutls.org) ist das Paket zu entpacken und mit dem üblichen Dreisatz zu installieren. Einige überflüssige Features kann man dabei deaktivieren:

```
> cd /usr/src/gnutls-3.3.14.
> ./configure --disable-ocsp --disable-doc --disable-tests.
> make.
> sudo make install.
```

Danach kann man mit dem Kommando *danetool -check* prüfen, ob das richtige Zertifikat für die Verschlüsselung verwendet werden würde, wenn man den SMTP, POP3 oder IMAP Server kontaktiert. Als Beispiel der Test eines SMTP Servers:

```
> danetool --check smtp.mailbox.org --port 465
Resolving 'smtp.mailbox.org'...
Obtaining certificate from '80.241.60.196:465'...
....
Verification: Certificate matches.
```

Und das gleiche nochmal für den POP3 Server:

```
> danetool --check pop3.mailbox.org --port 995
Resolving 'pop3.mailbox.org'...
Obtaining certificate from '80.241.60.199:995'...
....
Verification: Certificate matches.
```

Es ist mühsam, vor dem Lesen oder Schreiben von E-Mails jedesmal ein Terminal zu öffnen, die seltsamen Befehle einzutippen und dann erst Thunderbird zu starten. Mit einem Startscript für Thunderbird oder jeden anderen E-Mail Client kann man den Test automatisieren und vor dem Start prüfen, ob die Zertifikate ok sind. Dabei der wird der Rückgabewert von *danetool* ausgewertet und eine Meldung angezeigt, wenn Fehler auftreten:

```
#!/bin/bash

# Check des SMTP Servers
danetool --check smtp.mailbox.org --port 465
if [ $? -ne 0 ]; then
    # SSL Zertifikatsfehler! Warnung und Abbruch
    zenity --error --text="DANE/TLSA Fehler bei SMTP Server!" --no-wrap
    exit 0
fi

# Check des POP3 Servers
danetool --check pop3.mailbox.org --port 995
if [ $? -ne 0 ]; then
    # SSL Zertifikatsfehler! Warnung und Abbruch
    zenity --error --text="DANE/TLSA Fehler bei POP3 Server!" --no-wrap
    exit 0
fi

# alles ok, Thunderbird kann starten
thunderbird
```

Das Prinzip ist einfach erkennbar und jeder Linuxer kann es selbst an die Mail Server von Posteo.de, Ownbay.net oder Kolab oder anpassen und ergänzen - oder?

Script kann man von meiner Webseite herunter laden und nach den nötigen Anpassungen z.B. nach `$HOME/.local/bin/` kopieren und als ausführbares Script kennzeichnen:

```
> install -d $HOME/.local/bin
> cp Downloads/thunderbird_mit_danetest.sh $HOME/.local/bin
> chmod +x $HOME/.local/bin/thunderbird_mit_danetest.sh
```

Danach kann man in der Desktop Umgebung die Einstellungen für den bevorzugten E-Mail Client anpassen, einen Menüeintrag oder Starter auf dem Desktop erstellen, um das Script als E-Mail Client aufzurufen.

Einige kleine Vorschläge für Anpassungen:

- Im Beispiel habe ich das Tool *zenity* für die Anzeige der Warnung verwendet. Wer den KDE Desktop bevorzugt, möchte vielleicht lieber *kdialog* verwenden. Dann kann man die Zeilen für die Anzeige der Warnung (vor den *exit* Kommandos) austauschen:

```
kdialog --error "DANE/TLSA Fehler bei SMTP Server!"
```

- Wenn man Anonymisierungsdienste verwendet, kann man *proxychains* mit *danetool* nutzen, um z.B. die SSL Verbindung über die JonDonym Mixkasakde zu testen.

```
proxychains danetool --check .....
```

Bei Tor ist der Test vielleicht weniger aussagekräftig, weil die Route durch das Tor Netzwerk häufig wechselt. Wenn man 15min nach dem Test eine neu geschriebene E-Mail endlich abschickt, dann wird eine andere Route mit einem anderen Tor Exit Node verwendet und das Testergebnis von *danetool* ist hinfällig.

- Wenn man mehrere Profile in Thunderbird verwendet (z.B. *default* und *anonym mit JonDo/Tor*), dann möchte man am Ende mit dem letzten Kommando gleich das passende Profil starten. Das funktioniert mit folgender Option für Thunderbird/Icedove:

```
thunderbird -P "r3wq6m51.default"
```

Der Name des Profils ist selbst anzupassen. Wenn man einen anderen E-Mail Client verwendet, ist der letzte Befehl zu ersetzen (z.B. kmail, evolution...).

### 6.2.3 Sichere Konfiguration des E-Mail Client

Einige Hinweise für die sichere und unbeobachtete Nutzung des Mediums E-Mail mit Mozilla Thunderbird:

- 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. Am einfachsten deaktiviert man diese Features, wenn man nur die Anzeige von *Reinem Text* zulässt. Die Option findet man im Menüpunkt *Ansicht* -> *Nachrichtentext* (siehe Bild 6.6).

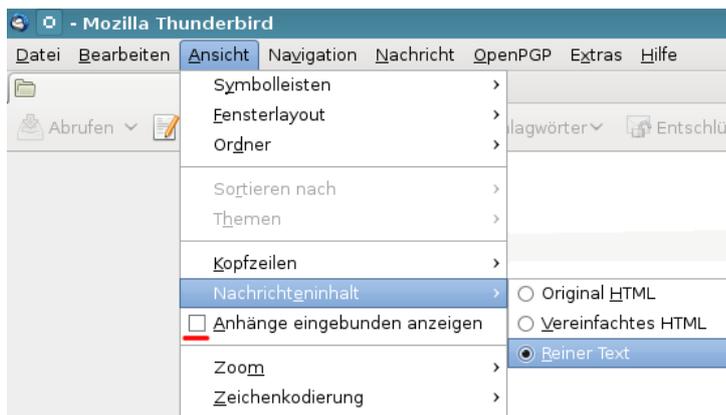


Abbildung 6.6: E-Mails als reinen Text darstellen

- 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 einem Trojaner zu infizieren.

- Es ist nicht immer möglich, E-Mails als Plain Text zu lesen. Viele Newsletter sind nur als HTML-Mail lesbar, eBay verwendet ausschließlich HTML-Mails für Benachrichtigungen usw. In der Regel enthalten diese HTML-only Mails mehrere Trackingelemente.

Um diese E-Mails trotzdem lesen zu können (wenn auch nicht in voller Schönheit), kann man die Darstellung *Vereinfachtes HTML* nutzen. Außerdem können folgende Features in den *Erweiterten Einstellungen* deaktiviert werden, die jedoch nur für die Darstellung von *Original HTML* relevant sind:

```

javascript.enabled           = false
network.cookie.cookieBehavior = 2
dom.storage.enabled         = false
geo.enabled                  = false
webgl.disabled               = true
layout.css.visited_links_enabled = false
gfx.downloadable_fonts.enabled = false
network.http.sendRefererHeader = 0
network.http.use-cache       = false

```

- Alle Bilder in HTML-Mails, die von einem externen Server geladen werden, können direkt mit der E-Mail Adresse des Empfängers verknüpft sein. Anhand der Logdaten kann der Absender erkennen, wann und wo die E-Mail gelesen wurde. Einige Newsletter verwenden auch HTML-Wanzen. Im Newsletter von Paysafecard findet man beispielsweise ganz unten eine kleine 1x1-Pixel Wanze, die offenbar mit einer individuellen, nutzerspezifischen URL von einem Trackingsservice geladen wird:

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

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

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

Um Tracking mit Bildern und HTML-Wanzen zu verhindern, kann man in den *Erweiterten Einstellungen* das Laden externer Bilder blockieren:

```
permissions.default.image = 2
```

Auch andere Medienformate können von einem externen Server geladen und als Wanzen genutzt werden. Einen 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.

- Die *extension blocklist* kann Mozilla nutzen, um einzelne Add-ons in Thunderbird zu deaktivieren. Es ist praktisch ein kill switch für Thunderbird 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 das Feature 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
```

- Gespeicherte Passwörter für den Zugriff auf SMTP-, POP- oder IMAP-Server können mit einem Masterpasswort geschützt werden.

#### 6.2.4 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. Hierzu ist mit der rechten Maustaste auf den Ordner zu klicken und der Punkt *Komprimieren* zu wählen. Während des Komprimierens sollten keine anderen Aktionen in Thunderbird ausgeführt werden.

Alternativ kann man in den Einstellungen von Thunderbird in der Sektion *Erweitert* auch eine automatische Komprimierung konfigurieren, sobald es lohnenswert ist (siehe Bild 6.7). Bei jedem Start prüft Thunderbird, ob die Ordner komprimiert werden können.

- Regelmäßig sollten Backups des gesamten Profils von Thunderbird angelegt werden. Unter WINDOWS sichert man *C:/Dokumente und Einstellungen/<NAME>/Anwendungsdaten/Thunderbird*, unter Linux ist *\$HOME/.thunderbird* zu sichern.

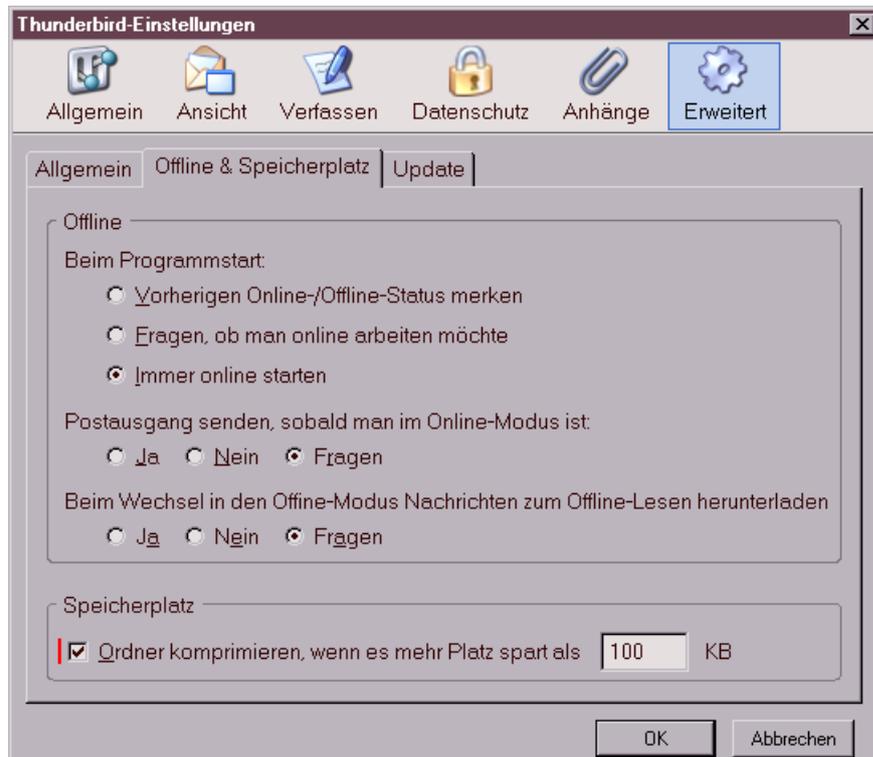


Abbildung 6.7: Ordner automatisch komprimieren

### 6.2.5 Wörterbücher installieren

Nach der Installation von Thunderbird sind keine Wörterbücher für die Rechtschreibkontrolle vorhanden. Die Wörterbücher müssen zusätzlich in-

stalliert werden, wenn man auf das Feature nicht verzichten möchte. Nach dem Download der Wörterbücher <sup>24</sup> 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 6.8, kann man die Dateien mit den Wörterbüchern als Add-on installieren.

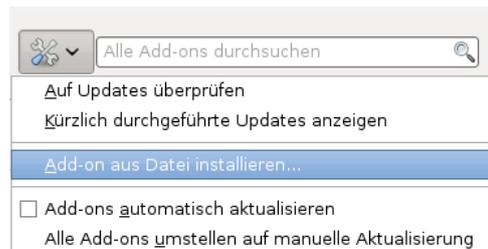


Abbildung 6.8: Wörterbücher in der Add-on Verwaltung installieren

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.

### 6.2.6 X-Mailer Kennung modifizieren

Ich habe gelesen, dass es böse Buben geben soll, die via Internet ihre Software auf fremden Rechnern installieren möchten. In diesem Zusammenhang werden oft die Stichworte "Spambot" oder "Bundstrojaner" genannt.

Voraussetzung ist die Kenntnis der vom Opfer genutzten Software. Genau wie jeder Webbrowser sendet auch Thunderbird eine User-Agent-Kennung im Header jeder E-Mail, die Auskunft über die genutzte Programmversion und das Betriebssystem liefert. Das folgende (veraltete) Beispiel stammt aus der Mail eines Unbekannten:

```
...
User-Agent: Thunderbird 2.0.0.6 (X11/20070728)
X-Enigmail-Version: 0.95.3
...

----- BEGIN PGP MESSAGE -----
Version: GnuPG v1.4.6 (GNU/Linux)
...
```

Aha, er nutzt also Thunderbird in der Version 2.0.0.6 unter Linux, hat die Enigmail-Erweiterung v.0.95.3 installiert und verwendet die GnuPG-Version 1.4.6. Das war damals eine typische Kombination für Ubuntu Edgy.

<sup>24</sup> <https://addons.mozilla.org/de/thunderbird/language-tools/>

Die User-Agent-Kennung kann in den erweiterten Einstellungen modifiziert werden. Im Einstellungs-Dialog findet man in der Sektion *Erweitert* den Reiter *Allgemein*. Ein Klick auf den Button Konfiguration bearbeiten öffnet eine Liste aller Optionen.

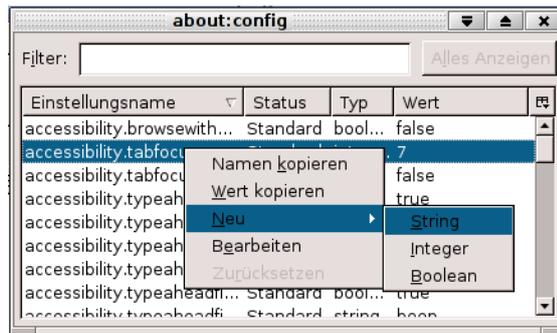


Abbildung 6.9: Neue Config-Variable anlegen

Hier fügt man die neue String-Variable **general.useragent.override** als neuen Wert ein, indem man mit der rechten Maustaste auf einen freien Bereich klickt und im Kontext-Menü den Punkt *Neu - String* wählt. Als Wert für diese Variable wird eine leere Zeichenkette eingesetzt. Damit sendet Thunderbird keine Kennung mehr. Nachteile sind nicht erkennbar.

Wer das Add-on Enigmail für die Verschlüsselung nutzt, sollte dem Add-on die Geschwätzigkeit abgewöhnen und die Ausgabe von Versionen im Header deaktivieren. Anderenfalls kann ein Schnüffler anhand einer signierten oder verschlüsselten E-Mail Schlussfolgerungen über die verwendete Software ableiten. Folgende Parameter sind in den erweiterten Einstellungen zu setzen:

```

extensions.enigmail.addHeaders           = false
extensions.enigmail.useDefaultComment    = true
extensions.enigmail.agentAdditionalParam = --no-emit-version

```

## 6.2.7 Spam-Filter aktivieren

Das Mozilla Team bezeichnet nicht erwünschte E-Mails (Spam) als Junk. Den integrierten lernfähigen Filter aktiviert man über den Menüpunkt *Extras -> Junk-Filter*.

Im Einstellungsdialog des Filters sollte man die beiden Optionen für das automatische Verschieben der Junk-Mails in einen speziellen Ordner aktivieren, am einfachsten in den Ordner *Junk* des entsprechenden Kontos. Außerdem sollte der lernfähige Filter aktiviert werden. Ich bin immer wieder von der guten Erkennungsrate beeindruckt.

### 6.2.8 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.

#### AnonBox des CCC

Bei der AnonBox.net des CCC <sup>25</sup> kann ein E-Mail Account für den Empfang von einer Nachricht erstellt werden. Der Account ist bis 24:00 Uhr des folgenden Tages gültig und nicht verlängerbar. Eingehende Nachrichten kann man nur im Webinterface lesen und sie werden nach dem Abrufen gelöscht. Sie können 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 ankommende Mails 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.

Die AnonBox bietet SSL-Verschlüsselung und verwendet ein Zertifikat, das von CAcert.org signiert wurde. In den meisten Browsern ist diese CA nicht als vertrauenswürdig enthalten. Das Root-Zertifikat dieser CA muss von der Webseite zusätzlich importiert werden.

#### 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

---

<sup>25</sup> <https://anonbox.net>

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):

- <http://discard.email> (weitere Domains auf der Webseite, Account kann mit Passwort gesichert werden, Schreiben von E-Mails ist 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)
- <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](http://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)

### Firefox Add-on Bloody Vikings

Die Firefox Add-ons *Bloody Vikings* <sup>26</sup> und der JonDoFox vereinfacht die Nutzung von Wegwerfadressen. Nach der Installation von der Webseite kann ein bevorzugter Dienst für die Wegwerfadressen gewählt werden.

---

<sup>26</sup> <https://addons.mozilla.org/de/firefox/addon/bloody-vikings>

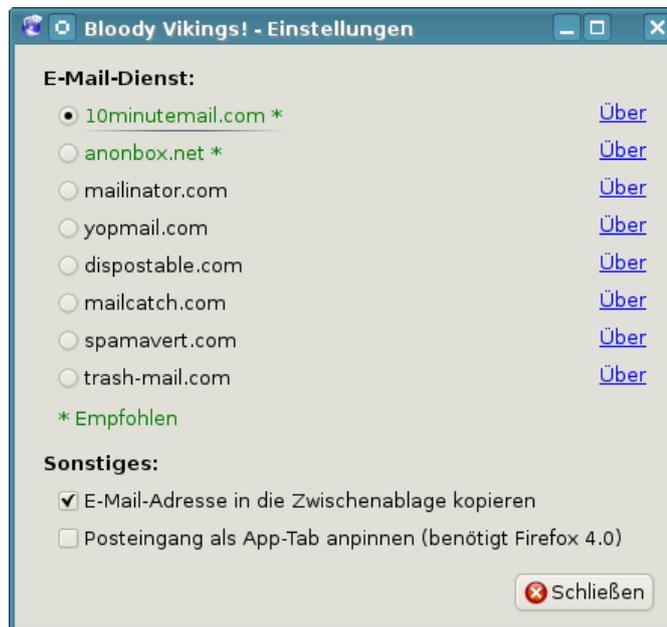


Abbildung 6.10: Bloody Vikings konfigurieren

In Zukunft kann man in jedem Anmeldeformular mit der rechten Maustaste auf das Eingabefeld der E-Mail Adresse klicken und aus dem Kontextmenü den Punkt *Bloody Vikings* wählen. Es wird in einem neuen Browser Tab die Webseite des Anbieters geöffnet und die temporäre E-Mail Adresse in das Formularfeld eingetragen. Nach dem Absenden des Anmeldeformular wechselt man in den neu geöffneten Browser Tab und wartet auf die Bestätigungsmail.

### 6.2.9 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, das 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 folgende Dienste der Firma *insophia* nutzen:

- *Certified Privnote*<sup>27</sup> ist vom ULD mit dem EuroPrise Siegel zertifiziert. Die Zertifizierung garantiert die Respektierung der Privatsphäre der Nutzer durch den Anbieter.

<sup>27</sup> <https://certified.privnote.com>

- *Privnote*<sup>28</sup> ist eine nicht-zertifizierte Version. Damit sind Änderungen an der Software und Weiterentwicklungen möglich.

Man schreibt die Nachricht auf der Webseite des Anbieters und klickt auf den Button *Create Note*. Javascript muss dafür freigegeben werden. Es wird ein Link generiert, unter dem man die Nachricht EINMALIG abrufen kann. Die Daten werden verschlüsselt auf dem Server gespeichert und nur der Link enthält den Key, um die Daten zu entschlüsseln.

Den Link sendet man per E-Mail dem Empfänger der Nachricht. 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.

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 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.

Es gibt einige ähnliche Projekte, die ich NICHT empfehle:

- *Burn Note* erfordert eine Registrierung mit E-Mail Adresse, was überflüssig ist. Für jeden Account wird die Nutzung des Dienstes protokolliert und eine monatliche Statistik erstellt. Außerdem werden die Notes mit einem Key verschlüsselt, der auf dem Server von Burn Note gespeichert wird. Im Gegensatz zu den Privnote-Diensten von *insophia* ist der Betreiber damit in der Lage, die Nachrichten zu entschlüsseln.
- *Road-Message* sammelt aus meiner Sicht zuviel Daten. Beim Besuch der Webseite wird beispielsweise die innere Größe des Browserfensters ausgelesen, was ein sehr individueller Wert ist und gut für das Tracking nutzbar. Es gibt keine Privacy Policy auf der Webseite, welche Daten gespeichert werden und wie die Daten genutzt werden. Auch bei *Road-Message* wird der Schlüssel für das Entschlüsseln der Nachricht nicht in der URL kodiert (wie bei den Diensten von *insophia*) sondern auf dem Server gespeichert.

### 6.2.10 RSS-Feeds

RSS-Feeds bieten die Möglichkeiten, sich schnell über Neuigkeiten in häufig gelesenen Blogs zu informieren ohne die Webseiten einzeln abklappern zu

---

<sup>28</sup> <https://privnote.com>

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 6.11 dargestellt.

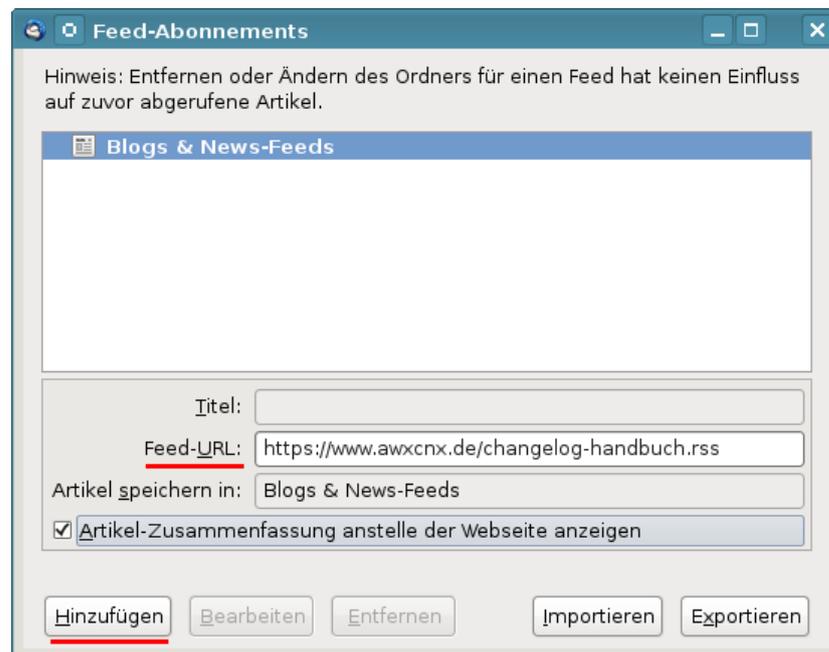


Abbildung 6.11: RSS-Feed hinzufügen

Die Neuigkeiten aus den Blogs kann man zukünftig wie E-Mails lesen. Dabei kann man eine simple Textanzeige wählen oder die Ansicht als Webseite. Wer die Ansicht als Webseite bevorzugt, sollte Javascript, Cookies und andere

Tracking Elemente deaktivieren. Zum Kommentieren muss man allerdings die Webseite des Blogs im Browser aufrufen.

### 6.2.11 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. In der Version 16.0 unterstützt Thunderbird die Filehoster YouSendIt<sup>29</sup> und Box.net<sup>30</sup> sowie Ubuntu One.

Ich kann dieses Feature nicht empfehlen.

1. YouSendIt protokolliert alle Aktivitäten und die Protokolle werden für drei Jahre gespeichert:

*YouSendIt will retain the Log Data collected from you in its active, internal company databases for up to six months, at which point it will migrate such Log Data to its offline archival systems, where YouSendIt will retain the Log Data for a period of three years.*

2. Die bei einem Cloud-Service gespeicherten Dateianhänge unterliegen nicht dem besonderen Schutz des Post- und Fernmeldegeheimnisses.
3. Außerdem ist das Filelink 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. Dann kann man sie auch gleich selbst zu einem 1-Click-Hoster hochladen.

Um nicht ständig mit der Frage belästigt zu werden, ob man einen großen Dateianhang bei einem Cloude-Anbieter speichern möchte, kann man das Feature in den Einstellungen deaktivieren.

## 6.3 ProtonMail und Lavaboom

Durch die Veröffentlichungen von Snowden/Greenwald sind viele hochmotivierte IT-Aktivisten angefeuert, neue Ideen und Konzepte für privacy-freundliche Dienste zu entwickeln. Die E-Mail Dienste ProtonMail.ch<sup>31</sup> (Schweiz), unseen.is<sup>32</sup> (Island), Lavaboom.com<sup>33</sup> (Deutschland), SCRYPT-mail<sup>34</sup> (early Beta) und Tutanota.de<sup>35</sup> möchte ich kurz vorstellen. Die Angebote sind derzeit noch als Beta anzusehen (Stand: Mai 2014).

Diese E-Mail Dienste stellen einfache Benutzbarkeit von Verschlüsselung (DAU-kompatibel im Nerd-Slang) sowie Kompatibilität mit den gängigen

---

<sup>29</sup> <https://www.yousendit.com>

<sup>30</sup> <https://www.box.com/>

<sup>31</sup> <https://protonmail.ch>

<sup>32</sup> <https://unseen.is>

<sup>33</sup> <https://lavaboom.com>

<sup>34</sup> <https://scryptmail.com>

<sup>35</sup> <https://tutanota.de>

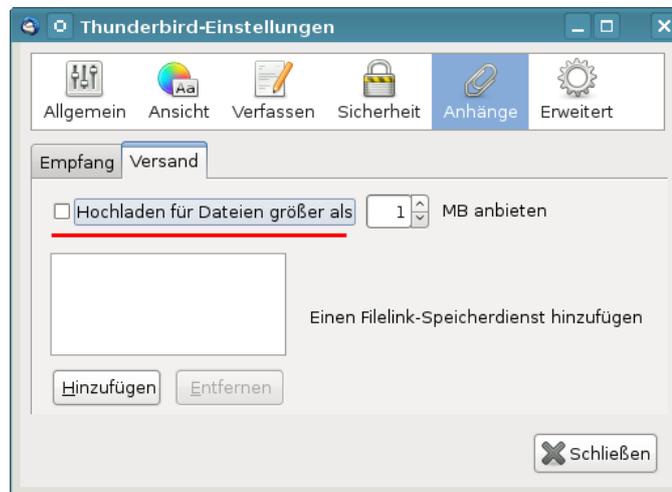


Abbildung 6.12: Filelink deaktivieren

E-Mail Protokollen in den Vordergrund und bemühen sich (im Rahmen der Möglichkeiten) um max. Schutz gegen staatlichen Zugriff.

Das Schreiben und Lesen von E-Mails erfolgt ausschließlich im Webinterface im Browser. Das ermöglicht eine einfach nutzbare Verschlüsselung der Inhalte der Kommunikation mit einer Krypto-Implementierung in Javascript.

Die Daten werden verschlüsselt auf den Servern abgelegt. die Betreiber werben damit, dass sie keinen Zugriff auf den Klartext der Kommunikation haben. Die Kommunikation mit Partnern innerhalb des Dienstes ist automatisch Ende-zu-Ende verschlüsselt. Bei der Kommunikation mit Nutzern anderer E-Mail Provider ist Verschlüsselung möglich, aber nicht immer automatisch.

### Zu den Schwächen

Konzeptionell bedingt haben beide Dienste einige Schwächen, die man kennen sollte:

- 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 Cryptocat (für Chats) und die Kritiken an diesem Konzept lassen sich auch für die oben genannten Dienste übernehmen.
  - Die Server-basierte Kryptografie von Hushmail wurde bereits 2007 von der US Drogenbehörde DEA kompromittiert<sup>36</sup>. Hushmail wur-

<sup>36</sup> <http://www.wired.com/2007/11/encrypted-e-mai>

de 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 o.ä. generell nicht geeignet wie Patrick Ball in einem Essay bei Wired.com<sup>37</sup> ausführlich dargelegt.
- Javascript ist für die Implementierung starker Kryptografie nur bedingt geeignet<sup>38</sup>. Einige Probleme können mit sorgfältiger, aufwändiger Programmierung umgangen werden.

Andere Probleme sind mit Javascript im Browser nicht lösbar. Javascript bietet z.B. keine Möglichkeit, bestimmte Speicherbereiche im Hauptspeicher (RAM) zu überschreiben. Es ist nicht möglich, verwendete Keys nach der Nutzung sicher zu löschen. Es bleiben Daten im Speicher zurück, wo sie durch eine Schadsoftware ausgelesen werden könnten. Bei Tor war dieses Verhalten ein schwerer Bug<sup>39</sup>, aber bei der Verschlüsselung von Mails wird dieses Verhalten einfach pauschal akzeptiert?

- Webanwendungen bieten viel mehr Angriffsmöglichkeiten als E-Mail Clients mit lokalen Tools zur Verschlüsselung. Thomas Roth demonstriert in dem Video Hacking protonmail - with a browser, wie man die Verschlüsselung von ProtonMail mit einem Browser und einfachen XSS-Hacks angreifen konnte.<sup>40</sup>
- Die Schlüssel werden im HTML5 Storage des Browsers gespeichert und sind somit durch Webanwendungen leichter angreifbar. G. Greve (CEO bei MyKolab) sieht diesen Punkt als entscheidenden Nachteil und lehnt es deshalb ab, eine vergleichbare Lösung für MyKolab.com zu implementieren.
- Die alternative Nutzung starker Kryptografie wie OpenPGP oder S/MIME ist bei einigen oben genannten Diensten nicht möglich, auch wenn der Kommunikationspartner einen Public Key bereitstellt und technisch dazu in Lage wäre.
- Diese Provider wollen kompatibel mit dem gängigen E-Mail Protokoll sein und können somit Metadaten der Kommunikation NICHT schützen. Diese Dienste bieten keine echte *zero knowledge privacy*, wie Lavaboom behauptet.

Es gibt Lösungen für asynchrone Kommunikation mit Text-Nachrichten (sozusagen: E-Mail ähnlich), die wirklich *zero knowledge privacy* bieten. State-of-the-Art auf diesem Gebiet sind z.B. I2P-Bote oder POND. (Die Nutzung dieser Dienste ist aber wesentlich komplizierter.)

<sup>37</sup> [http://www.wired.com/2012/08/wired\\_opinion\\_patrick\\_ball/all/](http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/)

<sup>38</sup> <http://www.matasano.com/articles/javascript-cryptography/>

<sup>39</sup> <http://heise.de/-1746523>

<sup>40</sup> <http://vimeo.com/99599725>

**Schlussfolgerung:** ProtonMail.ch, unseen.is, Lavaboom.com und Tutanota.de bieten viele Vorteile für Normalanwender, die Ihre E-Mails bisher im Webinterface von GMail, Yahoo! oder Hotmail bearbeiten. Sie sind allerdings nicht State-of-Art im Bereich anonyme, unbeobachtete Kommunikation und die Verschlüsselung bietet nicht die gleiche Sicherheit lokal installierter Tools wie GnuPG. Man sollte die Grenzen kennen und diese Dienste entsprechend nutzen.

## Kapitel 7

# 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 abgeschnorchelten 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.

Mit dem **Verschlüsseln** von E-Mails wird die Vertraulichkeit der Kommunikation gewährleistet. Eine Nachricht kann nur vom Empfänger geöffnet und gelesen werden.

### Asymmetrischen Verschlüsselung

- 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 der Anwender Anton eine signierte E-Mail an die Anwenderin Beatrice senden will, erstellt er eine Signatur mit *seinem geheimen Schlüssel*. Die Anwenderin Beatrice kann mit dem *öffentlichen Schlüssel von Anton* die Nachricht verifizieren, da nur Anton Zugriff auf seinen geheimen

Schlüssel haben sollte.

- Wenn Beatrice eine verschlüsselte Nachricht an Anton senden will, nutzt sie den *öffentlichen Schlüssel von Anton*, um die Nachricht zu chiffrieren. Nur Anton kann diese E-Mail mit seinem geheimen Schlüssel dechiffrieren und lesen.

Mit OpenPGP und S/MIME haben sich zwei Standards etabliert:

- **OpenPGP:** PGP (Pretty Good Privacy) und die kostenlose Alternative GnuPG (GNU Privacy Guard) stellen für die Verschlüsselung eine lang erprobte Software zur Verfügung. In der Regel können gängige E-Mail Programme nicht out-of-the-box mit OpenPGP umgehen. Installation zusätzlicher Software ist nötig. Dafür ist es relativ einfach, die nötigen Schlüssel zu erzeugen. Für den Austausch der Schlüssel stellt das Internet eine ausgebaute Infrastruktur bereit.
- **S/MIME:** Das Secure MIME Protokoll (S/MIME) wurde 1998 entwickelt und ist heute in den meisten E-Mail Clients integriert. Es werden Zertifikate nach dem Standard X.509 für die Verschlüsselung genutzt. Diese Zertifikate werden von einer Certification Authority (CA) ausgestellt und beglaubigt. Es ist nötig, gegenüber der CA die Identität des Nutzers mit Ausweisdokumenten nachzuweisen.

## 7.1 GnuPG und Thunderbird

Die folgende Anleitung erläutert den Einsatz von **GnuPG** in Kombination mit **Thunderbird**, dem E-Mail Client der Mozilla Foundation. Alle Komponenten stehen für Linux, Mac OS und WINDOWS kostenfrei zur Verfügung:

### 7.1.1 Installation von 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 2.0.x.

**Windows:** Das Projekt [gpg4win](http://www.gpg4win.org) <sup>1</sup> stellt ein Paket für Windows bereit mit GnuPG v. 2.0, dem GNU Privacy Assisten für die Schlüsselverwaltung und einer Erweiterung für den Windows Explorer.

**MacOS:** nutzen Sie die GPGTools <sup>2</sup>.

**Linux, BSD:** installieren GnuPG 2.0 nicht immer standardmäßig. In der Regel muss man es nachträglich installieren. Für Debian/Ubuntu funktioniert:

```
> sudo apt-get install gnupg2 gpg-agent pinentry-gtk2 gpgsm sddaemon
```

Bei einigen Linux Distributionen ist *gpg-agent* im Paket *gpgsm* enthalten. Der *gpg-agent* 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
```

### 7.1.2 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:

---

<sup>1</sup> <http://www.gpg4win.org>

<sup>2</sup> <http://www.gpgtools.org>

```
# keine Informationen über ersion 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 Oxlong

# Keyserver-URLs in Keys ignorieren (Tracking möglich)
keyserver-options no-honor-keyserver-url

# Empfohlene Präferenzen für Schlüsselgenerierung vom
# Debian-Team: http://keyring.debian.org/creating-key.html
personal-digest-preferences SHA512
cert-digest-algo SHA512
default-preference-list SHA512 SHA384 SHA256 SHA224 AES256 AES192
                        AES CAST5 ZLIB BZIP2 ZIP Uncompressed

# sonstiges
fixed-list-mode
verify-options show-uid-validity
list-options show-uid-validity
```

### 7.1.3 Installation der Enigmail-Erweiterung

Enigmail <sup>3</sup> ist eine Erweiterung für Mozilla Thunderbird, welche eine Schnittstelle zu GnuPG bereitstellt und den Umgang mit Verschlüsselung im täglichen E-Mail Chaos vereinfacht. Am einfachsten installiert man Enigmail mit dem Add-on Manager von Thunderbird. Den Manager findet man unter *Extras - Add-ons*. Im Suchfeld gibt man *Enigmail* ein. Ein Klick auf den Button *Installieren* holt das Add-on.

Unter Linux kann man Enigmail auch mit dem bevorzugten Paketmanager installieren. Für Debian und Ubuntu kann man *aptitude* nutzen:

```
> sudo apt-get install enigmail
```

Unter NetBSD und OpenBSD muss man Thunderbird mit Enigmail neu kompilieren. In der Datei *mk.conf* ist dafür folgende Option zu setzen:

```
PKG_OPTIONS.thunderbird=mozilla-enigmail
```

Nach Installation von Enigmail muss Thunderbird neu gestartet werden! Nach dem Neustart kann man den Konfigurations-Assistenten unter *OpenPGP - OpenPGP-Assistent* aufrufen. Dabei werden folgende Schritte durchlaufen:

1. Abfrage, ob gesendete E-Mails standardmäßig signiert und verschlüsselt werden sollen. Um unbedarfte Anwender nicht zu verwirren, kann man diese Funktion deaktivieren.

---

<sup>3</sup> <http://enigmail.mozdev.org>

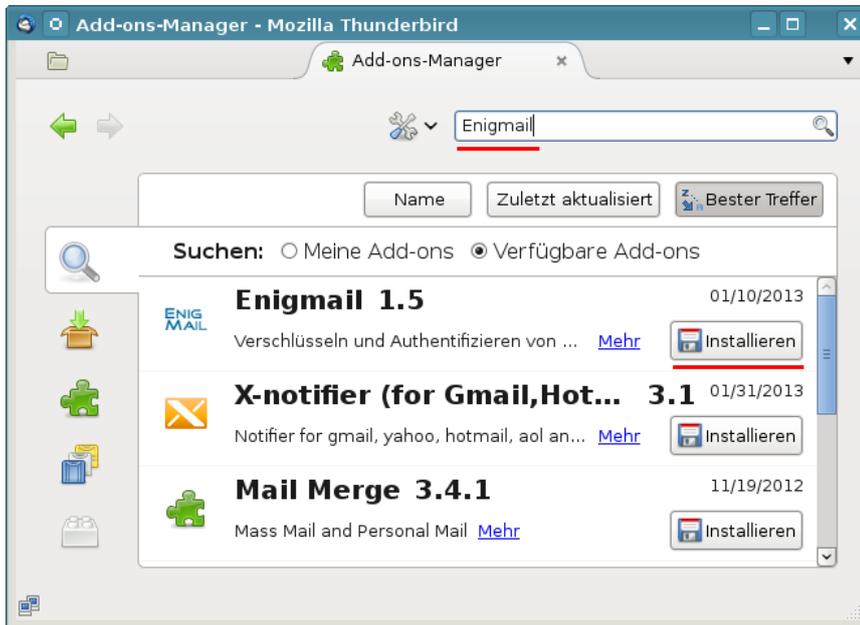


Abbildung 7.1: Installation von EnigMail

2. Abfrage, ob gesendete E-Mails standardmäßig verschlüsselt werden sollen. Da man meist nur OpenPGP-Schlüssel von wenigen Empfängern hat, kann man diese Option zunächst deaktivieren. Später, wenn sich die Verschlüsselung im Bekanntenkreis durchgesetzt hat, ist eine Aktivierung vielleicht sinnvoll.
3. Optimierung der Einstellungen für GnuPG. Die Vorgaben sind sinnvoll und sollten übernommen werden.
4. Generieren der Schlüsselpaare für alle vorhandenen Konten. Die Passphrase für den Zugriff auf den privaten Key sollte man sich vorher gut überlegen und merken! Es heißt *Passphrase* und nicht *Passwort*. Die Passphrase darf ruhig etwas länger sein und auch Leer- bzw. Sonderzeichen enthalten.

Die Vorschläge des Assistenten sind erst einmal sinnvoll. Individuelle Anpassungen (z.B. 4096 Bit Schlüssellänge usw.) kann man nur beim Erstellen eines neuen Schlüssels in der Schlüsselverwaltung wählen.

Kryptografischen Funktionen können nicht unbegrenzt den Fortschritten der Kryptoanalyse widerstehen. Es ist sinnvoll, die Nutzungszeit des Schlüssels mit einem Haltbarkeitsdatum zu versehen. Eine Nutzung länger als **5 Jahre** sollte man nur in begründeten Ausnahmen in Erwägung ziehen. Bei der Schlüsselerstellung sollte ein Verfallsdatum angegeben werden.

Mit jedem Schlüsselpaar kann auch ein Zertifikat für den Rückruf erstellt und sicher gespeichert werden. Mit diesem Zertifikat kann man einen Schlüssel für ungültig erklären, wenn der private Key kompromittiert wurde oder die Passphrase in Vergessenheit gerät.

Dieser 4. Schritt kann übersprungen werden, wenn man bereits gültige OpenPGP Schlüssel hat.

#### 5. FERTIG

Sollte Enigmail das Programm *gpg* nicht finden, weil man lieber die Version 2 *gpg2* von GnuPG nutzen möchte oder weil man es unter WINDOWS in einem selten verwendeten Verzeichnis liegt, wählt man den Menüpunkt *OpenPGP / Einstellungen* und gibt in der Dialogbox den Pfad zum GPG-Programm ein.

### 7.1.4 Schlüsselverwaltung

Die Schlüsselverwaltung findet man in Thunderbird unter dem Menüpunkt *Enigmail - Schlüssel verwalten*. Ist die Liste noch leer, wählt man zuerst den Menüpunkt *Erzeugen - Neues Schlüsselpaar*. Diesen Schritt übernimmt jedoch auch der Assistent zur Einrichtung von Enigmail.

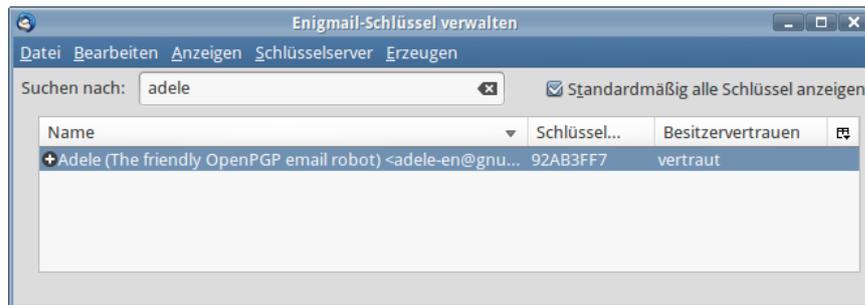


Abbildung 7.2: Schlüsselverwaltung von EnigMail

#### Exportieren des eigenen öffentlichen Schlüssels

Um verschlüsselt zu kommunizieren, muss den Kommunikationspartnern der eigene öffentliche Schlüssel zur Verfügung gestellt werden. Dafür gibt es mehrere Möglichkeiten:

- Man kann den eigenen öffentlichen Schlüssel als E-Mail Anhang versenden. Um den Schlüssel als Attachment an eine Mail anzuhängen, aktiviert man die Option *Meinen öffentlichen Schlüssel anhängen* beim Schreiben einer E-Mail in der Enigmail Toolbar.



- Man kann den eigenen öffentlichen Schlüssel auf einem Webserver ablegen. Den Menüpunkt für den Export in eine Datei findet man unter *Datei* -> *Schlüssel exportieren* in der Schlüsselverwaltung. Diese Textdatei kann man z.B. im eigenen Blog zum Download anbieten. Viele E-Mail Provider bieten auch einen kleinen Cloud Speicher für Daten. Man kann die Datei mit dem öffentlichen Key hochladen und für alle zum Download freigeben. In der E-Mail Signatur könnte man auf den Download hinweisen.
- Man zur Verteilung auch die Schlüsselservers im Internet nutzen. In der Schlüsselverwaltung findet man den Menüpunkt *Schlüssel-Server* -> *Schlüssel hochladen*. Der öffentliche Schlüssel wird auf den Schlüsselservers exportiert und steht dort allen Partnern zur Verfügung. Die verschiedenen Server synchronisieren ihren Datenbestand.

Hinweis: Beim Upload auf die Keyserver erfolgt keine Verifizierung der Identität! Jeder kann beliebige Schlüssel für beliebige E-Mail Adressen auf Keyservern veröffentlichen.

### Import der Schlüssel der Partner

Um an einen Kommunikationspartner verschlüsselte E-Mails zu senden oder die Signatur erhaltener Nachrichten zu prüfen, benötigt man den öffentlichen Schlüssel des Partners.

- Am einfachsten lässt sich dieser importieren, wenn man eine signierte E-Mail erhalten hat. Ein Klick auf den blauen Stift rechts oben im Header der E-Mail reicht aus, um den öffentlichen Schlüssel von einem Schlüsselservers zu importieren.
- Zum Importieren des Schlüssel eines Partners aus einer Datei, die man als Attachment oder per Download erhalten hat, wählt man den Menüpunkt *Datei / Importieren* in der Schlüsselverwaltung.
- Wenn der Schlüssel als Text angeboten wird, sieht es etwa so aus:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.1

mQENBEt5GIIBCACOnOeTtfBIUbdC0mw5D1LuxkQB4uQ/8HbSUaH96s1z
HqFA/31GB70podyEKqc41T2DdWWITfdy1dpXeGwopBK/wljPAuNagJQ
...
fU7xEW/RQT76n0RfTXnbj2m/DRPmoivcXW5G/zJM6QUj1++v070B+3xb
SnDCMQtaWHM57eLcmnsMAK3qHOY1VrNUTSvEgatjUqLU
=fP9T
-----END PGP PUBLIC KEY BLOCK-----
```

Man kann die Zeilen von BEGIN ...bis... END mit der Maus markieren und in die Zwischenablage kopieren. In der Schlüsselverwaltung von Enigmail importiert man den Schlüssel wie im Bild 7.3 dargestellt mit *Bearbeiten - Aus Zwischenablage importieren*.



Abbildung 7.3: OpenPGP-Schlüssel aus Zwischenablage importieren

- Man kann die OpenPGP Keyserver nach einem passenden Schlüssel durchsuchen (siehe unten). Dabei sollte man nach Möglichkeit den Fingerprint des Schlüssels als Suchkriterium wählen und nicht die E-Mail Adresse des Empfängers, da jeder einen falschen Schlüssel für eine E-Mail Adresse hochladen kann.

### 7.1.5 Signieren und Verschlüsseln erstellter E-Mails

Wurde in den Kontoeinstellungen in der Sektion *OpenPGP* die Option *Nachrichten standardmäßig verschlüsseln* aktiviert, sind beim Schreiben einer E-Mail keine weiteren Hinweise zu beachten. Anderenfalls muss man für jede E-Mail explizit festzulegen, dass sie verschlüsselt werden soll.

Das Fenster für das Erstellen einer neuen E-Mail zeigt nach der Installation von Enigmail eine neue Toolbar mit Buttons zum Verschlüsseln, Signieren und Anhängen des eigenen public Keys (Bild 7.4).

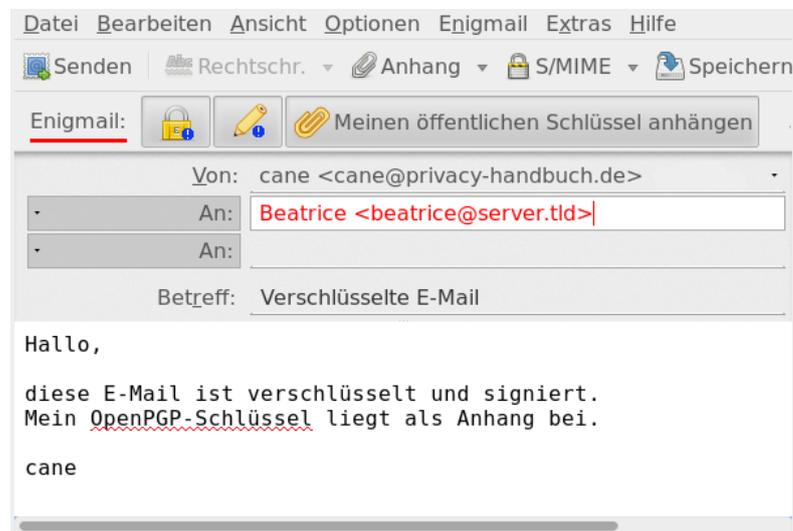


Abbildung 7.4: Signieren und Verschlüsseln einer E-Mail

Sollte die E-Mail Anhänge enthalten, ist die Option *PGP / MIME* zu aktivieren, um die Attachements standardkonform zu verschlüsseln.

**Achtung:** Die Betreffzeile wird nicht (!) mit verschlüsselt. Sicher wird man die Kontonummer nicht in der Betreffzeile schreiben, aber auch ein ausführlicher Betreff ermöglicht zusammen mit der/den Adressen der Empfänger einige Aussagen über die Kommunikation.

Wenn man als Betreff beispielsweise schreibt:

*Treffen der Aktivisten-Gruppe ... am 13.01.09*

und diese Mail per CC an alle Mitglieder der Gruppe versendet, sind 90% der relevanten Informationen bekannt und man kann sich die Verschlüsselung der Mail sparen.

Soll jede versendete E-Mail verschlüsselt werden, wenn der Schlüssel des Empfängers vorhanden ist, kann die entsprechende Option in den Einstellungen von Enigmail aktiviert werden (Bild 7.5). Alternativ ist es auch möglich, lediglich für bestimmte Empfänger festzulegen, dass alle E-Mails signiert oder verschlüsselt werden sollen. Diese Regeln kann man unter *Enigmail -> Empfängerregeln* definieren.

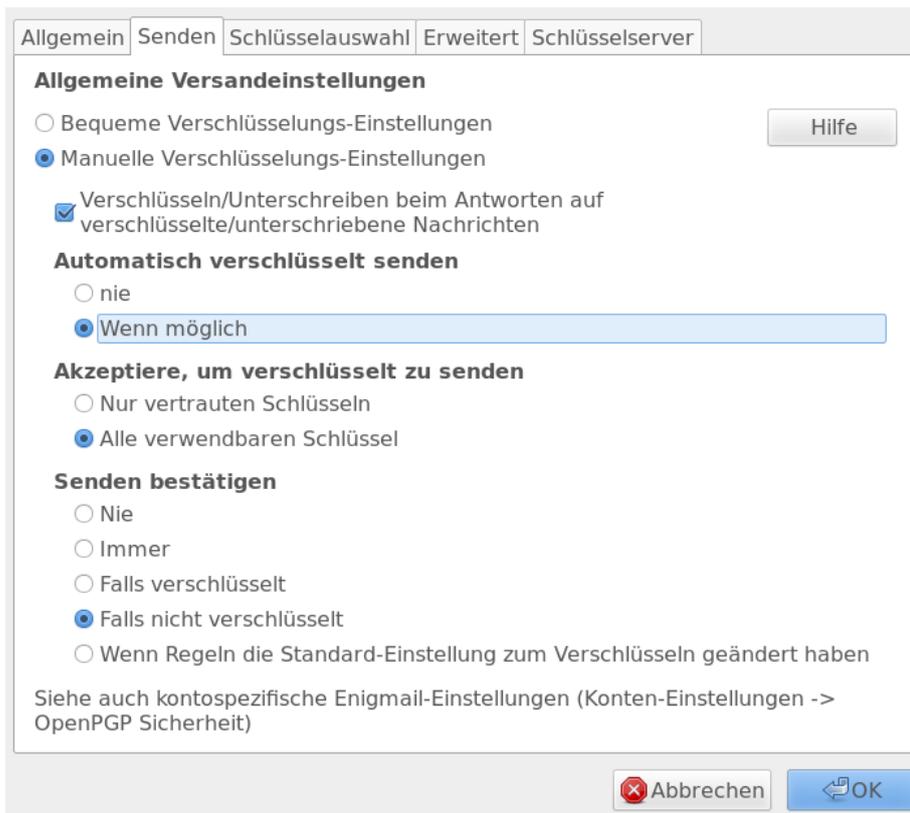


Abbildung 7.5: Signieren und Verschlüsseln aller E-Mails, wenn möglich

### 7.1.6 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 Anfängerprobleme 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
RouuaDQukNINWk2V2ErOWzFnJqdzpapeuPJiOWpOuIEvU3FRPhYlyt9dFfWAHv4
MJ7639tAx9PfXBmZ0d1PAoE451+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.

### 7.1.7 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 z.B. GPA (*GNU Privacy Assistant*)<sup>4</sup> oder KPGP 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. Entschlüsseln funktioniert umgekehrt.

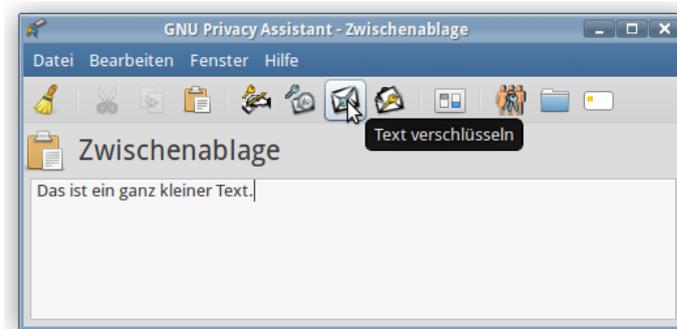


Abbildung 7.6: Text mit GPA verschlüsseln

Enthält das bevorzugte Tool für die Schlüsselverwaltung keinen Texteditor, kann man folgende Alternativen nutzen, die auch für unterwegs (auf dem USB-Stick) geeignet sind:

1. Das kleine Tool **gpg4usb**<sup>5</sup> bietet einen Editor mit den Buttons für das Ver- und Entschlüsseln des Textes, Dateiverschlüsselung sowie eine kleine Schlüsselverwaltung. Das ZIP-Archiv enthält Versionen für Windows und Linux. Es kann einfach auf dem USB-Stick genutzt werden.
2. **Portable PGP**<sup>6</sup> ist eine Java-Anwendung (plattformunabhängig), die

<sup>4</sup> [http://www.gnupg.org/related\\_software/gpa/index.de.html](http://www.gnupg.org/related_software/gpa/index.de.html)

<sup>5</sup> <http://www.gpg4usb.org/>

<sup>6</sup> <http://ppgp.sourceforge.net>

ebenfalls Texte und Dateien ver- und entschlüsseln kann. Eine einfache Schlüsselverwaltung ist ebenfalls enthalten. Zusätzlich zu Portable PGP benötigt man eine Java Laufzeitumgebung. Eine portable Version der Sun-JRE gibt es bei [portableapps.com](http://portableapps.com).

### Browser Add-ons

Browser Add-ons wie *Mailevelop* oder *Web PG* empfehle ich aus folgenden Gründen nicht:

1. Die Schlüssel werden im HTML5 Storage des Browsers gespeichert und sind damit leichter angreifbar als bei der Verwaltung durch ein lokal installiertes GnuPG Tool.
2. Javascript ist für starke Kryptografie nur bedingt geeignet. Es gibt z.B. keine Möglichkeit, Speicherbereiche im PAM (Hauptspeicher) gezielt zu überschreiben. Entsperrte Keys bleiben nach der Verwendung im RAM erhalten, wo sie durch eine Schadsoftware ausgelesen werden könnten. Bei Tor war dieses Verhalten ein schwerer Bug, aber bei der Verschlüsselung von Mails wird dieses Verhalten einfach pauschal akzeptiert?

### 7.1.8 GnuPG SmartCard nutzen

Die Sicherheit asymmetrischer Verschlüsselung hängt in hohem Maße von der sicheren Aufbewahrung des privaten Keys ab. Nutzt man GnuPG auf mehreren Rechnern, insbesondere wenn andere Nutzer Administrator- bzw. Root-Privilegien auf diesen Rechnern haben, könnte der private Key in falsche Hände gelangen.

Böswillige Buben könnten mit einem Trojaner versuchen, den privaten Key zu kopieren und das Passwort mit Tools wie *Elcomsoft Distributed Password Recovery* <sup>7</sup> ermitteln. Die unbedachte Entsorgung einer Festplatte oder eines Computers ist ein weiteres Risiko, wenn der private Key nicht zuverlässig gelöscht wurde.

**SmartCards:** ermöglichen eine sichere Nutzung von GnuPG unter diesen Bedingungen. Der private Key ist ausschließlich auf der SmartCard gespeichert, er verläßt diese sichere Umgebung nicht. Sämtliche kryptografischen Operationen werden auf der Card ausgeführt. CardReader (USB) und GnuPG-SmartCards gibt es bei [kernelconcepts.de](http://kernelconcepts.de) <sup>8</sup>.

**Yubikey NEO:** Der Yubikey ist ein One-Time-Passwordgenerator (OTP), den man für sichere Logins bei verschiedenen Webdiensten nutzen kann. Die etwas teurere Variante Yubikey NEO enthält zusätzlich eine OpenPGP Smartcard. Diese Funktion ist standardmäßig deaktiviert und muss erst mit dem Tool *ykpersonalize* freigeschaltet werden:

```
> ykpersonalize -m82
```

<sup>7</sup> <http://www.elcomsoft.de/programme/edpr.html>

<sup>8</sup> <http://www.kernelconcepts.de/shop/products/security.shtml?hardware>

Den Yubikey NEO kann man bei Yubico im Webshop kaufen oder als Kunde beim E-Mail Provider Mailbox.org ordern, wo man ihn auch für den Login nutzen kann.

**NitroKey:** Der NitroKey<sup>9</sup> ist der Nachfolger des Open Source Projektes Cryptostick. Der NitroKey Pro enthält zusätzlich einen OTP Generator. Für die Nutzung dieser Zusatzfunktion ist die NitroKey App<sup>10</sup> zu installieren.

### Hardware-Treiber installieren

Für den Yubikey NEO benötigt man zusätzlich das YubiKey Cross Platform Personalization Tool *ykpersonalize*, das man von der Webseite herunter laden kann.<sup>11</sup>

Nachdem die Software installiert wurde, sollte man prüfen, ob alles funktioniert. SmartCard anschließen und auf der Konsole bzw. DOS-Box eingeben:

```
> gpg --card-status
Application ID ...: D27600xxxxxxxxxxxxxxxxxx
Version .....: 2.0
Manufacturer .....: unknown
....
```

### SmartCards mit Enigmail nutzen

Enigmail ist voll kompatibel mit SmartCards. Das Add-on bietet eine grafische Oberfläche, um SmartCards zu verwalten. Diese Funktionen öffnet man über den Menüpunkt *Enigmail - Smartcard verwalten*.

1. Als Erstes kann man die Card personalisieren und den Namen usw. editieren, eine Download URL für den Public Key angeben... (*Edit Card Data*).
2. Im zweiten Schritt sollte der PIN und der Admin-PIN geändert werden. Der PIN ist eine 6-stellige Zahlenkombination (Default: 123456), welche den User-Zugriff auf die Card sichert. Der Admin-PIN ist eine 8-stellige Zahlenkombination (Default: 12345678) für die Verwaltungsoperationen.

Wurde der PIN 3x falsch eingegeben, wird die Card gesperrt und kann mit dem Admin-PIN wieder entsperrt werden (*Unblock PIN*). Wird der Admin-PIN 3x falsch eingegeben, ist die SmartCard zerstört!.

Die Festlegung auf 6- bzw. 8-stellige Zahlenkombinationen legt es nahe, ein Datum aus dem persönlichen Leben als PINs zu nutzen. Das reduziert die Vergesslichkeit. Es sollte jedoch kein einfach zu erratenes Datum wie der Geburtstag des Töchterchens sein.

<sup>9</sup><https://www.nitrokey.com/de>

<sup>10</sup><https://www.nitrokey.com/de/download>

<sup>11</sup><http://www.yubico.com/products/services-software/personalization-tools/use/>

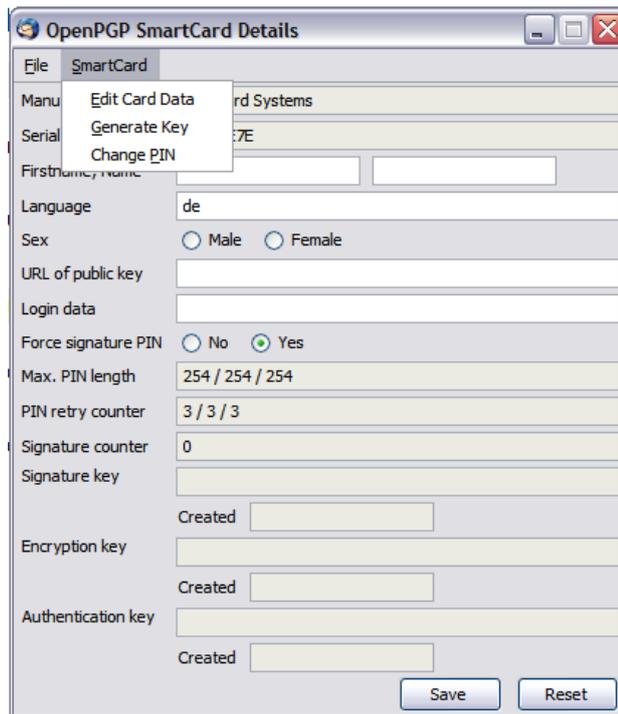


Abbildung 7.7: SmartCard verwalten

3. Als letzten Schritt vor der Nutzung der SmartCard im täglichen Krypto-Chaos sind die Keys auf der SmartCard zu generieren. Der entsprechende Dialog bietet die Auswahl eines Mail-Account an, für den die SmartCard genutzt werden soll. Für diesen Account darf kein(!) OpenPGP-Key vorhanden sein. Anderenfalls bricht der Vorgang mit einer wenig verständlichen Fehlermeldung ab.

Es sollte unbedingt bei der Erzeugung des Schlüssels ein Backup der Card-Keys angelegt und mit einem Passwort gesichert werden. Später ist kein Zugriff auf diese Schlüssel mehr möglich. Bei Beschädigung der SmartCard kann der gesicherte Card-Key in eine neue SmartCard importiert werden. Das Backup wird im GnuPG-Verzeichnis abgelegt und ist auf einem sicheren Datenträger zu speichern!

Wurden die Schlüssel erfolgreich generiert, findet man in der *Schlüsselverwaltung* ein neues Paar. Der Public Key dieses Schlüsselpaares kann wie üblich exportiert und den Partnern zur Verfügung gestellt werden. Der Private Key dieses Paares definiert lediglich, dass die kryptografischen Operationen auf einer SmartCard auszuführen sind. Er ist ohne die passende Card unbrauchbar.



Abbildung 7.8: SmartCard-PINs ändern

### Funktionen für Genießer

Die Nutzung von gpg auf der Kommandozeile bietet etwas mehr Möglichkeiten, als bisher im Enigmail-GUI implementiert sind. Natürlich stehen auch die mit dem GUI durchführbaren Funktionen auf der Kommandozeile zur Verfügung.

Einen Überblick über alle SmartCard-Funktionen gibt die Hilfe. Als erstes muss man den Admin Mode aktivieren, dann hat man vollen Zugriff auf alle Funktionen:

```
> gpg --card-edit
Befehl> admin
Befehl> help
```

Neue Schlüssel generiert man auf der SmartCard mit:

```
> gpg --card-edit
Befehl> admin
Befehl> generate
```

Hat man mehrmals den PIN falsch eingegeben kann man ein neuen (alten) PIN (rück-)setzen, wenn man den Admin-PIN kennt:

```
> gpg --card-edit
Befehl> admin
Befehl> passwd
```

Möglicherweise hat man bereits eine OpenPGP Schlüssel mit vielen Signaturen. Den möchte man nicht wegwerfen und im Web of Trust noch einmal von vorn beginnen. Als Ausweg bietet es sich an, einen vorhandenen, starken Schlüssel mit der SmartCard zusätzlich zu schützen. Der Zugriff auf den geheimen Schlüssel ist dann nur mit der SmartCard möglich. Es ist dem vorhandenen Schlüssel mit der ID key-id ein Subkey der SmartCard hinzuzufügen. Das geht nur auf der Kommandozeile:

```
> gpg --edit-key key-id
command> addcardkey
```

Dabei wird ein evtl. auf der SmartCard vorhandener Key zertört!

### 7.1.9 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. Die Funktion findet man in der Schlüsselverwaltung von Enigmail unter dem Menüpunkt *Schlüssel-Server* -> *Schlüssel suchen*.

#### Vorsicht bei der Nutzung von Keyservern

Man kann auf den Keyservern nach Schlüsseln anhand E-Mail Adressen (1), 8-stellige oder 16-stellige Key IDs oder dem bekannten Fingerprint (4) 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 die Verschlüsselung zu stören?). 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 von 2015!), wie Fefe in seinem Blog schreibt.<sup>12</sup>



Abbildung 7.9: Fünf OpenPGP-Schlüssel für eine E-Mail Adresse

Auch J. Schmidt von Heise.de beklagt, dass ein Scherzkeks OpenPGP Schlüssel für seine E-Mail Adresse auf die Keyserver hochgeladen hat und dass er die damit verschlüsselten E-Mails nicht lesen kann (Editorial c't 6/2015).

Wenn Fakes für die Signaturschlüssel von Krypto-Software in Umlauf gebracht werden, dann steckt vielleicht etwas mehr als nur ein *Scherzkeks* dahinter, der sich einen Spaß erlauben wollte?

- Erinn Clark signiert die Downloads des TorBrowserBundle. Für ihre E-Mail Adresse wurden Fake Schlüssel auf den Keyserver publiziert.<sup>13</sup>

<sup>12</sup> <https://blog.fefe.de/?ts=aa27d652>

<sup>13</sup> <https://lists.torproject.org/pipermail/tor-talk/2014-March/032308.html>

- Gavin Andresen signiert die Bitcoin Binaries, für seine E-Mail Adresse wurden ebenfalls Fake Schlüssel auf den Keyserver publiziert.<sup>14</sup>

Die kryptografische Sicherheit von OpenPGP wird durch diese Fakes nicht beeinträchtigt. Sie sind vor allem Sand im Getriebe und erzeugen Frust bei den Nutzern.

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.<sup>15</sup>
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.

### SSL-Verschlüsselung für Keyserver aktivieren

Seit Anfang Oktober 2012 bietet der Keyserverpool `sks-keyservers.net` einen Sub-Pool mit SSL-Verschlüsselung für das Abrufen und Senden von OpenPGP-Schlüsseln<sup>16</sup>. Die SSL-Verschlüsselung verhindert, dass ein Lauscher beobachtet, welche OpenPGP-Schlüssel man sucht und herunter lädt.

Um diesen sicheren Sub-Pool zu nutzen, sind folgende Schritte nötig:

1. Man benötigt eine Version von GnuPG, die das `hkps://` Protokoll unterstützt. Man kann `gnupg2` nutzen oder das Paket `gnupg-curl` installieren. Für Windows bietet `pgp4win` ein Paket mit `gnupg2`, unter Linux installiert man eines der genannten Pakete mit dem bevorzugten Paketmanager.
2. Das CA-Root Zertifikat des Keyserverpool `sks-keyservers.netCA.pem`<sup>17</sup> ist herunter zu laden und auf dem eigenen Rechner zu speichern.
3. In der Konfiguration von Enigmail sind die *Experten Optionen* zu aktivieren und folgende Werte einzutragen:
  - (a) Bei der Nutzung von `gnupg2` ist der Pfad zu diesem Programm auszuwählen.
  - (b) Auf dem Reiter *Schlüssel-Server* ist der HKPS-Pool als einziger Schlüssel-Server einzutragen:

```
hkps://hkps.pool.sks-keyservers.net
```

<sup>14</sup> <http://gavintech.blogspot.ch/2014/03/it-aint-me-ive-got-pgp-imposter.html>

<sup>15</sup> <http://heise.de/-2473281>

<sup>16</sup> <http://permalink.gmane.org/gmane.comp.encryption.pgp.sks/3559>

<sup>17</sup> <https://sks-keyservers.net/sks-keyservers.netCA.pem>

- (c) Auf dem Reiter *Erweitert* muss man als *Zusätzliche Parameter für GnuPG* die Keyserver-Option für das *ca-cert-file* ergänzen:

```
--keyserver-options ca-cert-file=<Path to>/sks-keyservers.netCA.pem
```

4. Wenn man die SSL-verschlüsselten Keyserver auch mit den Kommandozeiletool *gnupg2* nutzen möchte, kann man in der Konfigurationsdatei *gpg.conf* folgende Parameter setzen:

```
keyserver hkps://hkps.pool.sks-keyservers.net
keyserver-options ca-cert-file=<Path to>/sks-keyservers.netCA.pem,...
```

5. Wenn man GnuPG 2.1 nutzt, dann muss man in der Konfigurationsdatei *\$HOME/.gnupg/dirmngr.conf* folgende Zeile hinzufügen:

```
hkp-cacert <Path to>/sks-keyservers.netCA.pem
```

### 7.1.10 OpenPGP-Verschlüsselung für Kontaktformulare

Das 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-Scripte oder fertige Perl-CGI Scripte. Man kann eine individuell passende Lösung wählen. Dabei sollte man auf folgendes achten:

1. Das Kontaktformular sollte den Absender nicht zur Eingabe seiner E-Mail Adresse zwingen. Als work-around kann man im HTML-Code des Formulars das Feld für die Absender E-Mail Adresse als *hidden* deklarieren und einen Standardwert setzen.
2. Das Script sollte die IP-Adresse des Absenders nicht in den Header der E-Mail einfügen. Einige Scripte für Kontaktformulare wollen damit den Spam-Schutz verbessern. Einfach ausprobieren.
3. Das Kontaktformular sollte immer via HTTPS (SSL-verschlüsselt) aufgerufen werden. Wenn die Webseite auch via plain HTTP erreichbar ist, sollten alle Links auf der Webseite zum Kontaktformular mit der vollständigen URL angegeben werden:

```
<a href="https://www.server.tld/kontakt.html">Kontakt</a>
```

Jeder gute Webhoster bietet inzwischen SSL-Verschlüsselung für einen kleinen Aufpreis für alle Kunden, Wordpress.com hat es standardmäßig für alle Kunden 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.

### 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. Ich kenne bisher nur Mailbox.org als einzigen E-Mail Provider, bei dem man beide Features aktivieren kann.

- 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 OpenPGP 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.

1. Die aktuelle Version der Bibliothek *openpgp.min.js* von der Projektwebseite <https://github.com/openpgpjs/openpgpjs/releases> herunterladen und auf den eigenen Webserver kopieren.
2. Das Javascript Schnipselchen *encrypt\_message.js* von meiner Webseite [https://www.privacy-handbuch.de/handbuch\\_32v.htm](https://www.privacy-handbuch.de/handbuch_32v.htm) herunterladen und auf den Webserver kopieren. Dieses Javascript Schnipselchen verschlüsselt das Textarea Feld mit der ID `textitmessage`. Wenn das Textarea im Formular eine andere ID hat, ist die Zeilen 3 anzupassen:

```
var message = document.getElementById("message");
```

3. Im HTML-Header der Webseite des Formulars sind die Scripte zu laden:

```
...
<script src="/openpgp.min.js" type="text/javascript">
<script src="/encrypt_message.js" type="text/javascript">
...
```

4. Im HTML-Code des Formulars im FORM-Tag die Funktion *encrypt\_message()* als *onsubmit*-Tag hinzufügen, so dass die Funktion automatisch beim Versand der Daten ausgeführt wird:

```
<FORM name="contact" method="post" action="https://server.tld/..."
  onsubmit="return encrypt_message();">
```

5. Außerdem ist der eigenen OpenPGP public Key als versteckter DIV-Container mit der ID *pubkey* 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.

### 7.1.11 Web des Vertrauens

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 Anton überprüft, kann sie diesen mit ihrem geheimen Schlüssel signieren und auf die Schlüsselservers re-exportieren. Conrad, der den Schlüssel von Beatrice bereits überprüft hat, kann damit aufgrund der Signatur auch dem Schlüssel von Anton vertrauen. Es bildet sich ein weltweites Netz von Vertrauensbeziehungen. Die Grafik Bild 7.10 zeigt eine mögliche Variante für den Key von Anton (A).

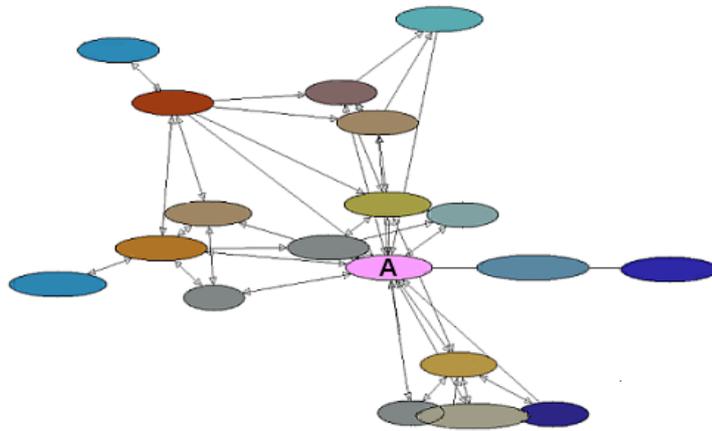


Abbildung 7.10: Beispiel für ein Web of Trust

### OpenPGP-Schlüssel signieren

Die Echtheit eines Schlüssels kann anhand des Fingerabdrucks geprüft werden. Zu jedem Schlüssel existiert ein eindeutiger Fingerabdruck. Dieser lässt sich in den Eigenschaften des Schlüssels anzeigen. In der Schlüsselverwaltung ist der zu prüfende Schlüssel auszuwählen und über den Menüpunkt *Anzeigen - Eigenschaften* den im Bild 7.11 dargestellten Dialog zu öffnen.

Der angezeigte Fingerabdruck des Schlüssels kann mit dem Wert verglichen werden, den man vom Eigentümer des Schlüssels erhalten hat. Sind beide identisch, kann das Vertrauen des öffentlichen Schlüssels auf ein hohes Niveau gesetzt werden. Den Dialog findet man in der Schlüsselverwaltung unter *Bearbeiten - Vertrauenswürdigkeit*.

Hat man sich von der Echtheit des Schlüssels überzeugt, kann man ihn in Absprache mit dem Schlüsseleigentümer auch signieren und den signierten Schlüssel auf einen Keyserver exportieren. Wenn viele Nutzer die Ergebnisse ihrer Überprüfung online verfügbar machen, entsteht das Web-of-Trust und es wird schwer, gefälschte Schlüssel in Umlauf zu bringen.

### 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.

Beispiele für Certification Authorities sind:

- CAcert.org signiert auch OpenPGP-Schlüssel

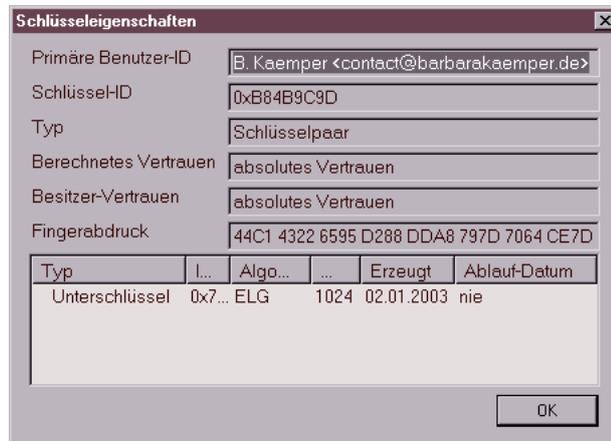


Abbildung 7.11: Schlüssel-Eigenschaften

- Krypto-Kampagne der Zeitschrift c't
- PCA des Deutschen Forschungsnetzes (DFN-PCA)

### Keysigning-Party

Wenn sich mehrere OpenPGP-Nutzer treffen um sich gegenseitig die Echtheit ihrer Schlüssel zu bestätigen, nennt man es eine *Keysigning-Party*. Dabei kommt es nicht darauf an, dass die Beteiligten sich persönlich kennen. Die Echtheit des Schlüssels können auch Unbekannte gegen Vorlage von Ausweisdokumenten und Fingerprint des Key bestätigen.

Eine Keysigning-Party läuft üblicherweise folgendermaßen ab:

1. Der Organisator lädt zu einer Party ein und bittet um Anmeldungen.
2. Wer an der Party teilnehmen möchte, sendet seinen public OpenPGP-Key zusammen mit Namen und dem Fingerprint an den Organisator.
3. In Vorbereitung der Party erstellt der Organisator einen Keyring für alle Beteiligte und eine Liste mit Namen, Key-IDs und Fingerprints von allen Teilnehmern.
4. Der Keyring und die Liste werden an alle Teilnehmer verteilt. Die Teilnehmer können auf der Party die Identität gegenseitig durch Vorlage von Ausweisdokumenten prüfen.
5. Wieder zuhause können die Schlüssel im Party-Keyring signiert und an die Inhaber per E-Mail versendet werden. In der Regel erfolgt dieser Schritt nicht beim Treffen.

Wer häufiger an Keysigning-Partys teilnimmt, kann unter Linux das Tool *caff* für den letzten Schritt nutzen. Das Tool ist im Paket *signing-party* für nahezu alle Linux-Distributionen verfügbar und kann mit dem Paket-Manager

der Wahl installiert werden.

Nach der Installation ist die Datei `$HOME/.caffrc` als Textdatei anzulegen und die Werte für den eigenen Namen, E-Mail Adresse, OpenPGP-ID sowie die Parameter zur Versendung von E-Mails sind zu konfigurieren:

```
$CONFIG{'owner'} = 'Michi Müller';  
$CONFIG{'email'} = 'm@m.de';  
$CONFIG{'keyid'} = [ qw{01234567890ABCDE} ];  
  
$CONFIG{'mailer-send'} = [ 'smtp', Server => 'mail.server', Auth => ['user','pass'] ];
```

Ein kleines Kommando im Terminal signiert alle Schlüssel des Party-Keyring, verpackt sie in E-Mails, die mit dem Key der Empfänger verschlüsselt werden, und sendet die E-Mails an die Inhaber der OpenPGP-Keys:

```
> caff --key-file party-keyring.asc
```

### 7.1.12 Schlüssel zurückrufen

Soll ein Schlüsselpaar nicht mehr verwendet werden (beispielsweise weil der geheime Schlüssel kompromittiert wurde oder die Passphrase in Vergessenheit gefallen ist), kann der öffentliche Schlüssel für ungültig erklärt werden.

Öffnen Sie die Schlüsselverwaltung, wählen Sie den Schlüssel, der für ungültig erklärt werden soll. Rufen Sie den Menüpunkt *Bearbeiten / zurückrufen* auf. Nach einer Sicherheitsfrage und Eingabe der Passphrase wird der Schlüssel auf den Schlüsselservers im Internet für ungültig erklärt. Auch wenn der geheime Schlüssel nicht mehr vorliegt oder die Passphrase in Vergessenheit geraten ist, kann der öffentliche Schlüssel für ungültig erklärt werden, indem das unter Punkt 4 erstellte Rückrufzertifikat importiert wird.

## 7.2 S/MIME mit Thunderbird

S/MIME nutzt Zertifikate nach dem Standard X.509 für die Verschlüsselung und Signatur von E-Mails. Eine *Certification Authority* (CA) bestätigt mit einer Signatur die Echtheit und die Identität des Besitzers eines ausgegebenen Zertifikates. Für diese Signatur wird das *Root Certificate* der CA genutzt. Die Root Certificates etablierter CAs sind in nahezu allen Browsern und E-Mail Clients enthalten. Wer diesen Zertifikaten vertraut, vertraut auch ohne weitere Nachfrage den damit signierten persönlichen Zertifikaten anderer Nutzer.

### 7.2.1 Kostenfreie Certification Authorities

In der Regel kostet dieser Service bei einer etablierten CA 30-100 Euro pro Jahr. [CAcert.org](http://CAcert.org) bietet eine kostenfreie Alternative für die Ausstellung und Signatur von X.509 Zertifikaten. CAcert.org ist ein *Web of Trust* von Nutzern, welche sich gegenseitig bei einem persönlichen Treffen die Identität bestätigen. Einfache Nutzer werden durch Assurer verifiziert, die ehrenamtlich für CAcert.org arbeiten.

Für jede Bestätigung durch einen Assurer erhält der Nutzer bis zu 35 Punkte. Sobald man 50 Punkte angesammelt hat, also nach mindestens 2 unabhängigen Bestätigungen, kann man sich auf der Website ein Class-3 Zertifikat mit dem eigenen Namen generieren. Mit einem Punktestand von 100 Punkten kann man den Status eines Assurers beantragen.

Auch ohne Bestätigungen durch Assurer kann man ein Zertifikat zu erzeugen. Dieses Class-1 Zertifikat enthält nur die E-Mail Adresse des Besitzers und keinen verifizierten Namen.

Der Weg zur Erstellung eines S/MIME-Zertifikates:

- Wer häufig CAcert.org nutzt, sollte das Root-Zertifikat dieser CA in den Browser importieren. Man erspart sich damit lästige Nachfragen beim Besuch der Website. Die Root Zertifikate von CAcert.org ist standardmäßig nicht in den häufig genutzten Browsern enthalten. CAcert.org bietet sie auf der Webseite zum Download.
- Es ist notwendig, die Root-Zertifikate von CAcert.org in den E-Mail Client als vertrauenswürdige CA zu importieren. Nur so kann die Gültigkeit des eigenen Zertifikates überprüft werden.
- Die Anmeldung folgt dem üblichen Schema. Nach Eingabe der Kontaktdaten erhält man eine E-Mail zu Verifizierung und kann sich im Anschluss auf der Website einloggen, um die persönlichen Angaben zu vervollständigen.
- Zur Bestätigung der Identität kann man auf der Website einen Assurer in der Nähe suchen und um ein persönliches Treffen bitten. Zum Treffen ist ein Ausdruck des WOT-Formulars für den Assurer mitzubringen.

- Hat man 50 Punkte durch Bestätigungen von mehreren Assurer erreicht, kann man auf der Webseite ein Zertifikat erstellen. Das Zertifikat und den Privaten Key findet man nach dem Vorgang in der Zertifikatsverwaltung des Browsers unter *Eigene Zertifikate!* Es gibt keinen Downloadlink o.ä.
- Das Zertifikat wird aus der Zertifikatsverwaltung des Browsers als \*.P12 Datei exportiert und im E-Mail Client wieder importiert.

### 7.2.2 Erzeugen eines Zertifikates

Die verschiedenen Certification Authorities (CAs) bieten ein Webinterface, um nach der Überprüfung der Identität ein signiertes Zertifikat zu erstellen. In der Regel stehen zwei Wege zur Auswahl:

1. Der Anbieter (CA) führt den kompletten Vorgang aus: die Generierung des privaten Key inklusive Sicherung mit einer Passphrase, die Generierung des Certification Request (CSR), die Signierung des CSR und die Erstellung der Zertifikatsdatei mit privatem und öffentlichem Schlüssel.

CAcert.org hat eine Lösung entwickelt, den privaten Key im Browser des Nutzers zu generieren und nur den CSR (public Key) zur Signatur auf den eigenen Server zu laden. Viele CAs generieren aber beide Schlüssel auf dem eigene Server und haben damit Zugriff auf den Private Key.

2. Der Anwender generiert den privaten Key und den CSR selbst, lädt nur den CSR auf den Server des Anbieters, der CSR wird dort signiert und als Zertifikat wieder zum Download bereitgestellt.

Da die Sicherheit asymmetrischer Verschlüsselung davon abhängt, dass nur der Anwender Zugriff auf den privaten Schlüssel hat, sollte man sich die Mühe machen und den zweiten Weg gehen. Anderenfalls ist es möglich, dass der private Schlüssel bereits vor der ersten Verwendung kompromittiert wird. Man sollte den Certification Authorities nicht blind vertrauen.

Die OpenSSL-Bibliothek bietet alles Nötige. Die Tools sind unter Linux installiert. Ein grafisches Interface ist *TinyCA*. Download: <http://tinyca.sm-zone.net>

#### Schrittweise Anleitung für die Kommandozeile

1. Generieren eines passwortgeschützten privaten Schlüssels in der Datei *mein.key*:

```
> openssl genrsa -out mein.key -des3 2048
```

2. Generieren eines Certification Request (CSR) in der Datei *mein.csr*, die folgenden Daten werden dabei abgefragt:

```
> openssl req -new -key mein.key -out mein.csr
Enter pass phrase for mein.key:
....
```

```
Country Name (2 letter code) [AU]: DE
State or Province Name (full name) []: Berlin
Locality Name (eg, city) []: Berlin
Organization Name (eg, company) []: privat
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []: Max Musterman
Email Address []: max@musterman.de
```

3. en CSR übergibt man der CA. Die Datei enthält nur den öffentlichen Schlüssel. Die CA signiert diesen CSR und man erhält ein signiertes Zertifikat als Datei *mein.crt* via E-Mail oder als Download Link.
4. Diese Datei kann man an alle Kommunikationspartner verteilen.
5. Für den Import im eigenen E-Mail Client fügt man privaten Schlüssel und signiertes Zertifikat zu einer PKCS12-Datei *mein.p12* zusammen.

```
> openssl pkcs12 -export -in mein.crt -inkey mein.key -out mein.p12
```

Diese passwortgeschützte Datei kann in allen E-Mail Clients importiert werden und sollte sicher verwahrt werden.

### 7.2.3 S/MIME-Krypto-Funktionen aktivieren

Liegt eine Datei mit signiertem Zertifikat und geheimem Schlüssel vor, können die S/MIME-Funktionen für ein E-Mail Konto aktiviert werden. Es ist der Dialog mit den Konto-Einstellungen zu öffnen und in die Sektion *S/MIME-Sicherheit* zu wechseln (Bild 7.12).

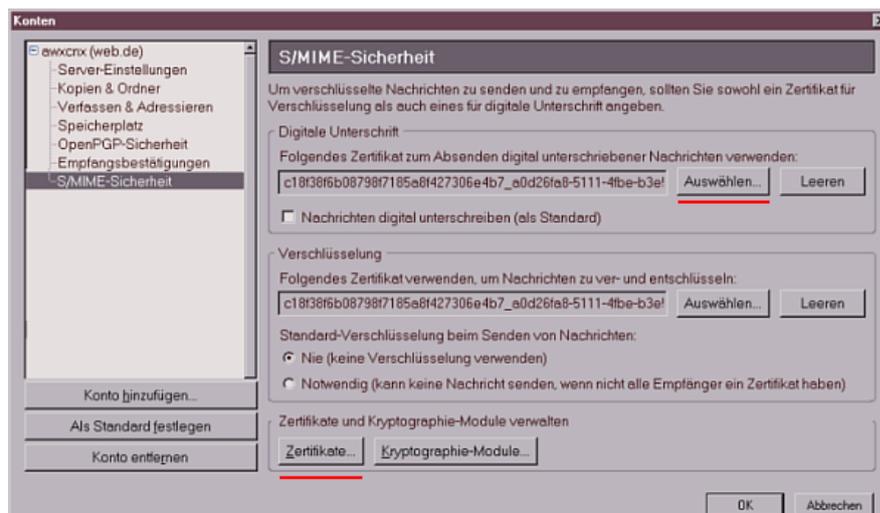


Abbildung 7.12: Kontoeinstellungen zur S/MIME-Sicherheit

Zuerst ist das persönliche Zertifikat zu importieren. Ein Klick auf den Button *Zertifikate* öffnet den Manager für eigene Zertifikate (Bild 7.13). Hier ist der Button *Importieren* zu wählen und das gespeicherte persönliche Zertifikat mit öffentlichem und geheimem Schlüssel zu importieren.

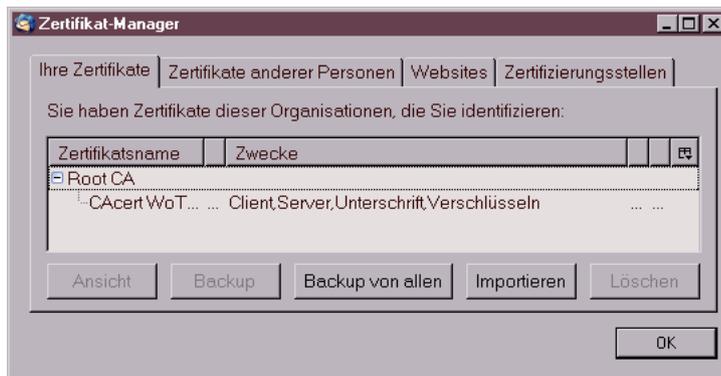


Abbildung 7.13: Zertifikatsmanager für eigene Zertifikate

Es folgt eine Abfrage des Passwortes, mit dem der Zugriff auf den geheimen Schlüssel geschützt werden soll und evtl. die Frage nach dem Passwort, mit welchem die Datei verschlüsselt wurde. Der Zertifikatsmanager ist im Anschluss mit einem Klick auf den Button *Ok* zu schließen und in den Konto-Einstellungen das frisch importierte Zertifikat für das Signieren und Entschlüsseln auszuwählen.

Sollen alle ausgehenden Nachrichten standardmäßig signiert werden, kann die entsprechende Option aktiviert werden.

Thunderbird bietet die Möglichkeit, das Online Certificate Status Protocol (OCSP) für die Validierung von Zertifikaten zu nutzen. Standardmäßig ist die Nutzung dieser Funktion sinnvoll deaktiviert. Da nur validierte Zertifikate für die Verschlüsselung und Signaturprüfung genutzt werden können, muss man das Root Zertifikat der ausstellenden CA von der Website herunterladen und importieren. Dies kann vereinfacht werden, wenn man im Dialog *Einstellungen* in der Sektion *Datenschutz* auf dem Reiter *Sicherheit* den Button *OCSP...* wählt und die Option *OCSP verwenden* aktiviert. Damit hat man jedoch keine Möglichkeit zu entscheiden, ob man der CA wirklich vertraut.

#### 7.2.4 Zertifikate der Partner und der CA importieren

Im Gegensatz zu OpenPGP, das im Internet eine ausgereifte Infrastruktur zur Verteilung öffentlicher Schlüssel bereitstellt, muss der Inhaber eines S/MIME-Zertifikates selbst die Verteilung übernehmen. Am einfachsten ist es, dem Partner eine signierte E-Mail zu senden. Alle E-Mail Clients mit S/MIME Support können aus der Signatur das Zertifikat importieren und tun dies in der Regel ohne Nachfrage.

Bevor der Empfänger einer signierten E-Mail die Signatur prüfen und verschlüsselt antworten kann, muss er das Zertifikat verifizieren. Viele Root-Zertifikate sind bereits in gängigen E-Mail Clients enthalten. Einige muss der Nutzer jedoch erst selbst importieren. Diese Root-Zertifikate stehen auf den Websites der Ausstellers zum Download bereit. Wurde die Gültigkeit verifiziert, kann der Empfänger im Anschluß verschlüsselt antworten.

Es ist auch möglich, eine Datei nur mit dem öffentlichen Schlüssel des Zertifikates auf den Rechner des Partners zu transferieren. Dort ist die Datei in Thunderbird zu importieren.

Für den Import eines Zertifikates in Thunderbird ist der Dialog *Einstellungen* zu öffnen. In der Sektion *Datenschutz* auf dem Reiter *Sicherheit* ist der Button *Zertifikate* zu wählen (Bild 7.14), um die Verwaltung zu öffnen.



Abbildung 7.14: Dialog Sicherheits-Einstellungen

Im Zertifikatsmanager ist auf dem Reiter *Zertifikate anderer Personen* der Button *Importieren* zu finden, welcher eine Dateiauswahl öffnet, um das erhaltene Zertifikat aus einer lokal gespeicherten Datei zu importieren.

Die Root-Zertifikate weiterer Certification Authorities (CAs) können auf dem Reiter *Zertifizierungsstellen* importiert werden.

### 7.2.5 Nachrichten verschlüsseln und signieren

Wenn das persönliche Zertifikat bestehend aus öffentlichem und geheimem Schlüssel importiert wurde, ist es möglich, signierte E-Mails zu versenden. Wurden Zertifikate mit den öffentlichen Schlüsseln der Kommunikationspartner importiert, kann die Nachricht auch verschlüsselt werden.

Für die Wahl der Optionen steht im Editor einer neuen Nachricht der Button *S/MIME* zur Verfügung. Klickt man auf den kleinen schwarzen Pfeil unmittelbar neben dem Button *S/MIME*, öffnet sich das im Bild 7.15 dargestellte Menü zum Festlegen der Kryptographie-Optionen für die aktuelle

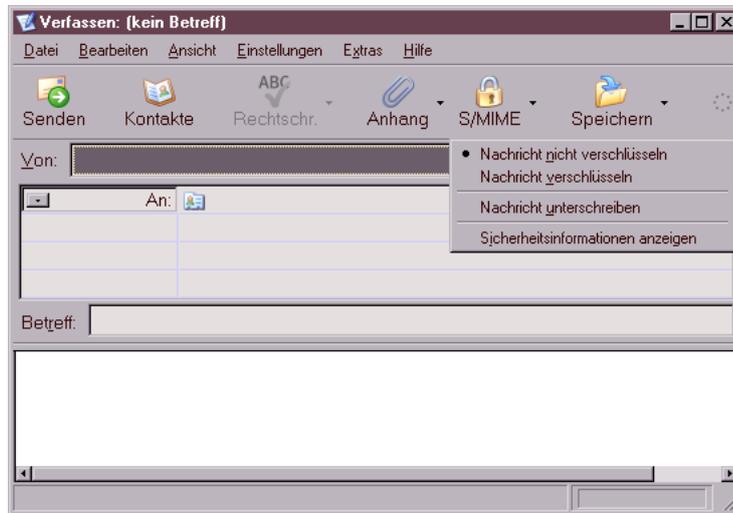


Abbildung 7.15: Verschlüsseln oder Signieren einer E-Mail

Nachricht.

Eine Möglichkeit, für bestimmte Empfänger die Einstellungen für Verschlüsselung dauerhaft festzulegen, bietet Thunderbird in der Standard-Konfiguration nicht. Man muß bei jeder neu verfassten E-Mail daran denken, sie wenn möglich zu verschlüsseln! Das ist sehr fehleranfällig.

Eine Lösung bietet das Plug-In **Virtual Identity**. Es kann bei jeder versendeten E-Mail die gewählten Einstellungen für die Verschlüsselung speichern. Damit lernt Thunderbird, welche Verschlüsselungseinstellungen für welche Empfänger gelten. Die Einstellungen werden bei jeder neuen E-Mail an den Empfänger als Default aktiviert.

Nach der Installation des Plug-Ins muss man unter dem Menüpunkt *“Extras - Virtual Identity - Einstellungen”* die Speicherung der Einstellungen für die Verschlüsselung aktivieren. (Bild 7.16)

Unter dem Menüpunkt *“Extras - Virtual Identity - Datenspeicher”* findet man die gesammelten Daten und kann sie auch editieren.

### 7.3 Root-Zertifikate importieren

Das Importieren der Zertifikate in Web-Browser und E-Mail-Client erspart lästige Nachfragen, ob man einem mit diesem Root-Zertifikat signierten Zertifikat vertrauen möchte.

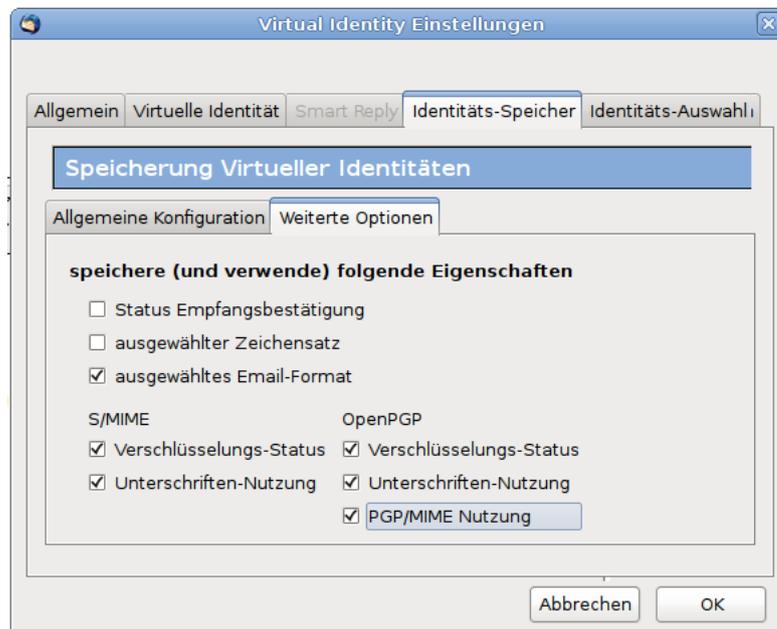


Abbildung 7.16: Einstellungen des Plug-In Virtual Identity

### 7.3.1 Webbrowser Firefox

Nutzer des Browsers Firefox klicken auf auf das *Root Certificate* und aktivieren in dem sich öffnenden Dialog (Bild 7.17) mindestens den ersten und zweiten Punkt.

### 7.3.2 E-Mail-Client Thunderbird

Für den Import der Root-Zertifikate in den E-Mail-Client sind diese lokal zu speichern. In der Regel benötigt man neben dem *Class 1 Root Certificate* auch das *Class 3 Root Certificate*, da mit diesem Unterzertifikat die E-Mail-Zertifikate der Nutzer signiert werden. Nutzer des Browsers Firefox klicken mit der rechten Maustaste auf den Link und wählen aus dem Kontextmenü den Punkt *Ziel speichern unter ...*

Anschließend ist Thunderbird zu starten und der Dialog *Einstellungen* zu öffnen. In der Sektion *Datenschutz / Sicherheit* ist der Button *Zertifikate* zu wählen, um den in Bild 7.18 dargestellten Manager für Zertifikate zu öffnen.

In diesem Dialog ist auf dem Reiter *Zertifizierungsstellen* der Button *Importieren* zu wählen und das zuvor gespeicherte Zertifikat zu importieren. Im Anschluss sind im folgenden Dialog mindestens die ersten beiden Optionen zu aktivieren (siehe Firefox).

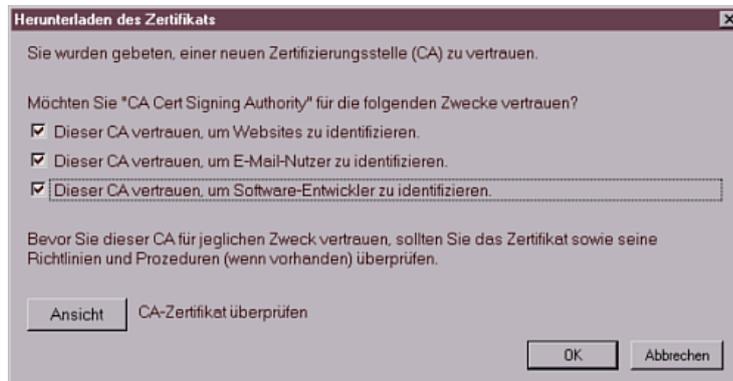


Abbildung 7.17: Herunterladen eines Zertifikates



Abbildung 7.18: Zertifikats-Manager von Thunderbird

## 7.4 Eine eigene Certification Authority

Wer eine eigene Certification Authority (CA) betreiben möchte, benötigt etwas Erfahrung, einige kleine Tools und ein paar Byte Webspace, um das eigene Root-Zertifikate, die Revocation List und die Policy der CA dort zum Download bereitzustellen.

Die OpenSSL-Bibliothek enthält alle nötigen Funktionen, um eine eigene CA zu verwalten. Die Hardcore Version auf der Kommandozeile hat M. Heimpold im Mini-Howto zur Zertifikatserstellung beschrieben.

<http://www.heimpold.de/mhei/mini-howto-zertifikatserstellung.htm>.

Komfortabler geht es mit dem GUI TinyCA (<http://tinyca.sm-zone.net>). Die Website bietet eine Live-CD zum Download an, so dass ich mir weitere Ausführungen zur Installation sparen kann. Unter Debian GNU/Linux kann

man das Tool mit Apt installieren:

```
# apt-get install tinyca
```

Nach dem Start mit dem Kommando *tinyca2* werden in zwei Dialogen die Angaben zum Root-Zertifikat der CA abgefragt. Da TinyCA mehrere CAs verwaltet, kann man erst einmal mit einem Test beginnen.

Abbildung 7.19: Anlegen einer neuen CA

Der *Common Name* der CA kann frei gewählt werden. Das Passwort sollte man sich gut überlegen und keinesfalls vergessen. Mit einem Klick auf *Ok* erscheint ein zweiter Dialog mit weiteren Angaben zur CA. Wichtig sind hier die URL der Revocation List für zurückgezogene Zertifikate und die URL der Policy der CA. Die Policy ist ein HTML-Dokument, welches beschreibt, wer ein Zertifikat von dieser CA erhalten kann, also z.B. etwas in der Art: *Nur für persönlich Bekannte!*

Im Anschluss können die E-Mail Zertifikate der Nutzer erstellt werden. Die nötigen Angaben sind selbsterklärend (Bild 7.20). Mit einem Klick auf *Ok* wird das S/MIME-Zertifikat erstellt und mit dem Root-Zertifikat der CA signiert. Dabei wird das Passwort für den geheimen Key der CA abgefragt.

Um einem Nutzer sein Zertifikat zur Verfügung zu stellen, ist es in eine Datei zu exportieren. Das PKCS#12-Format (\*.p12) enthält den geheimen und den öffentlichen Schlüssel, ist mit einem Passwort gesichert und kann von allen E-Mail Clients importiert werden.

Das Root-Zertifikat der CA ist als DER- oder PEM-Format zu exportieren. Diese Datei enthält nur den öffentlichen Schlüssel des Zertifikates und kann zum Download bereitgestellt werden. Außerdem ist regelmäßig eine Revocation List mit abgelaufenen oder zurückgezogenen Zertifikaten zu erstellen

Erstelle Anforderung

**Erstellen einer neuen Zertifikats Anforderung**

Comon Name (z.B. Ihr Name, Ihre eMail Adresse oder der Name des Servers): Pitti Platsch

eMail Adresse: pitti@maerchen.de

Passwort (sichert den privaten Schlüssel):

Passwort (Bestätigung):

Land (2 Buchstaben-Code): DE

Bundesstaat oder Provinz: Berlin

Standort (z.B. Stadt): Berlin

Organisation (z.B. Firma): privat

Organisationseinheit (z.B. Abteilung):

Schlüssellänge:  4096  1024  2048

Digest:  SHA-1  MD2  MDC2  MD4  MD5  RIPEMD-160

Algorithmus:  RSA  DSA

OK Abbrechen

Abbildung 7.20: Erstellen eines E-Mail Zertifikats

und ebenfalls zum Download unter der angegebenen URL bereitzustellen. Die Oberfläche bietet für beide Aufgaben einen Button in der Toolbar.

## 7.5 Ist S/MIME-Verschlüsselung unsicher?

Nach unserer Einschätzung ist die S/MIME-Verschlüsselung wesentlich schwächer, als OpenPGP. Die Ursachen liegen nicht in einer Schwäche der verwendeten Algorithmen, sondern in der Generierung und Speicherung der privaten Schlüssel außerhalb der Hoheit des Anwenders.

Die Sicherheit asymmetrischer Kryptografie hängt entscheidend von der Vertrauenswürdigkeit der privaten Schlüssel ab. Während der öffentliche Schlüssel möglichst breit zu verteilen ist, muss die Verfügungsgewalt für den privaten Schlüssel ausschließlich und vollständig(!) in der Hand des Anwenders liegen. Nur so kann gewährleistet werden, dass kein unbefugter Dritter die vertrauliche Kommunikation entschlüsseln kann.

Um die Nutzung der S/MIME-Verschlüsselung für unbedarfte Anwender zu erleichtern, wird die Erzeugung und Aufbewahrung der privaten Schlüssel häufig durch organisatorische Schwächen kompromittiert.

### Erzeugen der privaten Keys

Alle Anbieter von Zertifizierungen für X.509 Zertifikate bieten eine webbasiertes Interface für die Erzeugung und Signatur der Zertifikate. In der Regel werden nach erfolgreicher Überprüfung der Identität des Antragstellers zwei Varianten für die Generierung eines gültigen Zertifikates angeboten:

1. Man kann nach in einer selbst gewählten sicheren Umgebung den privaten Schlüssel und ein Certification Request (CSR) erzeugen. Der CSR



Abbildung 7.21: Zertifikat exportieren

enthält nur den öffentlich Schlüssel. Dieser wird im Webinterface hochgeladen und man erhält via E-Mail oder Download Link das signierte Zertifikat.

2. Man die komplette Generierung des privaten und öffentlichen Schlüssels der CA überlassen und muss darauf vertrauen, dass dieser keine Kopie des privaten Schlüssels speichert.

Aus Bequemlichkeit nutzt die absolute Mehrheit der Anwender den 2. Weg und geht damit das Risiko ein, dass die Schlüssel bereits vor der Verwendung kompromittiert werden könnte.

In einem Forschungspapier kommen die Sicherheitsforscher C. Soghoian und S. Stamm zu dem Schluss, dass die US-Regierung von kooperierenden Certification Authorities die privaten Keys von X509-Zertifikaten erhalten könnte und die US-Behörden somit die Daten problemlos entschlüsseln können. Eine ähnliche Zusammenarbeit gibt es unserer Meinung nach auch zwischen Startcom-SSL und dem israelischen Geheimdienst.

### Der Deutsche Bundestag

Der Deutsche Bundestag bietet allen Abgeordneten die Möglichkeit, S/MIME für die Verschlüsselung von E-Mails zu verwenden.

Die Abgeordneten sind scheinbar nicht über diese Möglichkeit informiert. Bei der technischen Umsetzung gilt das Prinzip *Security by obscurity*, wie ein Testbericht zeigt (<http://www.heise.de//tp/r4/artikel/27/27182/1.html>).

Um die Abgeordneten maximal von der "komplizierten" Technik des Entschlüsselns der E-Mail zu entlasten, erfolgt die Entschlüsselung auf einem zentralen Server des Bundestages. Auf diesem zentralen Server liegen auch die privaten Schlüssel und die Zertifikate der Abgeordneten.

Damit ist gesichert, dass auch die Sekretärinnen keine Probleme haben, wenn der Absender einer E-Mail diese verschlüsselt und damit sicherstellen wollte, dass nur der Abgeordnete selbst sie lesen kann.

Hier wird eine Vertraulichkeit der Kommunikation vorgegaukelt. Gefährlich wird dieser Placebo, wenn ein Bürger auf die Sicherheit vertraut und sich gegenüber seinem Abgeordneten freimütiger äußert, als er es unverschlüsselt tun würde.

### **Web.de (Free-) Mail-Account**

Beim Anlegen eines Mail-Accounts bei Web.de wird automatisch ein S/MIME-Zertifikat für den Nutzer generiert. Der öffentliche und der private Schlüssel liegen auf dem Server des Anbieters. Der Schlüssel ist nicht durch ein Passwort geschützt.

Dieses Feature wird von Web.de wie folgt beworben:

*“Versehen Sie Ihre E-Mail mit einer digitalen Unterschrift, kann diese auf dem Weg zum Empfänger nicht verändert werden. Die digitale Verschlüsselung sorgt dafür, dass die E-Mail auf dem Weg zum Empfänger nicht gelesen werden kann.”*

Außerdem fordert die Website dazu auf, das Zertifikat im eigenen E-Mail Client zu importieren und für die Verschlüsselung zu nutzen.

Diese Variante von S/MIME ist ein Placebo, den man ignorieren sollte.

Die Werbebotschaft entspricht nicht der Wahrheit. Gemäß geltendem Recht ist die E-Mail beim Empfänger angekommen, wenn der Empfänger Gelegenheit hatte, sie zur Kenntnis zu nehmen. Vorher kann sie jedoch auf dem Server von Web.de entschlüsselt werden (auch von staatlichen Stellen).

### **Projekt De-Mail**

Auch das geplante Portale De-Mail für die rechtsverbindliche und sichere deutsche Alternative zur E-Mail soll X.509 Zertifikate für die Gewährleistung der vertraulichen Kommunikation nutzen. Die Anforderungen sehen eine Entschlüsselung der vertraulichen E-Mails durch Betreiber des Dienstes ausdrücklich vor. Als Grund wird die Notwendigkeit des Virescans genannt.

Außerdem wirbt das Projekt damit, den Nutzern einen “Datentresor” für vertrauliche digitale Dokumente zur Verfügung zu stellen. Das Konzept kann jedoch nur als Placebo bezeichnet werden. Sowohl die verschlüsselten Dokumente als auch die Schlüssel für den Zugriff auf die Dokumente sollen beim Anbieter des Dienstes liegen. Die Entschlüsselung der vertraulichen Daten durch Mitarbeiter ist ebenfalls ausdrücklich vorgesehen.

Das Projekt De-Mail wird in Zusammenarbeit mit dem ePA einen Key-Escrow (Hinterlegung der Schlüssel bei den Behörden) für unbedarfte An-

wender vorantreiben. Den Anwendern wird eine Sicherheit vorgegaukelt, die durch Behörden einfach kompromittiert werden kann.

### Schlußfolgerung

Im Gegensatz zu OpenPGP kann man bei S/MIME nicht sicher davon ausgehen, dass der Gegenüber seinen privaten Schlüssel selbst generiert hat und dass der Schlüssel ausschließlich ihm zur Verfügung steht. Es besteht damit die Gefahr, dass die Vertraulichkeit der Kommunikation nicht umfassend gewährleistet ist.

In extremen Fällen ist die angebotene Verschlüsselung nur ein Placebo.

Staatliche Projekte wie der ePA zusammen mit dem Projekt De-Mail weichen die Sicherheit der S/MIME Verschlüsselung weiter auf.

## 7.6 Eine Bemerkung zum Abschluß

*“Mache ich mich verdächtig, wenn ich meine E-Mails verschlüsselt?”*

Eine Frage, die häufig gestellt wird, wenn es um verschlüsselte E-Mails geht. Bisher gab es darauf folgende Antwort:

*“Man sieht es einer E-Mail nicht an, ob sie verschlüsselt ist oder nicht. Wer befürchtet, dass jemand die Mail beschnüffelt und feststellen könnte, dass sie verschlüsselt ist, hat einen Grund mehr, kryptografische Verfahren zu nutzen!”*

Aktuelle Ereignisse zeigen, dass diese Frage nicht mehr so einfach beantwortet werden kann. Dem promovierten Soziologen Andrej H. wurde vorgeworfen, Mitglied einer terroristischen Vereinigung nach §129a StGB zu sein. Der Haftbefehl gegen ihn wurde unter anderem mit **konspirativem Verhalten** begründet, da er seine E-Mails verschlüsselte.

Am 21.Mai 2008 wurden in Österreich die Wohnungen von Aktivisten der Tierrechtsszene durchsucht und 10 Personen festgenommen. Der Haftbefehl wurde mit Verdunklungsgefahr begründet, da die Betroffenen z.B. über verschlüsselte E-Mails kommunizierten.

Am 18.10.07 hat der Bundesgerichtshof (BGH) in seinem Urteil [Az.: StB 34/07](#) den Haftbefehl gegen Andrej H. aufgehoben und eindeutig festgestellt, dass die Verschlüsselung von E-Mails als Tatverdacht NICHT ausreichend ist, entscheidend sei der Inhalt:

*“Ohne eine Entschlüsselung der in den Nachrichten verwendeten Tarnbegriffe und ohne Kenntnis dessen, was bei den - teilweise observierten und auch abgehörten - Treffen zwischen dem Beschuldigten und L. besprochen wurde, wird hierdurch eine mitgliedschaftliche Einbindung des Beschuldigten in die ‘militante gruppe’ jedoch nicht hinreichend belegt.”*

Außerdem geben die Richter des 3. Strafsenat des BGH zu bedenken, dass Andrej H. *“ersichtlich um seine Überwachung durch die Ermittlungsbehörden wusste”*. Schon allein deshalb konnte er *“ganz allgemein Anlass sehen”*, seine Aktivitäten zu verheimlichen. Woher Andrej H. von der Überwachung wusste, steht bei <http://annalist.noblogs.org>.

Trotz dieses Urteils des BGH bleibt für uns ein bitterer Nachgeschmack über die Arbeit unser Ermittler und einiger Richter. Zumindest die Ermittlungsrichter sind der Argumentation der Staatsanwaltschaft gefolgt und haben dem Haftbefehl erst einmal zugestimmt.

## Kapitel 8

# E-Mail jenseits der Überwachung

Auch bei der Nutzung von GnuPG oder S/MIME für die Verschlüsselung von E-Mails ist es mitlesenden Dritten möglich, Absender und Empfänger zu protokollieren und anhand der erfassten Daten Kommunikationsprofile zu erstellen. Insbesondere die Vorratsdatenspeicherung und die darauf aufbauenden internationalen ETSI-Standards für Geheimdienste und Strafverfolger zeigen, dass diese nicht verschlüsselbaren Informationen für die Überwachung bedeutsam sind.

Es gibt mehrere Projekte, die einen überwachungsfreien Austausch von Nachrichten ermöglichen und somit beispielsweise für investigative Journalisten und deren Informanten den nötigen Schutz bieten und die Erstellung von Kommunikationsprofilen für E-Mails behindern. Eine universelle Lösung auf Knopfdruck gibt es nicht. Jeder muss selbst die verschiedenen Möglichkeiten vergleichen und die passende Lösung auswählen.

### 8.1 Anonyme E-Mail Accounts

Im Kapitel Anonymisierungsdienste gibt es Anleitungen, wie man mit JonDo & Thunderbird oder mit Tor & Thunderbird einen anonymen E-Mail Account nutzen könnte. Als E-Mail Provider kann man einen zuverlässigen Anbieter im Web nehmen. Außerdem bieten I2P und Tor spezielle Lösungen:

- Das Invisible Internet Project (I2P) bietet mit Susimail einen anonymen Mailservice inklusive SMTP- und POP3-Zugang und Gateway ins Web oder mit I2P-Bote einen serverlosen, verschlüsselten Mailsdienst.
- Das *Lelantos-Project* ist ein E-Mail Dienst, der von Unbekannten als Tor Hidden Service unter der Adresse <http://lelantoss7bcnwvbv.onion> betrieben wird. *Mail2Tor* ist ein weiterer E-Mail Dienst, der von Unbekannten unter <http://mail2tor2zyjdctd.onion> bereitgestellt wird. Gateways ins normale Web sind bei beiden Projekten vorhanden.

**Hinweis:** Informationen über Langzeitkommunikation können ein Pseudonym deanonymisieren. Anhand der Freunde in der E-Mail Kommunikation sind Schlussfolgerungen auf ihre reale Identität möglich. Wenn sie einen wirklich anonymen E-Mail Account für eine bestimmte Aufgabe benötigen - z.B. für Whistleblowing - dann müssen sie einen neuen Account erstellen. Löschen sie den Account, sobald sie ihn nicht mehr brauchen.

## 8.2 Private Messages in Foren nutzen

Viele Diskussionsforen im Internet bieten die Möglichkeit, private Nachrichten zwischen den Mitgliedern zu verschicken. Die Nachrichten werden in der Datenbank des Forums gespeichert und nicht per E-Mail durch das Netz geschickt.

Eine böse Gruppe ganz gemeiner Terroristen könnte sich also in einem Forum anmelden, dessen Diskussionen sie überhaupt nicht interessieren. Dort tauschen sie die Nachrichten per PM (Private Message) aus und keiner bemerkt die Kommunikation. Es ist vorteilhaft, wenn das Forum komplett via HTTPS nutzbar ist und nicht beim Login HTTPS anbietet.

Die Nachrichten kann man mit OpenPGP verschlüsseln, damit der Admin des Forums nichts mitlesen kann. Die Verwendung von Anonymisierungsdiensten sichert die Anonymität.

## 8.3 alt.anonymous.messages

Um die Zuordnung von Absender und Empfänger zu erschweren, kann man das Usenet nutzen. In der Newsgruppe *alt.anonymous.messages* werden ständig viele Nachrichten gepostet und sie hat tausende Leser. Jeder Leser erkennt die für ihn bestimmten Nachrichten selbst. Es ist eine Art schwarzes Brett.

Es ist sinnvoll, die geposteten Nachrichten zu verschlüsseln. Dafür sollte der Empfänger einen OpenPGP-Key bereitstellen, der keine Informationen über seine Identität bietet. Normalerweise enthält ein OpenPGP-Schlüssel die E-Mail Adresse des Inhabers. Verwendet man einen solchen Schlüssel ist der Empfänger natürlich deanonymisiert.

Außerdem sollte man seine Antworten nicht direkt als Antwort auf ein Posting veröffentlichen. Da der Absender in der Regel bekannt ist (falls keine Remailer genutzt wurden) kann aus den Absendern eines zusammengehörenden Thread ein Zusammenhang der Kommunikationspartner ermittelt werden.

## 8.4 Mixmaster Remailer

Der Versand einer E-Mail über Remailer-Kaskaden ist mit der Versendung eines Briefes vergleichbar, der in mehreren Umschlägen steckt. Jeder Empfänger innerhalb der Kaskade öffnet einen Umschlag und sendet den darin

enthaltenen Brief ohne Hinweise auf den vorherigen Absender weiter. Der letzte Remailer der Kaskade liefert den Brief an den Empfänger aus.

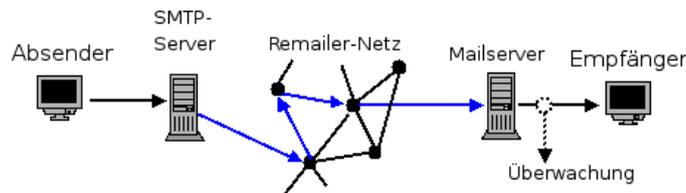


Abbildung 8.1: Konzept einer anonymen E-Mail

Technisch realisiert wird dieses Prinzip mittels asymmetrischer Verschlüsselung. Der Absender wählt aus der Liste der verfügbaren weltweit verteilten Remailer verschiedene Server aus, verschlüsselt die E-Mail mehrfach mit den öffentlichen Schlüsseln der Remailer in der Reihenfolge ihres Durchlaufes und sendet das Ergebnis an den ersten Rechner der Kaskade. Dieser entschlüsselt mit seinem geheimen Schlüssel den ersten Umschlag, entnimmt dem Ergebnis die Adresse des folgenden Rechners und sendet die jetzt (n-1)-fach verschlüsselte E-Mail an diesen Rechner. Der letzte Rechner der Kaskade liefert die E-Mail an den Empfänger aus.

Mitlesende Dritte können lediglich protokollieren, dass der Empfänger eine E-Mail unbekannter Herkunft und evtl. unbekanntes Inhalt (verschlüsselt mit OpenPGP oder S/MIME) erhalten hat. Es ist ebenfalls möglich, Beiträge für News-Groups anonym zu posten.

Um die Traffic-Analyse zu erschweren, wird die Weiterleitung jeder E-Mail innerhalb der Kaskade verzögert. Es kann somit 2...12h dauern, ehe die Mail dem Empfänger zugestellt wird! Sollte der letzte Remailer der Kette die Nachricht nicht zustellen können (z.B. aufgrund eines Schreibfehlers in der Adresse), erhält der Absender keine Fehlermeldung. Der Absender ist ja nicht bekannt.

**Wichtig:** Bei großen E-Mail Providern werden die anonymen E-Mails aus dem Mixmaster Netzwerk häufig als Spam einsortiert. Es ist somit nicht sichergestellt, dass der Empfänger die Mail wirklich zur Kenntnis nimmt! Oft beschwerten sich Nutzer bei mir, dass ihre Testmails an den eigenen Account nicht ankommen, weil sie auch nicht in den Spam-Ordner schauen.

**Wichtig:** Da die E-Mail keine Angaben über den Absender enthält, funktioniert der *Antworten-Button* der Clients auf der Empfängerseite nicht! Die Antwort-Mail geht dann an den letzten Remailer der Kette, der sie in die Tonne wirft. Der Text der anonymen E-Mail sollte einen entsprechenden Hinweis enthalten!

Software zur Versendung anonymen E-Mails via Mixmaster:

- Für Windows gibt es *Quicksilver* <https://quicksilvermail.net>

- Für Linux und BSD gibt es *mixmaster*. Das Paket ist in allen Linux Distributionen enthalten und kann mit dem bevorzugten Tool zur Paketverwaltung installiert werden.
- Wer sich nicht mit der komplizierten Konfiguration beschäftigen möchte, der kann eine Live-CD nutzen. Die JonDo Live-CD enthält *mixmaster*.

### Mixmaster installieren (Linux, BSD)

Mixmaster ist ein Kommandozeilen Tool, welches die Nachrichten mehrfach verschlüsselt an das Remailer Netzwerk übergibt. Für Debian, Ubuntu und Mint gibt es fertige Pakete in den Repositories. Die Installation folgt dem üblichen Schema:

```
> apt-get install mixmaster
```

Die Sourcen von Mixmaster stehen unter <http://mixmaster.sourceforge.net> zum Download bereit. Für die Übersetzung werden die Entwicklerpakete folgender Komponenten benötigt, welche von nahezu allen Distributionen bereitgestellt werden:

- vi Editor
- ncurses Bibliothek
- OpenSSL Bibliothek
- PCRE Bibliothek
- zlib Bibliothek
- OpenPGP Programm (z.B. GnuPG)

Nach dem Download ist das Archiv zu entpacken und in das neu angelegte Verzeichnis zu wechseln. Hier ist das Kommando *.Install* einzugeben.

Die Installationsroutine stellt einige kurze Fragen und bietet sinnvolle Vorgaben. Als Installationsverzeichnis ist es sinnvoll *\$HOME/.Mix* zu übernehmen. Die Frage *Do you want to set up a remailer?* ist mit ENTER zu verneinen.

Die Meldung *Client installation complete.* zeigt den erfolgreichen Abschluss der Installation an.

### Mixmaster konfigurieren

Die Konfiguration von Mixmaster erfolgt in der Datei *\$HOME/.Mix/mix.cfg*. Linux wird an dieser Stelle seinem Ruf als Volltext Adventure gerecht.

1. Für die Versendung an den ersten Remailer der Kaskade wird ein Absender und eine Absenderadresse benötigt. Der erste Remailer der Kaskade entfernt diese Angaben, sie werden nicht(!) an den Empfänger übermittelt. Es sind folgende Zeilen in der Konfiguration hinzuzufügen:

```
NAME <absendername>
ADDRESS <absender_email_adresse>
```

2. Außerdem ist die Versandart der Mail an den ersten Remailer der Kaskade zu konfigurieren. In der Regel wird man den SMTP-Server eines E-Mail Providers für die Versendung nutzen. Dafür muss man den Mail-Server und die Login Credentials konfigurieren. Die Daten findet man auf der Webseite des Mailproviders:

```
SMTPRELAY mail.server.tld
SMTPUSERNAME <smtp_nutzer_name>
SMTPPASSWORD <Passwort>
```

3. In der Konfiguration sind die Schlüsselringe für OpenPGP-Verschlüsselung anzugeben:

```
PGPPUBRING /home/<user>/.gnupg/pubring.gpg
PGPSECRING /home/<user>/.gnupg/secring.gpg
```

4. Außerdem sind die Speicherorte für die Statusdateien des Mixmaster Netzwerkes zu konfigurieren. Am einfachsten speichert man die Dateien im Verzeichnis *\$HOME/.Mix*

```
PGPREMPUBASC /home/<user>/.Mix/pubring.asc
PUBRING /home/<user>/.Mix/pubring.mix
TYPE1LIST /home/<user>/.Mix/rlist.txt
TYPE2REL /home/<user>/.Mix/mlist.txt
TYPE2LIST /home/<user>/.Mix/type2.list
```

5. Optional kann man mit CHAIN die Länge der Remailer Kaskade konfigurieren und mit NUMCOPIES mehrere Kopien der E-Mail versenden, um die Wahrscheinlichkeit der Zustellung bei Problemen mit einem Remailer zu verbessern. Um zwei Kopien der E-Mail über unterschiedliche Wege mit 5 statt 3 Remailern pro Kaskade zu versenden, sind folgende Optionen zu konfigurieren:

```
CHAIN *,*,*,*,*
NUMCOPIES 2
```

Werden mehrere Kopien versendet, da schickt der letzte Remailer der Kaskade nur eine E-Mail an den Empfänger und löscht alle weiteren Kopien.

Nachdem man die Konfiguration gespeichert hat, muss man die Liste der verfügbaren Pinger herunterladen. Die sogenannten Pinger stellen die Informationen über die verfügbaren Remailer bereit. Die Liste der Pinger wird mit folgendem Kommando heruntergeladen:

```
> mixmaster --update-pinger-list
```

### Anonyme E-Mails mit Mixmaster versenden

Man kann Mixmaster auf der Kommandozeile im Terminal starten und mit dem rudimentären Menü aus dem letzten Jahrhundert ein E-Mail schreiben und anonym versenden. Standardmäßig nutzt Mixmaster den Editor *vi*, was ein Krampf ist. Besser ist es, vor dem Start einen brauchbaren Texteditor wie *gedit*, *kwite* oder *mousepad* auszuwählen:

```
> export EDITOR gedit
> mixmaster
```

Eine zweite Möglichkeit nutzt einen beliebigen **Texteditor** oder besser eine komplette Textverarbeitung mit Rechtschreibprüfung und Vorlagenverwaltung, um die E-Mail auf Basis der folgenden Vorlage zu schreiben, als TXT-Datei zu speichern und diese mit Mixmaster anonym zu versenden.

```
To:
Subject:
Mime-Version: 1.0
Content-Type: text/plain; charset='utf-8'
Content-Transfer-Encoding: 8bit
```

```
Hallo alle miteinander,
hier beginnt der Inhalt
```

In den ersten beiden Zeilen ist die E-Mail-Adresse des Empfängers und der Betreff der Nachricht einzutragen. Zwischen dem Header und dem eigentlichen Inhalt ist eine Leerzeile frei zu lassen.

Nachdem die Nachricht geschrieben wurde, ist die Datei unter einem neuen Namen als TXT-Datei zu speichern, beispielsweise unter *\$HOME/anon-email.eml*.

Diese E-Mail kann mit den folgenden Befehlszeilen versendet werden, welche für häufige Nutzung auch als Shell-Script gespeichert werden können:

```
> mixmaster --update-stats=noreply
> mixmaster -m ~/anon-email.eml
> mixmaster -S
> shred -u ~/anon-email.eml}
```

Der erste Befehl aktualisiert die Remailer-Statistiken und kann entfallen, wenn diese nicht älter als 24h sind. Unter Debian GNU/Linux ist *mixmaster-update* zu nutzen.

Die zweite Befehlszeile übernimmt die Nachricht, wählt die Remailer-Kette aus und legt eine vorbereitete E-Mail im Spool-Verzeichnis ab. Der dritte Aufruf von Mixmaster versendet alle Mails aus dem Spool-Verzeichnis und der letzte Befehl beseitigt die Datei, indem sie zuerst mit Nullen überschrieben und anschließend gelöscht wird.

Soll die E-Mail an der Empfänger OpenPGP verschlüsselt ausgeliefert werden, ist die zweite Befehlszeile zusätzlich um die Option `-encrypt` zu erweitern.

Im Prinzip ist es auch möglich, Attachements an eine anonyme E-Mail zu hängen. Viele Remailer entfernen diese jedoch. Einige Remailer lassen Attachements bis zu 100KB passieren. Ich bin der Meinung, man kann auf Anhänge verzichten und werde hier nicht weiter darauf eingehen.

### Anonymes Usenet Posting mit Mixmaster versenden

Ein anonymes Usenet-Posting wird als E-Mail an ein Mail2News Gateway geschickt. Diese E-Mail wird durch die Remailer-Kaskade anonymisiert. Das Gateway wandelt die anonyme E-Mail in ein News-Posting um und schickt es an die Newsgroups.

- mail2news (at) bananasplit.info
- mail2news (at) dizum.com
- mail2news (at) reece.net.au
- mail2news (at) m2n.mixmin.net

Wie beim Schreiben einer anonymen E-Mail gibt es zwei Möglichkeiten, um ein anonymes Usenet-Posting zu schreiben. Man kann mixmaster auf der Kommandozeile starten:

```
> export EDITOR gedit
> mixmaster
```

Nach der Aktualisierung der verfügbaren Remailer mit [u] kann man ein Usenet-Posting verfassen mit [p] und anschließend mit [s] versenden.

Eine zweite Möglichkeit nutzt einen beliebigen **Texteditor** oder besser eine komplette Textverarbeitung mit Rechtschreibprüfung und Vorlagenverwaltung, um das Posting auf Basis der folgenden Vorlage zu schreiben, als TXT-Datei zu speichern und diese mit Mixmaster anonym zu versenden.

```
To: mail2news@newsanon.org, mail2news@dizum.org
Newsgroups:
X-No-Archive: Yes
Subject:
Mime-Version: 1.0
Content-Type: text/plain; charset='utf-8';
Content-Transfer-Encoding: 8bit
```

Ich möchte folgendes veröffentlichen: blabla

Zwischen dem Header und dem eigentlichen Inhalt ist eine Leerzeile frei zu lassen.

Nachdem die Nachricht geschrieben wurde, ist die Datei im TXT-Format unter einem neuen Namen zu speichern, beispielsweise unter `$HOME/anon-news.eml`. Diese Datei kann mit den folgenden Befehlszeilen an die Newsgroups gesendet werden:

```

> mixmaster --update-stats=noreply
> mixmaster -m ~/anon-news.eml
> mixmaster -S
> shred -u ~/anon-news.eml

```

Der erste Befehl aktualisiert die Remailer-Statistiken und kann entfallen, wenn diese nicht älter als 24h sind.

### Mixmaster mit Tor Onion Router verwenden

Man kann Mixmaster mit dem Anonymisierungsdienst Tor kombinieren. Ein Beobachter kann damit nicht erkennen, dass eine anonyme E-Mail via Mixmaster versendet wurde.

Dafür benötigt man neben Tor Onion Router und dem Tor-GUI *Vidalia* entweder das Tool *torify* oder *torsocks*. Der Tor Daemon muss am Port 9050 lauschen, damit diese beiden Tools korrekt funktionieren.

Es gibt zwei Tor Hidden Services, die als SMTPRELAY genutzt werden können. Einer dieser beiden Tor Hidden Services sollte in der Konfigurationsdatei *mix.cfg* als SMTP-Server eingetragen werden. Für diese beiden SMTP-Server muss man keine Login Credentials angeben. Als Beispiel eine komplette, funktionsfähige Konfigurationsdatei, in der man nur <USERNAME> durch den eigenen Namen ersetzen muss:

```

NAME Anonymous
ADDRESS ano@nymous.net

SMTPRELAY gbhpq7eihle4btsn.onion

CHAIN *,*,*
NUMCOPIES 2

PGPPUBRING /home/<USERNAME>/gnupg/pubring.gpg
PGPSECRING /home/<USERNAME>/gnupg/secring.gpg

PGPREMPUBASC /home/<USERNAME>/Mix/pubring.asc
PUBRING /home/<USERNAME>/Mix/pubring.mix
TYPE1LIST /home/<USERNAME>/Mix/rlist.txt
TYPE2REL /home/<USERNAME>/Mix/mlist.txt
TYPE2LIST /home/<USERNAME>/Mix/type2.list

```

Alternativ kann man den Tor Hidden Service vom Remailer *frell* nutzen. Dieser SMTP-Server nimmt nur E-Mails für *frell* an. Folgende Zeilen sind in dem Beispiel zu ersetzen:

```

SMTPRELAY zvrqjaxpgxglgjrz.onion
CHAIN frell,*,*

```

Nach Anpassung der Konfiguration startet man Tor und danach Mixmaster unter Kontrolle von *torify* oder *torsocks*. Der bevorzugte Editor ist mit *export* zu setzen, damit man sich nicht bei der Bedienung des Standardeditors vi Gehirnzellen und Finger verrenkt:

```
> export EDITOR gedit  
> torify mixmaster
```

## Kapitel 9

# Instant Messaging (Jabber/XMPP)

Instant Messaging und Chat können für sogenannte synchrone Kommunikation genutzt werden. Wie beim Telefonieren müssen die Kommunikationspartner gleichzeitig online sein und direkt miteinander in Kontakt treten. Das hat den Vorteil, dass die Inhalte nicht auf Servern zwischengespeichert werden müssen und teilweise auch direkt zwischen den Beteiligten ausgetauscht werden. Gegenüber E-Mail bietet Instant Messaging den Vorteil, dass die Metadaten der Kommunikation nicht so einfach ermittelt werden können.

Die Kontaktadressen werden wie bei E-Mails folgermaßen gebildet:

```
<username>@server.tld
```

Wenn man seine Adresse weitergibt oder veröffentlicht, muss man zusätzlich angeben, um welchen Dienst es sich handelt (XMPP, SILC...), um Missverständnisse zu vermeiden.

Ende-2-Ende-Verschlüsselung ist für Instant Messaging mindestens so wichtig, wie für E-Mail. Die Auswertung von 160.000 Überwachungsberichten aus dem Snowden-Fundus zeigt, dass die Geheimdienste diese Kommunikation massiv überwachen.

### 9.1 Jabber (XMPP)

Das Jabber-Protokoll (XMPP) wurde primär für die direkte Kommunikation zwischen zwei Teilnehmern entwickelt. Es ist aber auch möglich, Konferenzräume auf den Jabber-Servern einzurichten (allerdings ohne Ende-zu-Ende Verschlüsselung), Video- und Audio-Chats sind möglich und Dateien können ebenfalls direkt ausgetauscht werden.

Für die Ende-zu-Ende Verschlüsselung zwischen zwei Gesprächspartnern stehen bei XMPP folgende Verfahren zu Auswahl:

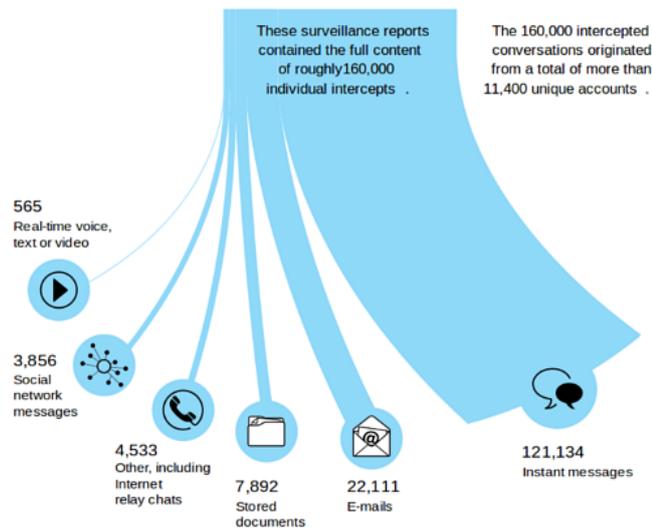


Abbildung 9.1: Auswertung von 160.000 Überwachungsberichten

**Off-the-record (OTR)** wurde von den Cypherpunkts mit dem Ziel entwickelte, möglichst einfach einsetzbar zu sein. Eine OTR-verschlüsselte Verbindung wird automatisch aufgebaut, wenn beide Jabber-Clients dieses Feature unterstützen.

Allerdings muss die Vertrauenswürdigkeit der Verschlüsselung von den Teilnehmern verifiziert werden. Ohne diese Prüfung könnte sich ein Lauscher als man-in-the-middle einschleichen. Die Software für diesen Angriff gibt es auch als Open Source, z.B. `mod_otr` für `ejabberd`. Für die Verifikation der Schlüssel bietet OTR drei Möglichkeiten:

- Vergleich der Fingerprints der Schlüssel.
- Verifizierung mit einem gemeinsamen Passwort.
- Verifizierung durch Frage/Antwort, wobei die Antwort nicht durch Dritte zu erraten sein darf.

Beide Kommunikationspartner müssen die Fingerprints der Schlüssel bzw. das gemeinsame Passwort oder die Frage/Antwort über einen unabhängigen, sicheren Kanal austauschen, bevor sie die OTR-Verschlüsselung verifizieren können.

**OpenPGP** wurde bereits bei der Verschlüsselung von E-Mail behandelt. Die Erstellung und Austausch der Schlüssel ist etwas komplizierter als bei OTR. Die Vertrauenswürdigkeit der Verschlüsselung muss aber nicht extra verifiziert werden, da sie durch das Vertrauen in die OpenPGP-Schlüssel gegeben ist.

Um XMPP zu nutzen installiert man einen Instant Messaging Client (z.B. Pidgin oder Jitsi) mit den evtl. nötigen Plug-ins, erstellt einen (meist)

kostenlosen Account auf einem Jabber-Server, aktiviert die OTR- oder OpenPGP-Verschlüsselung und kann loslegen. (Vorbereitung: 3-5min)

Folgende Jabber-Server respektieren die Privatsphäre der Nutzer und nutzen SSL nach dem Stand der Technik für den Datenverkehr zwischen Client-Server und zu anderen Servern:

| Anbieter                  | Port      | Dateitransfer-proxy   | Bemerkung   |
|---------------------------|-----------|-----------------------|---|
| jabber.calyxinstitute.org | 5222      |                       | TLS + DANE, erzwingt OTR von nine.ch betrieben durch Spenden finanziert |
| swissjabber.org           | 5222, 443 | proxy.swissjabber.com |   |
| jabber.dk                 | 5222      |                       |   |
| draugr.de                 | 5222, 443 | proxy.draugr.de       |   |

Die E-Mail Provider Mailbox.org und Ownbay.de bieten XMPP-Server für ihre Kunden. Mit dem Erstellen eines Kunden Account kann man die XMPP-Server nutzen. Die Aufzählung ist unvollständig, als kleine Anregung gedacht. Umfangreichere Listen gibt es beim IM Observatory<sup>1</sup> (mit einer Bewertung der SSL-Verschlüsselung), bei jabberes.org, bei xmpp.org oder im wiki.ubuntuusers.de.<sup>2</sup>

Bei spendenfinanzierten Server kann man für private Accounts 10-15 Euro pro Jahr investieren, um den Betreiber zu einem langfristigen und stabilen Betrieb des Dienstes zu motivieren.

## 9.2 Jabbern mit Jitsi

Jitsi<sup>3</sup> ist ein VoIP und Instant Messaging Client. Die Software ist in Java geschrieben und steht damit für alle Betriebssysteme zur Verfügung. Jitsi bietet einige Sicherheitsfeatures, die ich bei anderen Jabber Clients vermisste: DNSSEC kann erzwungen werden, die Account Passwörter können mit einem Masterpasswort verschlüsselt gespeichert werden (so wie der GCHQ es empfiehlt), OTR-Verschlüsselung ist vorhanden und muss nicht zusätzlich installiert werden.

### Installation

Jitsi ist ein Java-Programm, man benötigt ein Java Runtime Environment (JRE).

- Unter Linux installiert man das Paket *default-jre* mit dem Paketmanager der Distribution.
- Für Windows findet man das Java Installationsprogramm auf [www.java.com](http://www.java.com). Bei der Installation möchte der Installer unbedingt die Ask-Toolbar installieren. Diese überflüssige Option sollte man deaktivieren, braucht man nicht.

WICHTIG: Der Installer aktiviert auch ein Java-Plugin für alle Browser.

<sup>1</sup> <https://xmpp.net/directory.php>

<sup>2</sup> <http://wiki.ubuntuusers.de/XMPP/Server>

<sup>3</sup> <https://jitsi.org/>

Dieses Plugin ist ein Sicherheitsrisiko und muss nach der Installation im Java Control Panel unter *Systemsteuerung - Programme - Java* deaktiviert werden!

Anschließend installiert man Jitsi, indem man das zum Betriebssystem passende Paket von der Downloadseite <sup>4</sup> herunter lädt und als Administrator bzw. als root installiert - fertig.

### Account erstellen

Das Erstellen eines Jabber (XMPP) Accounts in Jitsi ist einfach. Man wählt den Konto Typ *XMPP* und trägt die Jabber Adresse sowie das Passwort ein. Man kann ein vorhandenes Konto nutzen oder ein neues Konto auf dem Server erstellen lassen.



Abbildung 9.2: Account erstellen (erster Schritt)

Unter *Erweitert* sollte man einige Features des Account anpassen:

- Aus Privacy Gründen empfehle ich, Audio und Videoanrufe via *libjingle* auf dem Reiter *Telefonie* zu deaktivieren. Es sieht nicht schön aus, wenn ich unrasiert im Schlafanzug vor dem Computer sitze und im Audio Chat kann man auch Hintergrundgespräche mithören.
- ICE (Interactive Connectivity Establishment) benötigt man nur für Audio- und Videoanrufe, kann man also auch alles deaktivieren.
- Auf dem Reiter *Verbindung* sind alle Google Features zu deaktivieren.

### OTR-Verschlüsselung

Nach dem man den Account erstellt hat, sollte ein OTR-Schlüssel erzeugt werden. Dafür öffnet man den Dialog *Werkzeuge -> Einstellungen* und geht auf den Reiter *Chat*. Hier findet man auch die Liste der verifizierten OTR-Schlüssel der Kommunikationspartner und kann in den Optionen die Ende-zu-Ende

<sup>4</sup> <https://jitsi.org/index.php/Main/Download>

Verschlüsselung erzwingen.

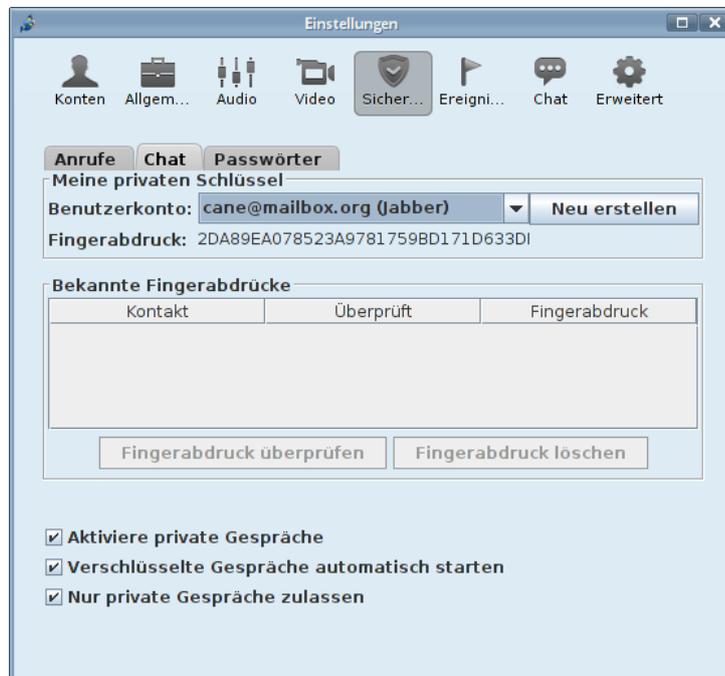


Abbildung 9.3: OTR-Schlüssel für eigenen Account erstellen

Wenn man einen *Sicheren Chat* startet, dann werden die OTR Schlüssel im Hintergrund automatisch ausgetauscht. Um sicher zu sein, dass sich bei diesem Schlüsseltausch kein man-in-the-middle eingeschlichen hat, muss man die Keys verifizieren. Jitsi bietet den Vergleich der Fingerprints, die Authentifizierung über ein gemeinsames Passwort oder eine Frage/Antwort Kombination. Die Fingerprints der OTR-Schlüssel, das gemeinsame Passwort oder die Frage/Antwort sind über einen unabhängigen, sicheren Kanal mit dem Gegenüber zuvor auszutauschen und dürfen nicht durch Dritte zu erraten sein. Den eigenen Fingerprint kann man auch veröffentlichen.

Im Chatfenster während des Gespräches kann man unter dem Menüpunkt *Sicherer Chat - Account verifizieren* den Schlüssel des Gegenüber verifizieren. Manchmal funktioniert mit anderen IM Clients wie Pidgin nur der manuelle Vergleich der Fingerprints der Schlüssel.

### DNSSEC erzwingen

Ein Angreifer könnte prinzipiell die DNS-Einträge manipulieren (DNS Spoofing), um den Verkehr über einen eigenen Server umzuleiten und einen Man-in-the-Middle Angriff auf die Transportverschlüsselung zu ermöglichen. Einige gute Jabber (XMPP) Provider haben die DNS-Einträge mit DNSSEC

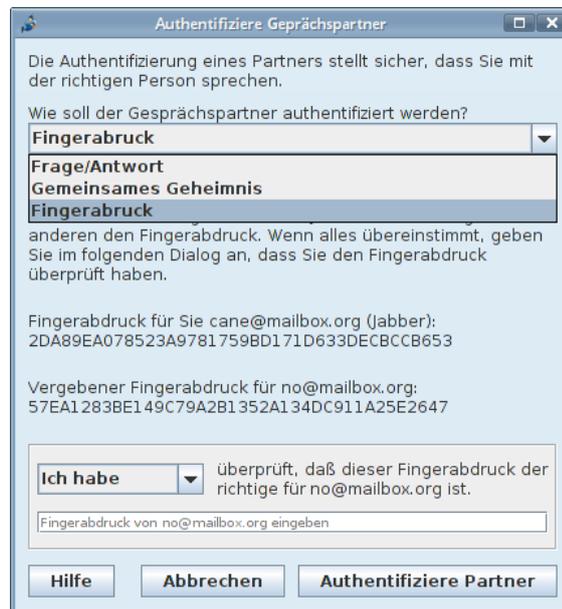


Abbildung 9.4: OTR-Schlüssel des Gegenüber verifizieren

signiert, um diesen Angriff zu verhindern. In den Testergebnissen des IM Repository kann man nachschauen, ob der eigene Provider DNSSEC unterstützt.

Die Nutzung von DNSSEC ist aber optional und könnte deshalb von einem Angreifer unterdrückt werden. In den Einstellungen von Jitsi kann man die Nutzung von DNSSEC erzwingen und für jeden DNS-Eintrag individuell konfigurieren. Dieses Sicherheitsfeature unterscheidet Jitsi von anderen Jabber Clients. Eine Liste von vertrauenswürdigen DNS-Servern mit DNSSEC Support findet man im Kapitel *Betriebssysteme*. Diese DNS-Server kann man als *Benutzerdefinierte DNS-Server* eintragen.

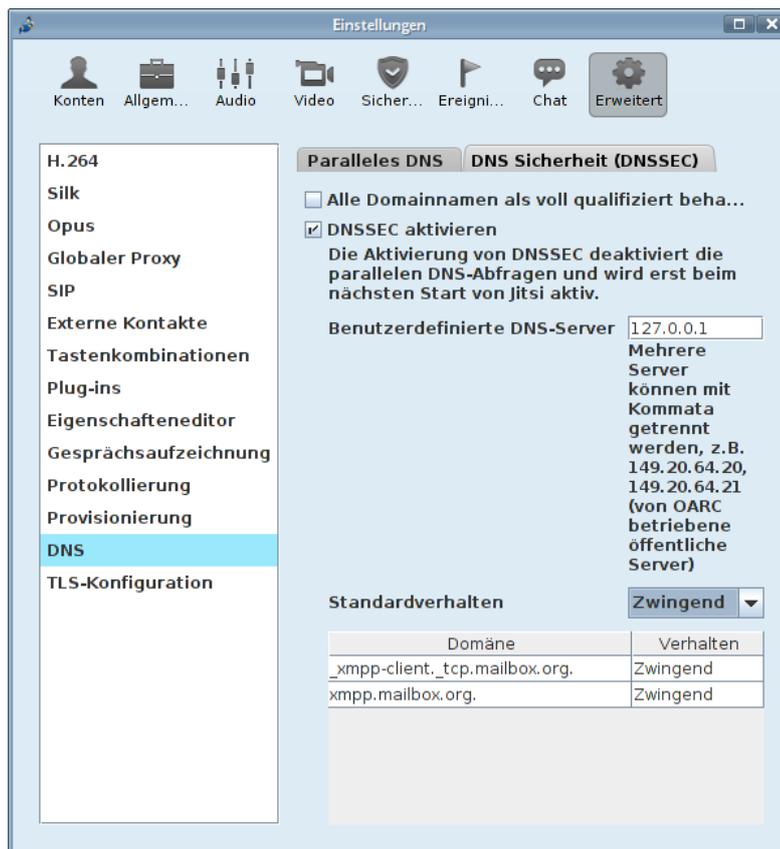


Abbildung 9.5: Jitsi Konfiguration: DNSSEC erzwingen

## Kapitel 10

# Internettelefonie (VoIP)

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 bietet eine Verschlüsselung und kann Verbindungen ins Festnetz und in Handynetze herstellen.

### Abhørschnittstellen

Anfang der 90er Jahre des letzten Jahrhunderts wurde das Festnetz in den westlichen 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.

Als Antwort auf diese Entwicklung wurden in allen westlichen Industriestaaten Gesetze beschlossen, die die Telekommunikationsanbieter zur Kooperation mit den Strafverfolgungsbehörden und Geheimdiensten verpflichten und Abhørschnittstellen zwingend vorschreiben. In den USA war es der *CALEA Act*<sup>1</sup> von 1994. In Deutschland wurde 1995 auf Initiative des Verfassungsschutz die *Fernmeldeverkehr-Überwachungsverordnung* (FÜV)<sup>2</sup> beschlossen, die 2002 durch die *Telekommunikations-Überwachungsverordnung* (TKÜV)<sup>3</sup> 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 Abhørschnittstellen zu implementieren. Mit der Übernahme von Skype durch Ebay im Nov. 2005 wurde die Diskussion beendet. Heute bietet Skype Abhørschnittstellen in allen westeuropäischen Ländern und zunehmend auch in anderen Ländern wie Indien. In Deutschland sind Abhörprotokolle aus Skype Gesprächen

<sup>1</sup> <https://secure.wikimedia.org/wikipedia/en/wiki/Calea>

<sup>2</sup> <http://www.online-recht.de/vorges.html?FUEV>

<sup>3</sup> <https://de.wikipedia.org/wiki/Telekommunikations-%C3%9Cberwachungsverordnung>

alltägliches Beweismaterial.<sup>4</sup>

Skype und andere VoIP-Anbieter, die Verbindungen in andere Telefonnetze herstellen können, sind in gleicher Weise abhörbar, wie Telefon oder Handy. Es ist albern, Skype als Spionagesoftware zu verdammen und gleichzeitig den ganzen Tag mit einem Smartphone rumzulaufen. Genauso ist eine Lüge, wenn man die Verbreitung von Skype als Grund für einen Staatstrojaner nennt.

## 10.1 Open Secure Telephony Network (OSTN)

Das Open Secure Telephony Network (OSTN)<sup>5</sup> wird vom Guardian Project entwickelt. Es bietet sichere Internettelefonie mit starker Ende-zu-Ende-Verschlüsselung, soll als Standard für Peer-2-Peer Telefonie ausgebaut werden und eine ähnlich einfache Nutzung wie Skype bieten.

Eine zentrale Rolle spielt das SRTP/ZRTP-Protokoll<sup>6</sup> von Phil Zimmermann, dem Erfinder von OpenPGP. 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. Daneben werden weitere etablierte Krypto-Protokolle genutzt.

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-Hellman 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 identisch ist, kann man davon ausgehen, dass kein Man-in-the-Middle das Gespräch belauschen kann.

Damit bleibt als einziger Angriff auf die Kommunikation der Einsatz eines Trojaners, der das Gespräch vor der Verschlüsselung bzw. nach der Entschlüsselung abgreift. Dagegen kann man sich mit einer Live-DVD schützen. Die JonDo-Live-DVD enthält z.B. den VoIP-Client Jitsi.

<sup>4</sup> <http://www.lawblog.de/index.php/archives/2010/08/17/skype-staat-hort-mit>

<sup>5</sup> <https://guardianproject.info/wiki/OSTN>

<sup>6</sup> <https://tools.ietf.org/html/draft-zimmermann-avt-zrtp-22>

### 10.1.1 OSTN-Provider

Um diese sichere Variante der Internettelefonie zu nutzen, benötigt man einen Account bei einem OSTN-kompatiblen Provider. Derzeit bietet nur Ostel.co<sup>7</sup> eine vollständige Umsetzung von OSTN. Die Serversoftware OSTel ist Open Source, man kann auch seinen eigenen Server betreiben.

Die SRTP/ZRTP-Verschlüsselung ist ausschließlich von den Fähigkeiten der VoIP-Clients abhängig. Sie kann nicht nur mit den OSTN-Providern genutzt werden sondern auch mit Accounts bei anderen SIP-Providern wie z.B. Ekiga.net oder iptel.org. Allerdings vereinfacht OSTN die Konfiguration der Accounts im VoIP-Client.

### VoIP-Clients mit OSTN-Support

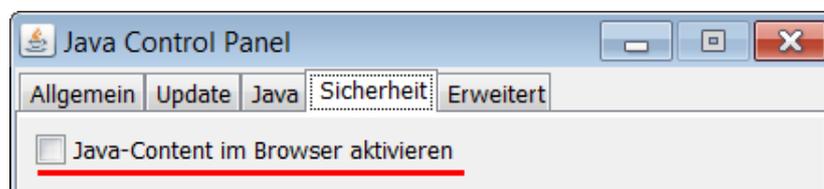
Es gibt einige VoIP-Clients, die bereits die nötigen Voraussetzungen zur Nutzung von OSTN implementiert haben.

- Für den Desktop empfehle ich *Jitsi*<sup>8</sup>, einen Java-basierter VoIP- und IM-Client für viele Betriebssysteme.
- Für Linux (Ubuntu, SUSE und Redhat) gibt es das SFLphone<sup>9</sup>.
- Für Android-Smartphones ist *CSipSimple*<sup>10</sup> am besten geeignet, das ebenfalls vom Guardian Project entwickelt wird.
- iPhone Nutzer können *Groundwire*<sup>11</sup> für \$9,99 im App Store kaufen.

## 10.2 VoIP-Client Jitsi

Jitsi ist einen Java-basierter VoIP- und Instant Messaging Client für viele Betriebssysteme. Er unterstützt die SRTP/ZRTP-Verschlüsselung und das OSTN-Protokoll. Für die Installation benötigt man zuerst einmal Java.

**Java für Windows:** Das Installationsprogramm für Java gibt auf der Webseite [www.java.com](http://www.java.com)<sup>12</sup>. Der Installer möchte unbedingt die *Ask-Toolbar* für alle Browser installieren. Das sollte man deaktivieren, braucht man nicht.



<sup>7</sup> <https://ostel.co>

<sup>8</sup> <https://jitsi.org>

<sup>9</sup> <http://sflphone.org>

<sup>10</sup> <http://nightlies.csipsimple.com>

<sup>11</sup> <https://itunes.apple.com/us/app/groundwire-business-caliber/id378503081?mt=8>

<sup>12</sup> <http://www.java.com/de/>



Abbildung 10.1: Account Daten eintragen

**WICHTIG:** Der Installer aktiviert auch ein Java-Plugin für alle Browser. Dieses Plug-in ist ein Sicherheitsrisiko und muss im Java Control Panel unter *Systemsteuerung - Programme - Java* deaktiviert werden!

**Java für Linux:** Installieren Sie als erstes das Paket *default-jre* mit der Paketverwaltung der Distribution.

**Jitsi installieren:** Anschließend installiert man Jitsi, indem man das zum Betriebssystem passende Paket von der Downloadseite <https://jitsi.org> herunter lädt und als *Administrator* bzw. *root* installiert - fertig.

Hat man einen Account bei einem OSTN-Provider, dann muss man lediglich beim Start von Jitsi die Login Daten für den SIP-Account (Username und Passwort) eingeben, wie im Bild 10.1 dargestellt. Alle weiteren Einstellungen werden automatisch vorgenommen.

Wenn man einen Account beim SIP-Provider *iptel.org* hat, ist die Konfiguration ähnlich einfach. Man schließt den *Sign in* Dialog, wählt den Menüpunkt *File - Add new account* und in dem sich öffnenden Dialog als Netzwerk *iptel.org*. Jitsi enthält vorbereitete Einstellungen für diesen SIP-Provider.

### SAS Authentication

Bei einem verschlüsselten Gespräch wird beiden Teilnehmern eine Zeichenkette aus vier Buchstaben und Zahlen angezeigt. Diese Zeichenkette ist über den Sprachkanal mit dem Gegenüber zu verifizieren. Dabei nennt der Anrufer üblicherweise die ersten zwei Buchstaben und der Angerufene die letzten beiden Buchstaben bzw. Zahlen. Wenn beide Teilnehmer die gleiche Zeichenkette sehen, ist die Verbindung sicher verschlüsselt und unbeobachtet.

### Anpassung der Konfiguration

Standardmäßig sind bei Jitsi viele Protokollierungen aktiv. In den den Einstellungen kann man diese Logfunktionen abschalten, um überflüssige Daten auf der Festplatte zu vermeiden.

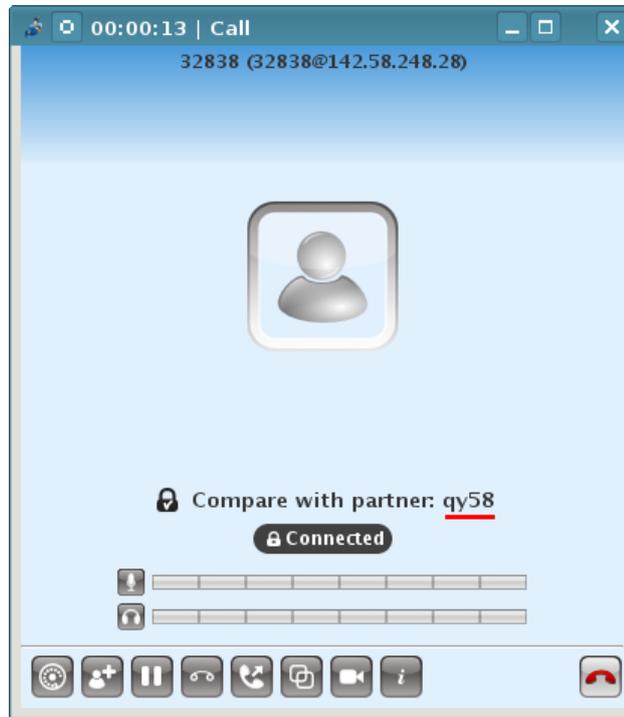


Abbildung 10.2: SAS Authentication

Wer durch die Gerüchte über die Fortschritte der NSA beim Knacken von AES128 etwas verunsichert ist, kann in den Einstellungen des ZRTP Ninja die Verschlüsselung mit Twofish bevorzugen. Allerdings müssen beide Gesprächspartner diese Anpassung vornehmen.

# 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 DoubleClick verhindert man effektiver, indem man den Zugriff auf Werbung unterbindet. Anbieter wie z.B. Google erfordern es, Cookies und JavaScript im Browser zu kontrollieren. Anderenfalls wird man trotz Nutzung von Anonymisierungsdiensten identifiziert.

### 11.1 Warum sollte man diese Dienste nutzen?

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. (Internet 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 täglichen Rasterfahndung nutzt. Facebook gibt täglich 10-20 IP-Adressen an US-Behörden, AOL übergibt 1000 Adressen pro Monat. . .
  5. **Vorratsdatenspeicherung:** Ein Schreiben des Bundesdatenschutzbeauftragten an das Bundesverfassungsgericht macht viele unglaubliche Verstöße gegen die Nutzung der VDS-Daten offenkundig. Es werden häufig mehr Daten gespeichert, als gesetzlich vorgegeben. Auch die Bedarfsträger halten sich nicht an die Vorgaben des BVerfG.

*Zitat: So haben mir sämtliche Anbieter mitgeteilt, dass es recht häufig vorkomme, dass Beschlüsse nicht den formellen Anforderungen ... genügen. Wenn die Anbieter in derartigen Fällen entsprechenden Auskunftersuchen nicht nachkämen, würde ihnen oft die Beschlagnahme von Servern oder die Vernehmung der leitenden Angestellten als Zeugen angedroht, um auf diesem Wege eine Auskunft zu erzwingen.*

Die Telekom hat in zwei Monaten 2198 Anfragen beantwortet und dabei wahrscheinlich zu 70% auf VDS-Daten zurück gegriffen. Auch nachdem die Vorratsdatenspeicherung offiziell vom BVerfG beendet wurde, speichern alle Telekommunikationsanbieter weiterhin VDS-ähnliche Datenberge über mehrere Wochen.

6. **Zensur:** Der Datenverkehr kann vom Provider oder einer restriktiven Firewall nicht manipuliert oder blockiert werden. Anonymisierungsdienste ermöglichen einen unzensierten Zugang zum Internet. Sie können sowohl die "Great Firewall" von China und Mauretanien durchtunneln sowie die in westeuropäischen Ländern verbreitet Zensur durch Kompromittierung des DNS-Systems.
7. **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
8. **Leimruten:** Einige Websites werden immer wieder als Honey-pot genutzt. Ein Beispiel sind die Leimrute des BKA. In mehr als 150 Fällen wurden die Fahndungseiten von LKAs oder des BKA als Honey-pot genutzt und

die Besucher der Webseiten in Ermittlungen einbezogen <sup>1</sup>. Surfer wurden identifiziert und machten sich verdächtig, wenn sie sich auffällig für bestimmte Themen interessieren.

9. **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.
10. **Belauschen durch den Dienst:** Im Gegensatz zu einfachen VPNs oder Web-Proxys schützen die hier vorgestellten 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.

## 11.2 Tor Onion Router und JonDonym

Ein kurzer, oberflächlicher Vergleich soll die technischen Unterschiede zwischen verschiedenen Diensten zeigen und Hilfe bei der Entscheidung bieten.

### Tor Onion Router

Tor nutzt ein weltweit verteiltes Netz von 2400 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.

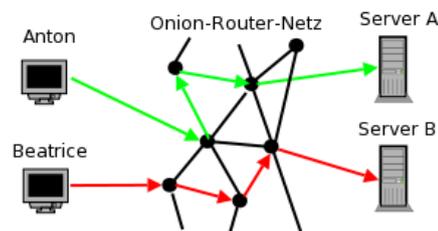


Abbildung 11.1: Prinzip von Tor

Da die Route ständig wechselt, müsste ein großer Teil des Netztes kompromittiert worden sein, um einen Zusammenhang von Surfer und angefragter

<sup>1</sup> <http://heise.de/-1704448>

Webseite herstellen zu können.

Die weltweite Verteilung der Nodes und der hohe Anteil privater Rechner mit langsamer Internetanbindung kann zu deutlich langsameren Downloads führen.

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 sogenannte *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, der HTTP-Header, ETags aus dem Cache oder Javascript 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.
- 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. Im Februar 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.
- 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.

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, SSL-Warnungen nicht einfach 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 Hidden Services bieten Möglichkeiten, anonym und zensurresistent zu publizieren.

## JonDonym

JonDonym arbeitet mit wenigen festen Mix-Kaskaden, bestehend aus zwei oder drei Knoten. Diese Knoten sind leistungsfähige Computer mit schneller Internetanbindung. Die Daten der einzelnen Nutzer werden mehrfach verschlüsselt, weitergeleitet und gemixt. Informationen über verfügbare Kaskaden werden von Infoservices bereitgestellt, die Abrechnung der Premium-Accounts erfolgt über die Bezahlinstanz der JonDos GmbH.

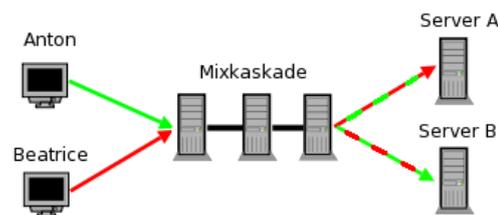


Abbildung 11.2: Prinzip von JonDonym

Der Dienst bietet derzeit kostenfrei nutzbare Mix-Kaskaden und Premium-Kaskaden, die nur gegen Bezahlung nutzbar sind. Die kostenfreien Mix-Kaskaden bieten nur eine geringe Geschwindigkeit von 30-50 kB/s und sind nur für anonymes Surfen nutzbar. Erst mit den Premium-Kaskaden entfaltet der Dienst seine volle Leistung. Diese Kaskaden bieten hohe Geschwindigkeit und sind für alle Protokolle nutzbar (Instant-Messaging, SSH, E-Mail...).

Anonymes Surfen erfordert mehr, als nur die IP-Adresse zu verstecken. Der JonDoFox ist ein Profil für Firefox, das optimal für diese Aufgabe vorbereitet ist (auch für Tor geeignet).

Strafverfolgung: Einzelne Verbindungen können bei JonDonym gezielt überwacht werden, wenn alle Betreiber einer Mix-Kaskade einen richterlichen Beschluss in ihrem Land erhalten. Für Mix-Betreiber aus Deutschland ist eine Gerichtsbeschluss nach §100a StPO nötig. Im Gegensatz zu Tor und I2P ist damit eine Verfolgung schwerer Verbrechen prinzipiell möglich.

Die internationale Verteilung der Kaskaden verhindert eine pauschale Überwachung. Inzwischen sind alle kostenfreien und Premium-Kaskaden internationalisiert. Nach Aussage der JonDos GmbH gab es bisher noch nie eine internationale Zusammenarbeit der Behörden bei einer Überwachung und damit auch keine Überwachung der Premium-Kaskaden. Politische Aktivisten können das Risiko weiter minimieren, indem sie Kaskaden ohne deutsche Mixe nutzen.

Schnüffelnde Mix-Server wurden bisher nicht bekannt.

### 11.2.1 Finanzierung der Anonymisierungsdienste

Wie wird die Entwicklung der Software und die Infrastruktur des Dienstes finanziert und welche Abhängigkeiten ergeben sich möglicherweise daraus?

#### Tor Onion Router

Die Softwareentwicklung wird durch Spenden finanziert. TorProject.org benötigt pro Jahr ca. 1 Mio. Dollar für die Weiterentwicklung der Software und den Betrieb weniger Kernkomponenten des Dienstes. Die Grafik 11.3 zeigt die Zusammensetzung der Spender für 2009 (Quelle Tor Financial Report 2009).

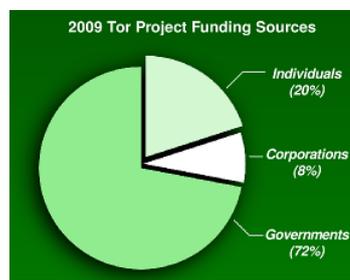


Abbildung 11.3: Anteil der Finanzierung von TorProject.org

Die Hauptsponsoren der NGOs, Companies und Einzelspender werden von TorProject.org auf der Webseite <https://www.torproject.org/about/sponsors.html.en> veröffentlicht. Der große Anteil "Gouvernements" (72% der Einnahmen) kommt von US-Regierungsorganisationen und zu einem kleineren Teil von der schwedischen Regierung. Diese Spenden werden nicht einzeln aufgelistet.

Der Hauptteil der Infrastruktur wird von Enthusiasten finanziert und technisch in der Freizeit betreut. Die Kosten von 600-800 Euro pro Power-Server und Jahr sind als weitere Spenden anzusehen, die in der Grafik nicht erfasst sind. Die Administratoren ziehen keinen Vorteil aus ihrem Engagement, abgesehen von einem Zwiebel-T-Shirt.

#### Jondonym

Das Projekt AN.ON als Vorläufer von JonDonym wurde von 2000-2005 aus dem deutschen Forschungsetat mit insgesamt 1. Mio Euro finanziert. Die Finanzierung wurde 2006 von Schleswig-Holsteins Justizminister U. Döring (SPD) im Rahmen der damaligen Anti-Terror-Kampagne wie folgt kritisiert:

*Es ist nicht mehr zu verantworten, Steuergelder für ein Projekt bereitzustellen, das es Terroristen und Straftätern aller Art ermöglicht, unentdeckt Straftaten zu begehen.*

Seit dem Ende der Förderung bemüht sich die JonDos GmbH, die Finanzierung durch kostenpflichtige Premium-Angebote zu sichern. Für dieser

Angebote ist eine volumenabhängige Gebühr im Voraus zu bezahlen. Die Einnahmen sollen die Kosten für die Weiterentwicklung der Software, die Betreuung des Projektes und die Infrastruktur der Premium-Dienste decken. Dieses Ziel ist noch nicht vollständig erreicht.

Die Entwicklung der Software wird zu 70% aus den Einnahmen der Premium-Dienste finanziert und zu 30% aus Forschungsprojekten in Kooperation mit Universitäten. Die Premium-Mix-Kaskaden werden kostendeckend durch Einnahmen finanziert.

### 11.2.2 Security Notes

Die Sicherheit von IP-Anonymisierern wie Tor und JonDonym ergibt sich nicht alleine aus der Qualität der Anonymisierungssoftware. Durch Fehler in der verwendeten Anwendung oder falsche Konfiguration kann die Anonymität komplett ausgehebelt werden.

- Wer die Browser Google Chrome, iCap, Safari oder einen anderen auf WebKit basierenden Browser für anonymes Surfen verwendet, kann durch FTP-Links deanonymisiert werden. Der Anonymitätstest von JonDonym demonstriert es.
- Wer in seinem Standardbrowser nur die Proxy-Einstellungen anpasst um Tor oder JonDo zu verwenden, ist auch nicht sicher anonym. Eine Deanonymisierung ist mit WebRTC sowie Flash- oder Java-Applets möglich. Diese Features sind unbedingt zu deaktivieren!
- Viele Jabber Clients (XMPP) anonymisieren DNS-Requests nicht. Der IM-Client Pidgin (Version < 2.8) hat außerdem Probleme mit Voice- und Video-Chats. Die Proxy-Einstellungen werden bei Voice- und Video-Chats übergangen und es ist möglich, einen User mit einer Einladung zum Voice-Chat zu deanonymisieren.
- Einige Protolle übertragen die IP-Adresse des eigenen Rechners zusätzlich in Headern des Protokoll-Stacks. Ein Beispiel dafür sind nicht-anonyme Peer-2-Peer Protokolle wie BitTorrent. Damit ist es ebenfalls möglich, User zu deanonymisieren. Eine wissenschaftliche Arbeit zeigt, wie 10.000 BitTorrent Nutzer via Tor deanomisiert werden konnten.
- 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 und JonDos empfehlen für anonymes Surfen ausdrücklich eine angepasste Version des Browser Mozilla Firefox (TorBrowser bzw. JonDoFox). Nur diese Konfiguration kann als wirklich sicher nach dem aktuellen Stand der Technik gelten. Die vielen Sicherheitseinstellungen dieser beiden Browser-Erweiterungen 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 oder JonDonym genutzt werden.
- Verwenden Sie ausschließlich die Originalsoftware der Entwickler.

## 11.3 Tor Onion Router nutzen

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. Das Tor Onion Router Netzwerk besteht gegenwärtig aus ca. 2500 Servern (Nodes), die weltweit verteilt sind.

### 11.3.1 Anonym Surfen mit Tor

Das TorBrowserBundle ist für anonymes Surfen vorbereitet. Es enthält einen modifizierten Firefox als Browser sowie den Tor Daemon und ein Control Panel. 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 den bevorzugten Archiv-Manager oder erledigt es auf der Kommandozeile mit:

```
tar -xaf tor-browser-*
```

Anschließend wechselt man in das neu erstellte Verzeichnis und startet das Script **TorBrowser Setup**.

Beim ersten Start öffnet sich zuerst das Kontroll 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.



Abbildung 11.4: Start des TorBrowser

### 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

1. Im Sommer 2013 wurden tausende Tor-Nutzer mit dem FBI-Trojaner *Magneto* infiziert, der einen Javascript Bug im TorBrowser mit einem Exploit ausnutzte.
2. 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.<sup>2</sup>
3. Außerdem geht aus den Snowden Dokumenten hervor, dass die NSA eine *QUANTUMCOOKIE insert attack* aktiv nutzt, um Tor Nutzer zu de-

<sup>2</sup><http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity>

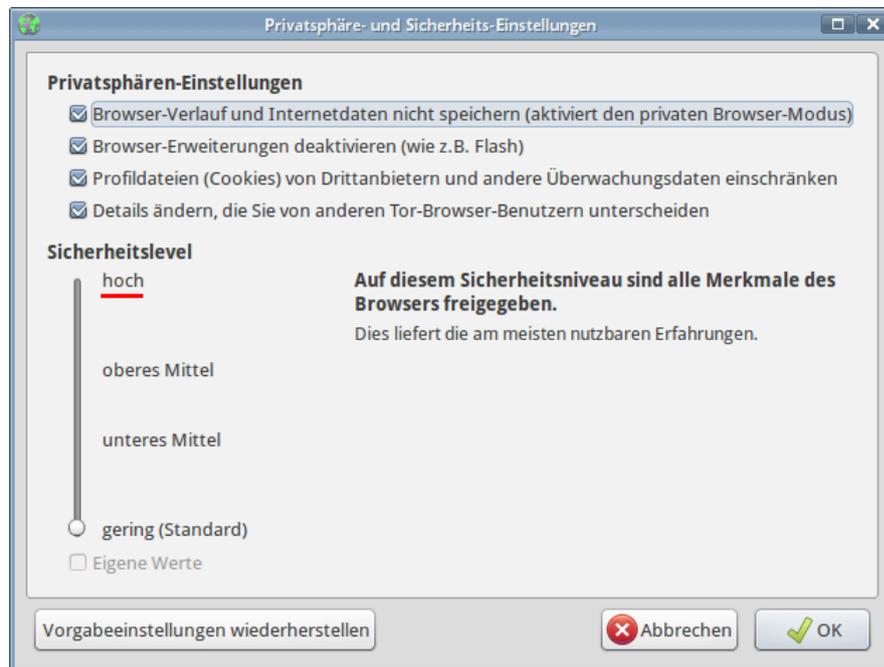


Abbildung 11.5: Sicherheitseinstellungen im TorBrowser anpassen

anonymisieren.<sup>3</sup>

Die Tor-Entwickler haben den Tradeoff zwischen einfacher Benutzbarkeit und Sicherheit in den Default-Einstellungen zugunsten einfacher Benutzbarkeit entschieden. Es wird 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 ab TorBrowser Version 4.5 darauf hingewiesen, dass man die Sicherheitseinstellungen anpassen kann. TorBrowser startet standardmäßig mit dem niedrigsten Sicherheitslevel *gering*, um das Surferlebnis möglichst wenig einzuschränken. Bei Bedarf kann man den Sicherheitslevel erhöhen.

Ich empfehle den umgekehrten Weg. Meiner Meinung nach sollte man den Sicherheitslevel auf *hoch* setzen und nur verringern, wenn es unbedingt für die Nutzung einer (vertrauenswürdigen) Webseite nötig ist und wenn die Webseite via HTTPS oder als Tor Hidden Service geladen wurde. Wenn die Webseite

<sup>3</sup> <http://www.wired.com/2013/11/this-is-how-the-internet-backbone-has-been-turned-into-a-weapon/>

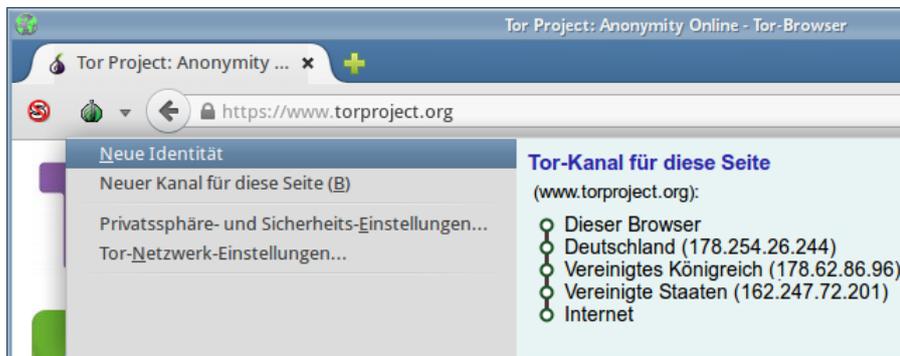


Abbildung 11.6: Neue Identität im TorBrowser wählen

unverschlüsselt via HTTP geladen wurde, würde ich die Sicherheitseinstellungen nicht reduzieren, da bösartige Exit Nodes dann unschöne Dinge in den HTML Code einfügen könnten.

### Cookies und EverCookies

Alle Cookies und alle bekannten EverCookie Markierungen werden beim Beenden des TorBrowsers gelöscht oder wenn man den Menüpunkt *Neue Identität* der Zwiebel in der Toolbar wählt (Bild 11.6). Man sollte dem Anonymitätskonzept des TorBrowser folgen und bei Bedarf gelegentlich alle Identifikationsmerkmale löschen. Insbesondere vor und nach dem Login bei einem Webdienst sollte man alle Markierungen entfernen, um eine Verknüpfung des Surfverhaltens mit Accountdaten zu verhindern.

### PDFs und andere Dokumente

Auf der Downloadseite des TorBrowserBundles findet man unten einige Sicherheitshinweise<sup>4</sup>, 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 address.*

*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.*

<sup>4</sup><https://www.torproject.org/download/download>

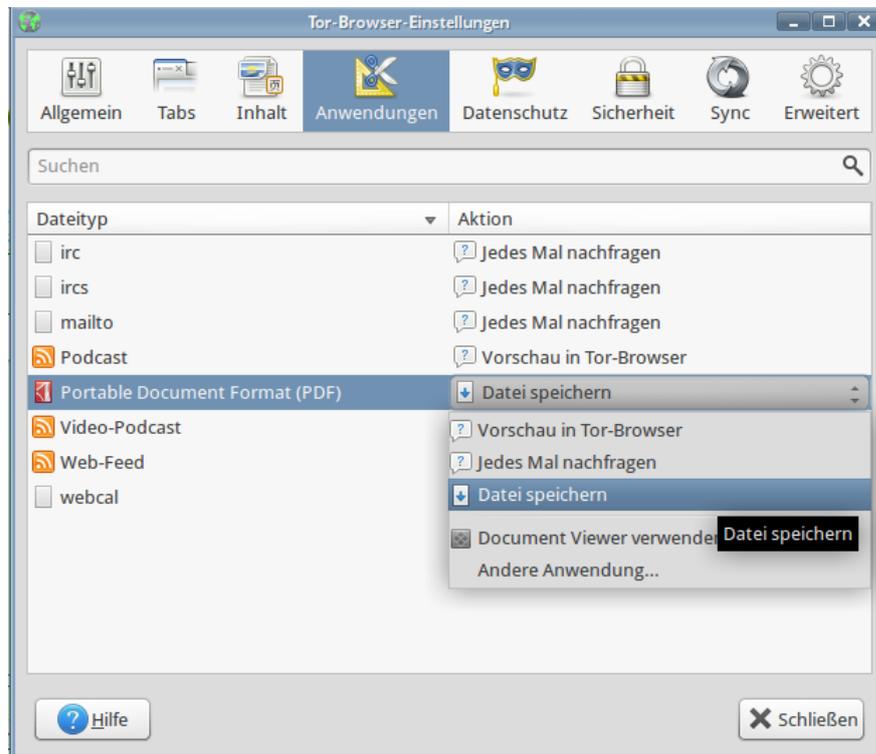


Abbildung 11.7: Einstellungen für PDF-Dokumente im TorBrowser

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, empfehle ich, die Einstellung im TorBrowser für PDF-Dokumente zu ändern und auf *Speichern* zu 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.

Mit dem Metadata Anonymisation Toolkit (MAT) kann man PDF-Dokumente nach dem Download säubern. Die Technik von MAT garantiert,

dass die Tracking Wanzen entschärft werden und nicht mehr spionieren können. Die gesäuberten PDFs kann man gefahrlos im Online-Modus öffnen und weitergeben.

### 11.3.2 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 Node im Klartext vor, wenn sie nicht SSL- oder 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 anonymes Surfen via Tor genauso, wie 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.

|                  |   |
|------------------|---|
| apple            | \$232986CD960556CD8053CBEC47C189082B34EF09  |
| CorryL           | \$3163a22dc3849042f2416a785eaeefbfeea10cc48 |
| tortila          | \$acc9d3a6f5ffcd67ff96efc579a001339422687   |
| whistlersmother  | \$e413c4ed688de25a4b69edf9be743f88a2d083be  |
| BlueMoon         | \$d51cf2e4e65fd58f2381c53ce3df67795df86fca  |
| TRHCourtney1..10 | \$F7D6E31D8AF52FA0E7BB330BB5BBA15F30BC8D48  |
|                  | \$AA254D3E276178DB8D955AD93602097AD802B986  |
|                  | \$F650611B117B575E0CF55B5EFBB065B170CBE0F1  |
|                  | \$ECA7112A29A0880392689A4A1B890E8692890E62  |
|                  | \$47AB3A1C3A262C3FE8D745BBF95E79D1C7C6DE77  |
|                  | \$0F07C4FFE25673EF6C94C1B11E88F138793FEA56  |
|                  | \$0FE669B59C602C37D874CF74AFEA42E3AA8B62C6  |
|                  | \$E0C518A71F4ED5AEE92E980256CD2FAB4D9EEC59  |
|                  | \$77DF35BBCDC2CD7DB17026FB60724A83A5D05827  |
|                  | \$BC75DFAC9E807FE9B0A43B8D11F46DB97964AC11  |
| Unnamed          | \$05842ce44d5d12cc9d9598f5583b12537dd7158a  |
|                  | \$f36a9830dcf35944b8abb235da29a9bbded541bc  |
|                  | \$9ee320d0844b6563bef4ae7f715fe633f5ffdba5  |
|                  | \$c59538ea8a4c053b82746a3920aa4f1916865756  |
|                  | \$0326d8412f874256536730e15f9bbda54c93738d  |
|                  | \$86b73eef87f3bf6e02193c6f502d68db7cd58128  |

Diese Tor-Nodes sind nicht mehr online, die Liste ist nur ein Beispiel.

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.<sup>5</sup>
  - (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<sup>6</sup>.
  - (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<sup>7</sup>.

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<br>IP: 89.208.192.83  |
| TorRelay3A2FL     | ee25656d71db9a82c8efd8c4a99ddbec89f24a67<br>IP: 92.48.93.237   |
| lolling           | 1f9803d6ade967718912622ac876feef1088cfaa<br>IP: 178.76.250.194 |
| Unnamed           | 486efad8aef3360c07877dbe7ba96bf22d304256<br>IP: 219.90.126.61  |
| ididedittheconfig | 0450b15ffac9e310ab2a222adecfef35f4a65c23<br>IP: 94.185.81.130  |
| UnFilTerD         | ffd2075cc29852c322e1984555cddfbc6fb1ee80<br>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

<sup>5</sup> <http://www.teamfurry.com/wordpress/2007/11/20/tor-exit-node-doing-mitm-attacks/>

<sup>6</sup> <http://archives.seul.org/or/talk/Mar-2008/msg00213.html>

<sup>7</sup> <https://trac.torproject.org/projects/tor/ticket/8657>

OnionDuke auf Oktober 2013 datieren. Der Bad Exit Node wurde nur gefunden, weil ein Sicherheitsforscher gezielt nach diesem Angriff suchte.<sup>8</sup>

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.<sup>9</sup>

*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.<sup>10</sup>
7. Tor Exit Nodes aus dem Iran sind generell als Bad Exits markiert. Diese Nodes unterliegen der iranischen Zensur. Außerdem wird beim Aufruf von Webseiten über diese Nodes von der staatlichen Firewall ein unsichtbarer IFrame aus dem Hidden Internet<sup>11</sup> 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>
```

8. 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 sein müssen). Zum Engagement des GSHQ wurden keine Zahlen bekannt.
9. 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.

### 11.3.3 Tor Good Exit Nodes

Im Abschnitt *Tor Bad Exits* sind einige Nodes genannt, denen man nicht trauen sollte. Diese Aufzählung kann nicht abschließend und vollständig sein.

Verschiedene Sicherheitsforscher haben nachgewiesen, dass es recht einfach möglich ist, mit schnüffelnden Exits Informationen über die Nutzer

<sup>8</sup> <http://heise.de/-2457271>

<sup>9</sup> <https://lists.torproject.org/pipermail/tor-talk/2015-April/037549.html>

<sup>10</sup> <https://chloe.re/2015/06/20/a-month-with-badonions/>

<sup>11</sup> <http://arxiv.org/abs/1209.6398>

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 können Nutzer in der Tor-Konfiguration Exit Nodes angeben, denen sie vertrauen und ausschließlich diese Nodes als Exit-Nodes nutzen. Welche Nodes vertrauenswürdig sind, muss jeder Nutzer selbst entscheiden, wir können nur eine kurze Liste als Anregung zum Nachdenken liefern.

- Torservers.net ist eine vertrauenswürdige Organisation, die mehrere Exit-Nodes betreibt.
- Die von der Swiss Privacy Foundation betriebenen Server sammeln keine Informationen. Eine Liste der Server findet man unter:  
<https://www.privacyfoundation.de/service/serveuebersicht>.
- Der CCC betreibt nach eigenen Aussagen die Tor Nodes: *chaoscomputerclub42*, *chaoscomputerclub23* ... (wird ergänzt, sobald verifiziert)
- Der Tor Node *FoeBud3* wird wirklich vom FoeBud betrieben.
- .... 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* bzw. für das TorBrowserBundle in *<TorBrowserBundleVerzeichnis>/Browser/TorBrowser/Data/Tor/torrc-defaults* kann man die gewünschten Nodes mit folgenden Optionen konfigurieren:

```
StrictExitNodes 1
ExitNodes $B15A74048934557FCDEA583A71E53EBD2414CAD9,
          $2DDAC53D4E7A556483ACE6859A57A63849F2C4F6,
          $B15A74048934557FCDEA583A71E53EBD2414CAD9,
          $6D3EE5088279027AD8F64FF61A079DC44E29E3DF,
          $9E9FAD3187C9911B71849E0E63F35C7CD41FAAA3,
          $FDBA46E69D2DFA3FE165EEB84325E90B0B29BF07,
          $FDFD125372A694F0477F0C4322E613516A44DF04
```

Die erste Option gibt an, dass nur die im folgenden gelisteten Nodes als Exit verwendet werden dürfen. Für die Liste der Exits nutzt man die Fingerprints der Nodes, beginnend mit einem Dollar-Zeichen. Die Fingerprints erhält man von verschiedenen TorStatus Seiten. Diese Liste enthält die oben genannten Nodes.

### 11.3.4 Tor Hidden Services

Das Tor Netzwerk ermöglicht nicht nur den anonymen Zugriff auf herkömmliche Angebote im Web sondern auch die Bereitstellung anonymer, zensurreisiterter und schwer lokalisierbarer Angebote auf den Tor-Nodes. Der Zugriff auf die Tor Hidden 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 der Angebote nur sehr schwer ermittelt werden können.

#### Tor Hidden Services als Alternative

Es gibt mehrere Angebote im normalen Web, die zusätzlich als Tor Hidden Service anonym und unbeobachtet erreichbar sind. Wenn man Tor nutzt, sollte man diese Hidden Services den normalen Webadressen vorziehen, da dann keine Gefahr durch Bad Tor Exit Nodes besteht.

- *Riseup.net* bietet Kommunikationsdienste für politische Aktivisten. Alle Dienste wie E-Mail (POP3, SMTP, IMAP), Jabber XMPP usw. gibt es als Riseup's Hidden Services.
- Die Suchmaschine *DuckDuckGo* ist unter der Adresse <http://3g2upl4pq6kufc4m.onion> zu finden und die Suchmaschine Metager unter <http://b7cxf4dkdsko6ah2.onion/tor/>. Für Firefox gibt es bei Mycroft Add-ons für die Suchleiste, das diese Hidden Services nutzen.
- Metager (deutsche Suchmaschine) ist unter <http://b7cxf4dkdsko6ah2.onion> zu finden.
- Die E-Mail Dienste von *PrivateDEMail* und *RuggedInbox* sind auch als Tor Hidden Service nutzbar. Um mit anderen Tor Mail Usern zu kommunizieren, kann man eine Hidden Service E-Mail Adresse angeben, um ein Routing durch das normale Internet und die damit verbundene Überwachung zu vermeiden.
- Der XMPP-Server des *CalyxInstitut.org* ist unter [ijeynrc6x2uy5ob.onion](http://ijeynrc6x2uy5ob.onion) erreichbar.
- Das SILC-Netz des CCC Dresden ist unter [t3oisiyugzgvxph5.onion](http://t3oisiyugzgvxph5.onion) erreichbar.
- das Freenode IRC-Netzwerk kann als Tor Hidden Service unter der Adresse [p4fsi4ockecnea7l.onion](http://p4fsi4ockecnea7l.onion) (Port: 6667) genutzt werden (nur mit registriertem Nick!)
- <https://keys.indymedia.org> ist ein Webinterface für die Suche nach OpenPGP-Schlüsseln. Es ist ein Hidden Service erreichbar unter <http://qtt2yl5jocgrk7nu.onion>.

- Wikileaks bietet eine Submission Plattform für Uploads unter <http://wlupld3ptjvsgwqw.onion> und einen sicheren Webchat unter <http://wlchatc3pjwpli5r.onion>.

### Hidden Services für E-Mail imd Jabber/XMPP

Für unbeobachtete Kommunikation gibt es folgenden Dienste, die ausschließlich aus Tor Hidden Service genutzt werden können:

- Das *Lelantos-Project* ist ein E-Mail Dienst, der von Unbekannten als Tor Hidden Service unter der Adresse <http://lelantoss7bcnwv.onion> betrieben wird. Für einen E-Mail Account muss man mit Bitcoins bezahlen, Gateway ins normale Web ist vorhanden.
- *Mail2Tor* ist ein weiterer E-Mail Dienst, der von Unbekannten als Tor Hidden Service unter der Adresse <http://mail2tor2zyjcdtd.onion> betrieben wird. Accounts sind kostenlos, E-Mail können ebenfalls ins normale Internet gesendet und von dort empfangen werden.
- *SIGAIN*T ist ein kostenfreier E-Mail Service mit kostenpflichtigem Premium Angebot unter der Adresse <http://sigaintevyh2rzvw.onion>. Die kostenfreie Version bietet nur ein Webmail Interface. SMTP/POP3/IMAP für die Nutzung mit Thunderbird + TorBirdy gibt es nur für Premium Kunden. E-Mails können ebenfalls ins normale Internet gesendet und von dort empfangen werden.
- *TorBox* ist ein kostenfreier Hidden-only E-Mail Service und unter Adresse <http://torbox3uiot6wchz.onion> erreichbar. Es können keine E-Mails ins normale Internet gesendet oder von dort empfangen werden.
- Eine Liste von Tor Hidden Jabber Server (XMPP) findet man beim IM Repository.<sup>12</sup>

### 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](http://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-get 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 main
```

Zukünftig nutzen alle Tools zur Softwareverwaltung (aptitude, Synaptic, KPackagekit, ...) den Tor Hidden Service für die Installation und Aktualisierung der Software.

<sup>12</sup><https://xmpp.net/reports.php#onions>

### Reputation und Sonstiges

Für die Tor Hidden Services gibt es kein Vertrauens- oder Reputationsmodell. Es ist unbekannt, wer die Hidden Services betreibt und es ist damit sehr einfach, einen honeypot aufzusetzen. Anonym bereitgestellten Dateien sollte man immer ein gesundes Misstrauen entgegen bringen und in Diskussionen wird aus dem Deckmantel der Anonymität heraus alles mögliche behauptet.

Ansonsten kenne ich kaum etwas, dass ich weiterempfehlen möchte. Meine "Sammlung" an reinen Tor Hidden Services enthält im Moment:

- 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).<sup>13</sup>
- 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.
- 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.

---

<sup>13</sup><http://heise.de/-2124930>

## 11.4 JonDonym nutzen

**JonDo** ist das Client-Programm für JonDonym, welches jeder Nutzer des Anonymisierungsdienstes JonDonym auf seinem Rechner installieren muss. Das Programm dient als Proxy für verschiedene Internet Applikationen. Der Datenverkehr wird verschlüsselt und an eine Mix-Kaskade weitergeleitet. Ein GUI ermöglicht die Konfiguration.

JonDo ist in Java programmiert und damit unter verschiedenen Betriebssystem nutzbar. Es wird ein Java Runtime Environment (JRE) benötigt.

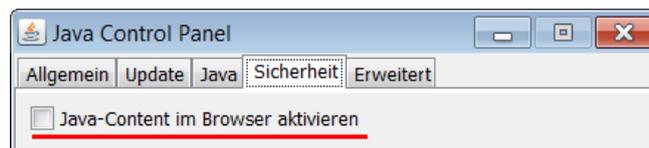
1. Die Downloadseite<sup>14</sup> bietet ein Setup Programm für JonDo, das alle nötigen Komponenten einschließlich Java installiert. Es besteht die Möglichkeit, JonDo auf dem Computer zu installieren, oder als portable Version auf einem USB-Stick. Für die portable Installation auf braucht man keine Administratorrechte und es werden keine Spuren auf dem Rechner hinterlassen.



Abbildung 11.8: Installation von JonDo

Im Anschluss an die portable Installation wird angeboten, auch gleich den JonDoFox (portable Version) für anonymes Surfen zu installieren.

**WICHTIG:** Der Installer aktiviert auch ein Java-Plugin für alle Browser. Dieses Plug-in ist ein Sicherheitsrisiko und muss im Java Control Panel unter *Systemsteuerung - Programme - Java* deaktiviert werden!



2. Für **Ubuntu** sowie **Debian** bietet JonDos fertige DEB-Pakete und ein Software Repository. Um das Repository der JonDos GmbH zu nutzen, ist in

<sup>14</sup> [https://www.anonym-surfen.de/software\\_win.html](https://www.anonym-surfen.de/software_win.html)

der Datei `/etc/apt/sources.list` folgende Zeile einzufügen und DISTRI durch die verwendete Distribution zu ersetzen:

```
deb http://debian.anonymous-proxy-servers.net DISTRI main
```

Das Repository ist mit dem OpenPGP-Key `0xF1305880` signiert, der unter folgender Adresse zum Download bereit liegt:

[https://anonymous-proxy-servers.net/downloads/JonDos\\_GmbH.asc](https://anonymous-proxy-servers.net/downloads/JonDos_GmbH.asc)

Nach dem Download ist der Schlüssel in den APT-Keyring einzufügen:

```
sudo apt-key add JonDos_GmbH.asc
```

Danach kann das Paket `jondo` wie üblich installiert werden.

```
> sudo apt-get update
> sudo aptitude install jondo jondofox-de
```

Nach der Installation kann man JonDo über das Programmmenü starten *Applications -> Internet -> Jondo* oder auf der Kommandozeile mit `jondo`. Wenn man das Browserprofil *JonDoFox* für Firefox/Iceweasel gleich mit installiert, findet man auch einen fertig konfigurierten Browser in der Menügruppe *Internet*.

3. Für andere **Linux/BSD** Distributionen ist als erstes Java zu installieren. Linux-Nutzer installieren das Paket `default-jre` mit dem bevorzugten Paketmanager. BSD-Nutzer können `openjdk7` aus den Ports oder als Package installieren. Im Unterschied zu Windows wird dabei kein Java Plug-in für die Browser installiert.

Anschließend lädt das Archiv `jondo_linux.tar.bz2` von der Downloadseite für Linux<sup>15</sup> herunter, entpackt es und installiert JonDo mit folgendem Kommando:

```
> tar -xjf jondo_linux.tar.bz2
> cd jondo_linux
> sudo ./install_jondo
```

Die Installationsroutine richtet Menüeinträge in der Programmgruppe *Internet* für die gängigen Desktop Umgebungen ein. Auf der Kommandozeile startet man das Proxyprogramm mit `jondo`.

Deinstallieren kann man das Programm mit:

```
> sudo jondo --remove
```

Startet man JonDo, öffnet sich das im Bild 11.9 gezeigte Hauptfenster des Programms. Hier kann man eine Kaskade auswählen und mit Klick auf die Option *Anonymität Ein* die Verbindung herstellen.

<sup>15</sup> [https://www.anonym-surfen.de/software\\_linux.html](https://www.anonym-surfen.de/software_linux.html)



Abbildung 11.9: Hauptfenster von JonDo

### 11.4.1 JonDonym Premium Account einrichten

JonDonym ist ein kommerzieller Dienst, der nicht von Finanzierungen durch Regierungen abhängig ist. Die Einnahmen der Premium-Nutzer bilden Hauptteil der Finanzierung und ermöglichen damit einen von Regierungsinteressen unabhängigen Anonymisierungsdienst.

Die Premium-Dienste von JonDonym bieten folgende Vorteile:

- 20x höhere Geschwindigkeit (siehe: Status der Mix-Server)
- Keine Begrenzung der Dateigröße für Up- und Downloads auf 2 MB.
- Alle Internet-Protokolle nutzbar (kostenfreie Kaskaden nur für Surfen)
- SOCKS5 Support für Anwendungen, die keinen HTTP-Proxy kennen
- Hohe Verfügbarkeit (kostenfreie Kaskaden sind häufig überlastet)
- In der Regel wird der Datenverkehr durch 3 Länder geleitet.

Am einfachsten ist es, wenn man im **Webshop der JonDos GmbH** <sup>16</sup> einen Premium Coupon kauft und mit Paysafecard bezahlt (siehe: *Bezahlen im Netz*). Die Tarife von JonDonym sind auf die angebotenen Paysafecard Gutscheine abgestimmt, so dass man für alle Tarife passende Gutscheine kaufen kann.

Im ersten Schritt wählt man den Tarif und akzeptiert die AGB:

<sup>16</sup> <https://shop.anonymous-proxy-servers.net/bin/payment>

### Auswahl des Premium Tarifs

| Auswahl                          | Tarif    | Preis/Monat | Volumen      | Laufzeit  | Preis (ges.) |
|----------------------------------|----------|-------------|--------------|-----------|--------------|
| <input type="radio"/>            | Flat-M   | 8.33 €      | 2 GB / Monat | 6 Monate  | 50 €         |
| <input type="radio"/>            | Flat-L   | 16.67 €     | 5 GB / Monat | 6 Monate  | 100 €        |
| <input type="radio"/>            | Volume-S |             | 650 MB       | 6 Monate  | 5 €          |
| <input checked="" type="radio"/> | Volume-M |             | 1500 MB      | 1 Jahr(e) | 10 €         |
| <input type="radio"/>            | Volume-L |             | 5000 MB      | 2 Jahr(e) | 30 €         |

**Allgemeine Geschäftsbedingungen der JonDos GmbH** werden akzeptiert.

Bei Volumentarifen gilt das angegebene Volumen ALS GANZES bezogen auf die gesamte Laufzeit. Bei Flat-Tarifen steht das Volumen während der Laufzeit jeden Monat neu zur Verfügung.

Alle Zahlungen sind EINMAL-Zahlungen. Persönliche Daten werden NICHT erhoben.

Tarif auswählen und Gutscheincode kaufen

Im zweiten Schritt kann man die Bezahlmethode wählen.

### 2. Auswahl der Bezahlmethode

| Auswahl                          | Methode               | Daten                          | Buchungszeit   | Bemerkungen            |
|----------------------------------|-----------------------|--------------------------------|----------------|------------------------|
| <input type="radio"/>            | PayPal                | E-Mail-Adresse                 | 5-10 Minuten   | -                      |
| <input checked="" type="radio"/> | Paysafecard           | -                              | < 1 Minute     | nur €, keine \$        |
| <input type="radio"/>            | Liberty Reserve       | Account ID                     | < 1 Minute     | -                      |
| <input type="radio"/>            | Bitcoin               | -                              | 2 Stunden      | 10 € = 1 BTC           |
| <input type="radio"/>            | Überweisung           | Bankverbindung                 | 1-3 Tage       | 0,00-0,30 €            |
| <input type="radio"/>            | Barzahlung per Brief* | Fingerabdruck, Herkunftsregion | 1-7 Tage       | Briefmarke             |
| <input type="radio"/>            | Western Union**       |                                | bis zu 1 Woche | Kosten der Überweisung |

Bezahlmethode wählen und Bezahlung durchführen

Nach der Auswahl von Paysafecard wird man auf die Webseite von Paysafecard weitergeleitet, gibt dort den Gutscheincode ein und erhält dann auf der Webseite von JonDos einen Premium Code (wenn Paysafecard den Gutschein akzeptiert hat).

### Die Bezahlung wurde erfolgreich abgeschlossen

Ihr JonDonym Premium Code: **51D8BD02BD027DE9**

**WICHTIG: Bewahren Sie Ihren JonDonym Code sorgfältig auf!  
Der Code geht verloren, wenn Sie diese Webseite schließen!**

Mit dem Code kann man im JonDo ein Konto erstellen. Im Hauptfenster klickt man auf den Button *Bezahlen*. Es startet ein Assistent, der durch die Einrichtung des Kontos führt. Den Premium Code kann man im ersten Schritt

eingeben - fertig. Zukünftig kann man im Hauptfenster von JonDo Kaskaden mit 3 Mix-Servern wählen, um die Vorteile der Premiumdienste zu genießen.

Konto erstellen

Tarifauswahl

Alle Tarife sind "Prepaid-Tarife" und vollständig im Voraus zu bezahlen.

|   | Preis (Euro)  | Laufzeit | Datenvolumen      | Gesamt     |
|---|---------------|----------|-------------------|------------|
| <input type="radio"/> Medium              | 7,50 / Monat  | 4 Monate | 1,5 GByte / Monat | 30,00 Euro |
| <input type="radio"/> Large               | 18,75 / Monat | 4 Monate | 5,0 GByte / Monat | 75,00 Euro |
| <input type="radio"/> S-Volume            | 5,00          | 6 Monate | 650,0 MByte       | 5,00 Euro  |
| <input checked="" type="radio"/> M-Volume | 10,00         | 1 Jahr   | 1,5 GByte         | 10,00 Euro |
| <input type="radio"/> L-Volume            | 40,00         | 2 Jahre  | 6,5 GByte         | 40,00 Euro |

Oder geben Sie hier einen JonDonym-Code ein

\_\_\_\_ - \_\_\_\_ - \_\_\_\_ - \_\_\_\_

Weiter >    Abbrechen

Abbildung 11.10: Jondonym Premium Code einlösen

### 11.4.2 Anonym Surfen mit dem JonDoFox

JonDoFox ist ein fertiges Profil für Firefox, optimiert für sicheres und anonymes Surfen. Neben der Anpassung der Proxy-Einstellungen bietet es einige Hilfsmittel, um sich anonym im Web zu bewegen. Es wird der HTML-Header modifiziert, Cookies und Javascript werden kontrolliert, SSL-Zertifikate werden überprüft, Werbung wird blockiert und einiges mehr. Pakete zur Installation stehen für verschiedene Betriebssysteme auf der Downloadseite<sup>17</sup> bereit.

Als erstes ist der Browser Mozilla Firefox zu installieren, wenn man bisher einen anderen Browser genutzt hat, und einmal zu starten. Dann kann das JonDoFox Profil installiert werden. Mozilla Firefox fragt zukünftig bei jedem Start, welche Konfiguration genutzt werden soll (Bild 11.11).

#### Erste Schritte nach der Installation

Als Erstes sollte man den Anonymitätstest von JonDos besuchen, um sicher zu gehen, dass alles richtig funktioniert. Ein Lesezeichen ist vorbereitet.  
<http://ip-check.info>

<sup>17</sup> <https://www.anonym-surfen.de/jondofox.html>

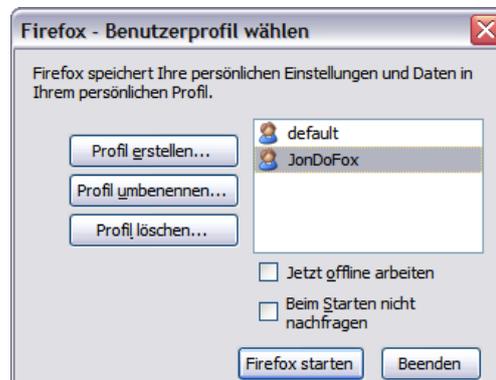


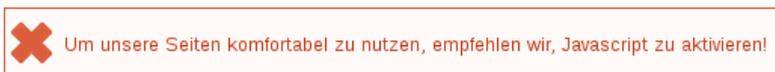
Abbildung 11.11: Profil beim Start von Firefox wählen

Die Lesezeichen kann man vom Profil *default* übernehmen (exportieren und importieren) oder via Firefox Sync holen.

### Cookies und Javascript

JonDoFox setzt einige Restriktionen, um eine hohe Anonymität beim Surfen zu garantieren. Gelegentlich kommt es dabei auch zu Einschränkungen der Funktion einiger Websites.

Um grundsätzlich die Anonymität zu wahren, sind die Annahme von Cookies und das Ausführen von Javascript deaktiviert. Viele Webseiten nutzen Cookies und Javascript. Neben der Sammlung von Informationen über den Surfer können diese Techniken auch sinnvoll eingesetzt werden. Professionelle Webdesigner weisen einen Surfer auf die notwendigen Freigaben hin:



Weniger gute Webseiten liefern seltsame Fehlermeldungen:



Ganz schlechte Websites machen irgendwas, aber nicht was man erwartet.

Bei diesen Problemen sollte man als erstes Cookies temporär freigeben. Diese Kekse wird man einfach wieder los. CookieController ermöglicht es, die Restriktion für einzelne, vertrauenswürdige Webseiten temporär oder dauerhaft aufzuheben.

- Standardmäßig sind Cookies verboten, in der Toolbar ist das Cookie-Icon mit dem roten Kreuz zu sehen.

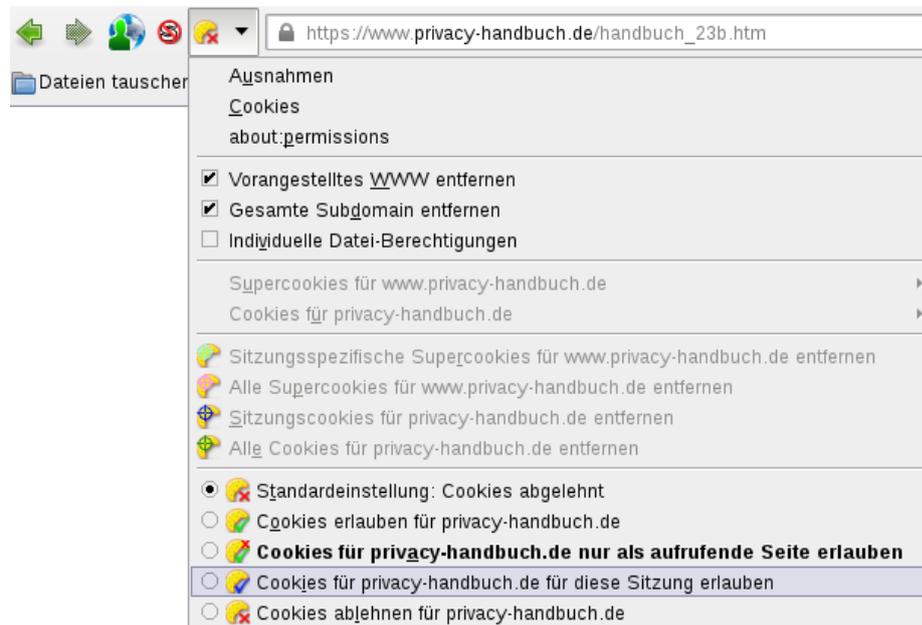


Abbildung 11.12: Cookies für eine Websites freigeben

- Mit einem Klick auf das Icon kann man der aktuellen Webseite das Setzen von Cookies als First-Party erlauben. Dann ist das Icon mit der grünen Ecke + rotes Kreuz zu sehen. Nach dem Logout muss man der Webseite das Setzen von Cookies wieder verbieten.
- Einige große Webseiten und E-Mail Anbieter funktionieren mit der Einschränkung für das Setzen von Cookies nur als First-Party nicht, weil der DOMStorage dabei nicht freigegeben wird (z.B. WEB.de). Für diese Webseiten kann man im Menü von CookieController das Setzen von Cookies allgemein erlauben oder nur für die aktuelle Session erlauben. Das Menü erscheint, wenn man auf den Pfeil neben dem Icon klickt. (Bild 11.12)
- Wenn die Freigabe von Cookies das Problem nicht löst, kann man Javascript für einzelne Domains mit einem Klick auf das NoScript-Symbol neben CookieController temporär freigegeben. Hat man die nötigen Freigaben für Javascript eingerichtet, kann man die Einstellungen für die aktuelle Webseite speichern, um nicht bei jedem Besuch von vorn beginnen zu müssen.
- Bei Mail-Providern (z.B. mailbox.org), die Open-Xchange nutzen, bei den Google Docs und einigen anderen Anbietern sieht man nur einen ewigen Ladebalken. Das liegt daran, dass diese Webseiten Daten in der IndexedBD speichern wollen. Der JonDoFox bietet bisher keine Möglichkeit, dieses Feature mit einem Klick freizugeben. Unter der Adresse *about:config* muss man dann folgende Variable auf true setzen:

```
dom.indexedDB.enabled = true
```

Beim Neustart des Browsers wird der Wert zurück gesetzt. Wenn man dieses Feature dauerhaft aktivieren möchte, kann man folgende Variable setzen:

```
extensions.jondofox.indexedDB.enabled = true
```

### Flash Videos (Youtube o.ä.)

Aus Sicherheitsgründen ist Flash im JonDoFox deaktiviert. Ohne sichere Konfiguration des Flash-Player ist möglich, mit Flash-Applets die Proxy-Einstellungen zu umgehen und die reale IP-Adresse des Surfers zu ermitteln. Außerdem können Flash Applets viele Informationen sammeln und damit das Surfverhalten anhand des Fingerprint des Browser verfolgen.

Um Videos von Youtube o.ä betrachten zu können, ist es nötig, die Videos herunter zu laden und dann mit einem Mediaplayer (z.B. VLC-Player) zu betrachten. Für den Download enthält der JonDoFox das Add-on VideoDownloadHelper. Wenn Sie auf die drei bunten Kugeln neben dem Downloadpfeil rechts oben klicken, dann können Sie die eingebundenen Videos der Webseite in verschiedenen Formaten speichern. Das Format MP4 kann von allen Mediaplayern abgespielt werden.

### Temporäre E-Mail Adressen

Der JonDoFox unterstützt die Verwendung temporärer E-Mail Adressen für die Anmeldung in Foren o.ä. Fünf Anbieter können mit zwei Mausklicks genutzt werden.

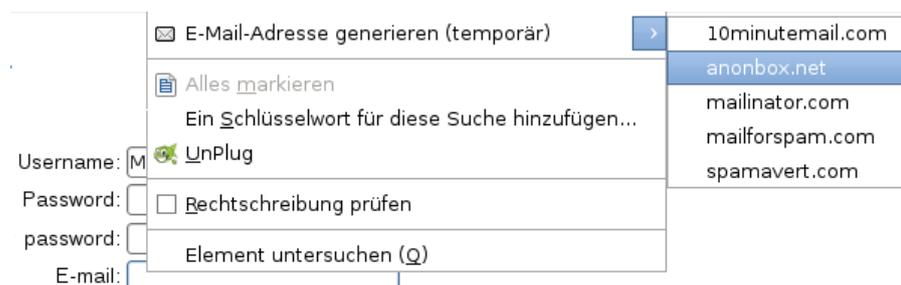


Abbildung 11.13: Temporäre E-Mail Adresse generieren

Um eine temporäre E-Mail Adresse zu nutzen, klickt man mit der rechten Maustaste auf das Eingabefeld für die E-Mail Adresse und wählt den Menüpunkt *E-Mail Adresse generieren (temporär)*. Wenn man auf den kleinen Pfeil am Ende des Menüeintrages klickt, dann kann man den Anbieter auswählen. Anderenfalls wird der Standard-Anbieter genommen, der in den Einstellungen konfiguriert werden kann.

Es wird ein neuer TAB mit dem temporären Postfach geöffnet und gleichzeitig die E-Mail Adresse in das Eingabefeld kopiert. Während man auf die Mail wartet muss man den Posteingang im temporären Postfach öfters aktualisieren. Nutzen Sie dafür nur bei der AnonBox.net den *Reload* Button des Browsers. Bei allen anderen Anbietern wird eine neue Adresse generiert und die alte Adresse ist verloren. Klicken Sie auf den Button *Aktualisieren* in der Webseite!

### Zusätzliche Validierung von SSL-Zertifikaten

In den Einstellungen des JonDoFox können Sie wählen, ob und wie SSL-Zertifikate zusätzlich validiert werden sollen, um *Man-in-the-middle* Angriffe zu erkennen (Bild 11.14).



Abbildung 11.14: Konfiguration der Validierung von SSL-Zertifikaten

1. Wenn man das SSL Observatory der EFF.org nutzen, wird der Fingerprint der SSL-Zertifikate der besuchten Websites zusammen mit dem Domainnamen an das Observatory gesendet und dort mit den Daten verglichen, die andere Nutzer gesendet haben. Sollte mit dem Zertifikat etwas nicht ok sein, wird eine Warnung gezeigt. Standardmäßig wird das SSL-Observatory nur mit JonDo als Proxy genutzt.
2. Alternativ kann man Certificate Patrol nutzen. In einer lokale Datenbank werden die Fingerprints der Zertifikate beim ersten Aufruf der Webseite gespeichert, um später eine Warnung anzuzeigen, wenn sich das Zertifikat unerwartet geändert hat.

## 11.5 Anonyme E-Mails mit Thunderbird

Nicht nur beim Surfen, sondern auch bei jedem Versenden und Abrufen von E-Mails werden IP-Adressen erfasst und ausgewertet. Die anhaltende Diskussion um die Vorratsdatenspeicherung zeigt, dass diese Daten bedeutsam sind. Um unbeobachtet sein E-Mail Konto nutzen zu können, ist es möglich, diese Daten mit Anonymisierungsdiensten zu verschleiern.

### Vorbereitung

Es ist wenig sinnvoll, einen bisher ganz normal genutzten E-Mail Account bei einem Provider mit Vorratsdatenspeicherung plötzlich anonym zu nutzen. Es haben sich in den letzten Monaten genug Daten angesammelt, die eine Identifizierung des Nutzers ermöglichen. Der erste Schritt sollte also die Einrichtung eines neuen E-Mail Accounts sein. In der Regel erfolgt die Anmeldung im Webinterface des Providers. Für die Anmeldung ist ein Anonymisierungsdienst (JonDonym, Tor) zu nutzen. Privacy-freundliche E-Mail Provider findet man im Kapitel *Mozilla Thunderbird nutzen*.

Man kann den E-Mail Account in der Regel komplett im Webinterface des Providers nutzen. Viele Webseiten bieten jedoch keine sichere HTTPS-Verschlüsselung nach dem Stand der Technik und blockieren Tracking Features in E-Mails nicht zuverlässig. Sicherer ist die Nutzung eines E-Mail Clients. Außerdem muss man sich nicht durch ein überladenes Webinterface kämpfen, es gibt keine Probleme mit Cookies und Javascript und die OpenPGP oder S/MIME Verschlüsselung ist wesentlich einfacher und sicherer.

### Thunderbird-Profil erstellen

Ich empfehle, für anonyme E-Mails Thunderbird mit einem anonymen Profil zu nutzen. Ein separates Profil gewährleistet eine konsequente Trennung von nicht-anonymer und anonymer E-Mail Kommunikation. Anderenfalls kommt man bei mehreren Konten schnell einmal durcheinander und gefährdet durch eine hektisch gesendete Mail die Anonymität des Accounts.

Man startet den Profil-Manager in der Konsole bzw. DOS-Box mit der Option -P:

```
> thunderbird -P
```

Es öffnet sich der Dialog Bild [11.15](#) zur Verwaltung verschiedener Profile.

Es ist ein neues Profil zu erstellen und die Option *Beim Starten nicht nachfragen* zu deaktivieren. In Zukunft wird Thunderbird genau wie Firefox bei jedem Start fragen, welches Profil genutzt werden soll.

### Thunderbird-Profil konfigurieren

Am einfachsten konfiguriert man das Profil anonym, indem man das Add-on TorBirdy installiert. Am einfachsten installiert man TorBirdy mit dem Add-on Manager von Thunderbird unter *Extras -> Add-ons*. Im Suchfeld gibt man *TorBirdy* ein. Ein Klick auf den Button *Installieren* holt das Add-on. Nach der Installation muss Thunderbird neu gestartet werden.

Das Add-on TorBirdy erledigt folgende Aufgaben:

- Es werden alle sicherheits- und privacy-relevanten Einstellungen aktiviert, die im Kapitel *Thunderbird nutzen* beschrieben wurden. Eine sichere und anonyme Nutzung ist ohne weitere Konfigurationen gewährleistet.

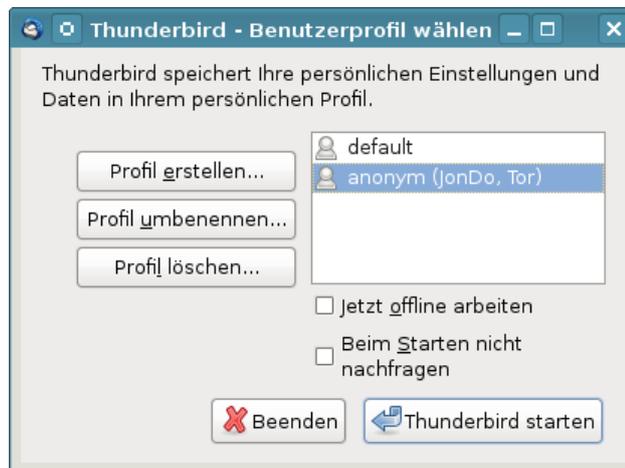
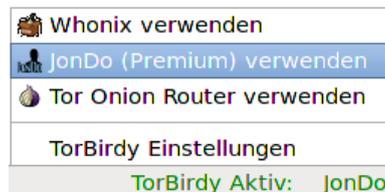


Abbildung 11.15: Profilmanager für Thunderbird

- Der Assistent für die Kontenerstellung wird deaktiviert, da der Assistent aufgrund eines Fehlers unter Umständen den Proxy umgeht. Beim Anlegen eines neuen E-Mail Kontos sind POP3- und SMTP-Server per Hand zu konfigurieren. Dabei ist auf die Aktivierung der SSL-Verschlüsselung zu achten.
- Die Proxy-Einstellung werden angepasst. Dabei kann man in der Statusleiste unten rechts wählen, ob man Tor oder JonDonym (Premium) nutzen möchte.



Um Tor Onion Router zu nutzen, ist das TorBrowserBundle zu starten, für JonDonym ist JonDo zuerst zu starten und eine Premium Mix-Kaskade mit 3 Mix-Servern zu wählen.

Danach kann man das Add-on Enigmail für die OpenPGP-Verschlüsselung installieren und die Wörterbücher der bevorzugten Sprachen hinzufügen.

### OpenPGP Keyserver verwenden

Bei der Verwendung von *JonDo* als Proxy werden auch alle Verbindungen zu den OpenPGP Keyserver anonymisiert, wenn man die Schlüsselverwaltung von Enigmail nutzt.

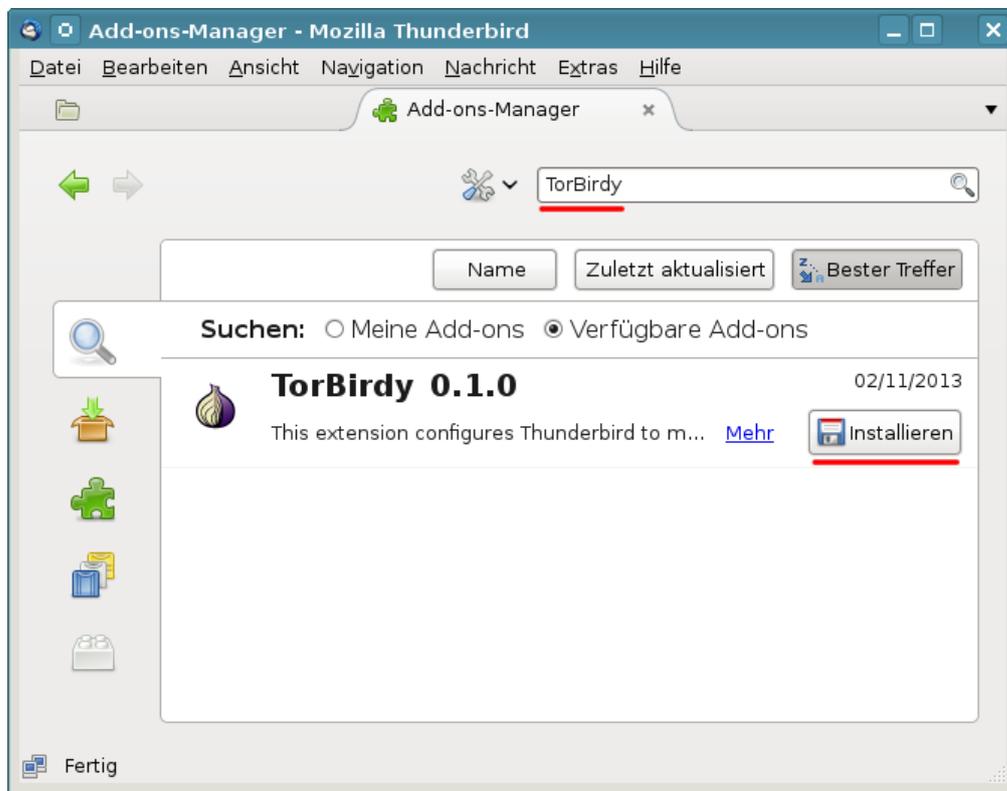


Abbildung 11.16: Add-on aus Datei installieren

Da das TorBrowserBundle keinen HTTP-Proxy mehr enthält, sollte man mit *Tor* keine Keyserver in der Schlüsselverwaltung von Enigmail nutzen. Statt Keyserver kann man den Hidden Service <http://qtt2yl5jocgrk7nu.onion> mit dem TorBrowser nutzen (Hidden Service für <https://keys.indymedia.org>). Im Webinterface kann man nach Schlüsseln suchen oder einen eigenen Schlüssel veröffentlichen. Gefundene Schlüssel kann man mit der Maus markieren, in die Zwischenablage kopieren und dann in der Enigmail importieren.

Live-CDs wie die JonDo Live-CD/DVD sind in der Regel besser konfiguriert und können auch mit *Tor* als Proxy die Keyserver anonym nutzen.

### Hinweise für die Nutzung

Anonymisierungsdienste sperren den Port 25 für die Versendung von E-Mails, um nicht von Spammern missbraucht zu werden. In der Regel bieten die Provider auch den Port 465 für SSL-verschlüsselte Verbindungen oder 587 für TLS-verschlüsselte Versendung von E-Mails.

Im Dialog *Konten...* findet man in der Liste links auch die Einstellungen für den SMTP-Server. In der Liste der Server ist der zu modifizierende Server

auszuwählen und auf den Button *Bearbeiten* zu klicken. In dem sich öffnenden Dialog ist der Port entsprechend zu ändern.

TorBirdy erzwingt sicher SSL/TLS Verbindungen. Nicht alle E-Mail Provider unterstützen eine sichere SSL/TLS Verschlüsselung nach dem Stand der Technik. Probleme mit Yahoo!, Cotse und AOL sind bekannt. Diese Provider bieten keine Secure Renegotiation, was seit 2009 als schwerwiegender Bug im SSL-Protokoll bekannt ist. Wenn ständig, trotz korrekter Konfiguration, nur eine Fehlermeldung beim Senden von E-Mails erscheint, dann kann man mit der OpenSSL Bibliothek prüfen, ob eine sichere SSL-Verschlüsselung überhaupt möglich ist:

```
> openssl s_client -connect smtp.aol.com:465
...
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1
    Cipher  : DHE-RSA-AES256-SHA
    ...
```

Sollte *Secure Renegotiation* NICHT unterstützt werden, kann man sich nur einen neuen E-Mail Provider suchen. Wenn es nicht anders geht, kann man in den Einstellungen von TorBirdy die Verbindung zu unsicheren Mailservern erlauben.

### 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.

### 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 <sup>18</sup> zukünftig alle E-Mails der Gmail Accounts in das NSA-Datacenter in Bluffdale kopiert.

## 11.6 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 (TorBrowserBundle oder JonDo+JonDoFox). Gut geeignet sind die Live-CDs TAILS und JonDo Live-CD, 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.
- 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, Thunderbird als E-Mail Client zu konfigurieren. Man kann die E-Mails auch im Webinterface des Providers im Browser lesen. Dabei ist Tor oder JonDonym zu nutzen.
- Man braucht einen Bloghoster, der anonyme Registrierung oder Registrierung mit Fake-Daten ermöglicht und anonym mit Paysafecard oder UKash bezahlt werden kann.
  - *Wordpress.com* ist empfehlenswert oder die kostenfreie Variante von *Twoday.net*. Um Premium Features bei *Wordpress.com* zu nutzen, kann man seit Nov. 2012 anonym mit Bitcoin bezahlen.<sup>19</sup>

<sup>18</sup> [http://www.wired.com/threatlevel/2012/03/ff\\_nsadatacenter/all/1](http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1)

<sup>19</sup> <http://en.blog.wordpress.com/2012/11/15/pay-another-way-bitcoin/>

- 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*<sup>20</sup> findet man eine die 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, die den Autor deanonymisieren.
- 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. Davon sollte man Gebrauch machen und neue Artikel nicht sofort veröffentlichen, sondern erst 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.

## 11.7 Anonymes Instant-Messaging (Jabber/XMPP)

Verschlüsselte Chats und Instant Messaging in Kombination mit Anonymisierungsdiensten (Tor, JonDo) sind auch für potente Geheimdienste wie die NSA ein Alptraum. Es gibt keine Metadaten, starke Verschlüsselung wie OTR kann noch nicht gebrochen werden und eine Zuordnung von Traffic zu IP-Adressen wird durch die Anonymisierungsdienste verhindert.

Um Jabber/XMPP mit Tor oder JonDo (Premium) zu anonymisieren, muss der Client folgende Anforderungen erfüllen:

1. Es muss ein SOCKS5 bzw. HTTP Proxy konfigurierbar sein, um die Datenverkehr durch den Anonymisierungsdienst zu schicken.
2. Die IP-Adresse des Jabber Servers muss als *Verbindungsserver* konfigurierbar sein, um DNS-Leaks bei den meisten XMPP Clients zu verhin-

---

<sup>20</sup> <https://blackblogs.org/policy/>

dern. Die IP-Adresse kann auf der Webseite DNS Resolve<sup>21</sup> von JonDonym ermitteln.

3. Die *libjingle* für Audio- und Video-Chats muss deaktiviert werden.

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 ohne Proxy herzustellen. Der User kann damit deanonymisiert werden.

### Pidgin für Linux selbst compilieren

Pidgin erfüllt die ersten beiden Anforderungen. Die *libjingle* ist in allen Binärpaketen leider enthalten und kann nicht deaktiviert werden. Um Pidgin mit Tor oder JonDonym zu nutzen, muss man sich selbst eine Version ohne *libjingle* bauen. Für Linux Nutzer ist das ein kleines Full-Text-Adventure, alle anderen Nutzer können die JoToSL-DVD bzw. TAILS nutzen (siehe: Kapitel Live-DVDs).

1. Bevor man mit dem Compilieren anfangen kann, werden die Entwicklerpakete für Gtk2, GtkSpell, libXML, libidn, Mozillas NSS3 Lib, OTR und GnuPG benötigt. Unter Debian/Ubuntu installiert man alles mit:

```
> sudo aptitude install g++ intltool libgtk2.0-dev
libgtkspell-dev libxml2-dev libnss3-dev libidn11-dev
libdbus-glib-1-dev libotr5-dev libpgpme11-dev
```

Optional kann man das Hardening aktivieren, um die selbst erstellten Binaries besser gegen Angriffe zu härten. Es ist das Paket *hardening-wrapper* zu installieren und vor dem üblichen Dreisatz zum Compilieren das Hardening durch Setzen einer Shellvariable zu aktivieren. Der Wrapper kümmert sich dann um die optimale Nutzung der Hardening Funktionen des Compilers und Linkers:

```
> sudo aptitude install hardening-wrapper
> export DEB_BUILD_HARDENING=1
```

Debian *wheezy* ist aufgrund der schwachen Crypto nicht mehr geeignet. Ein Update auf Debian 8 ist dringend empfohlen.

2. Wenn man SILC als verschlüsselte Alternative zu IRC nutzen möchte, dann müssen libsodium und silc-toolkit vor der Installation von Pidgin installiert werden. Nach dem Download und dem Entpacken der beiden Source Archive werden die Bibliotheken mit dem üblichen Dreisatz installiert:

```
> cd libsodium-1.0.2
> ./configure
```

<sup>21</sup> <https://anonymous-proxy-servers.net/bin/dns>

```
> make
> sudo make install

> cd silc-toolkit
> ./configure
> make
> sudo make install
```

3. Den Source Code von Pidgin kann man von der Webseite des Projektes <https://pidgin.im> herunterladen. Nach dem Entpacken des Archives kann man eine sichere Version mit reduziertem Funktionsumfang mit folgenden Befehlen bauen:

```
> cd pidgin-2.10.11

> ./configure --disable-screensaver --disable-gstreamer
--disable-vv --disable-meanswhile --disable-nm
--disable-perl --disable-tcl --disable-avahi
--enable-nss=yes --enable-gnutls=no
--with-system-ssl-certs=/etc/ssl/certs

> make
> sudo make install
```

4. Das OTR Plug-in<sup>22</sup> und das OpenPGP Plug-in<sup>23</sup> für die Ende-zu-Ende Verschlüsselung der Kommunikation sind nicht standardmäßig in Pidgin enthalten. Man muss diese Plug-ins selbst nachinstallieren. Nach dem Download und Entpacken des Source Codes installiert man die Plug-ins wieder mit dem üblichen Dreisatz:

```
> cd pidgin-otr-4.0.1
> ./configure
> make
> sudo make install

> cd pidgin-gpg-0.9
> ./configure
> make
> sudo make install
```

5. Nach der Installation kann man Pidgin starten, die Plug-in Verwaltung öffnen, das Plug-in für die Konfiguration der NSS3 Verschlüsselung aktivieren. Die IETF empfiehlt, ausschließlich TLS 1.2 zu nutzen und stuft nur Cipher mit Forward Secrecy und AES-GCM als sicher ein:

```
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
```

<sup>22</sup> <http://www.cypherpunks.ca/otr/>

<sup>23</sup> <https://github.com/segler-alex/Pidgin-GPG/wiki/Downloads>

Alle anderen TLS Versionen und Cipher sollte man deaktivieren, um TLS Downgrade Angriffe zu verhindern.

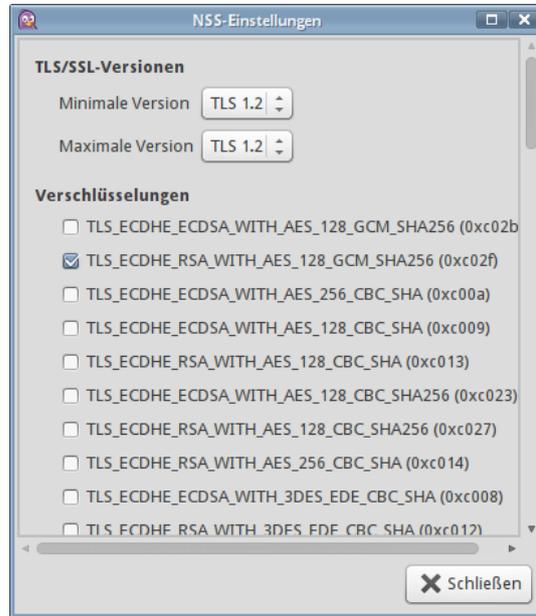


Abbildung 11.17: TLS Cipher für Pidgin konfigurieren

- Pidgin kann eine zentrale Proxy Konfiguration für alle Accounts verwalten oder individuelle proxy Konfigurationen für jeden Account einzeln.

**Tor:** Um das TorBrowserBundle als Anonymisierungsdienst zu verwenden, wählt man in der Proxy Konfiguration den Proxy-Typ *Tor/Privatsphäre*, als Host *127.0.0.1* und als Port *9150*. (Bild [11.18](#))

**JonDo:** Um JonDo als Anonymisierungsdienst zu verwenden, wählt man in der Proxy Konfiguration den Proxy-Typ *HTTP*, als Host *127.0.0.1* und als Port *4001*. Außerdem muss(!) man die IP-Adresse des Jabber Servers auf dem Reiter *Erweitert* als *Verbindungsserver* angeben, um die DNS-Leaks mit HTTP-Proxys wie JonDo zu vermeiden. Die IP-Adresse kann auf der Webseite [DNS Resolve von JonDo](#) ermittelt werden.

## 11.8 Anonymes Instant-Messaging mit TorChat

TorChat ist ein Instant-Messaging Client mit einem genialen Konzept. Jeder Account ist ein Tor Hidden Service. Die Kommunikation erfolgt direkt zwischen den Beteiligten, es gibt keinen Serverdienst wie bei Jabber (XMPP) oder anderen Instant-Messaging Varianten. Die Verschlüsselung wird durch Tor sichergestellt. Außerdem kann ein externer Beobachter nicht erkennen, welche



Abbildung 11.18: Proxy Konfiguration eines Pidgin Accounts für Tor

Art der Kommunikation abläuft.

Die Projektwebseite<sup>24</sup> stellt Installationspakete für Windows und Debian basierte Linux Distributionen zum Download bereit. Außerdem kann man die Sourcen nutzen.

**Windows:** Das ZIP-Archiv ist nach dem Download zu entpacken - fertig. Im Verzeichnis *bin* findet man die Datei *torchat.exe*. Ein Doppelklick auf die Datei startet alles Nötige. Zur Vereinfachung des Starts kann man eine Verknüpfung erstellen und auf den Desktop ziehen.

**Debian, Ubuntu, Mint:** Vor der Installation sind die Abhängigkeiten zu installieren. TorChat benötigt *Tor*, *Python-2.x* und die GUI-Bibliothek *WxGTK für Python*:

```
> sudo aptitude install tor python-wxgtk2.8
```

Anschließend installiert man das DEB-Paket mit dem bevorzugten GUI-Tool (Ubuntu Software Center, KPackage, Gdebi...) oder auf der Kommandozeile mit:

```
> sudo dpkg -i torchat-*.deb
```

**Sourcen:** Für alle Nicht-Debian Linuxe und UNIXe kann man das Source-Paket nutzen. Auch hier benötigt man *Tor*, *Python-2.x* sowie *WxGTK für Python*. Nach der Installation der nötigen Bibliotheken und dem Entpacken der Sourcen startet man TorChat in dem *src*-Verzeichnis:

<sup>24</sup> <https://github.com/prof7bit/TorChat/downloads>

```
> python torchat.py
```

Beim Start von TorChat wird eine Instanz von Tor mit den passenden Parametern gestartet. Ein Account wird automatisch erstellt, wenn noch nicht vorhanden. Dann dauert es 15-20 min bis der Account bekannt wird.

Die Bedienung ist einfach. Man klickt mit der rechten Maustaste in das Hauptfenster und fügt eine TorChat-ID hinzu. Wenn das Symbol farbig dargestellt wird, kann man eine Nachricht schreiben oder eine Datei senden. Farblos dargestellt Accounts sind nicht online. Eine TorChat-ID ist eine kryptische Tor Hidden Service Adresse ohne die Endung *.onion*.

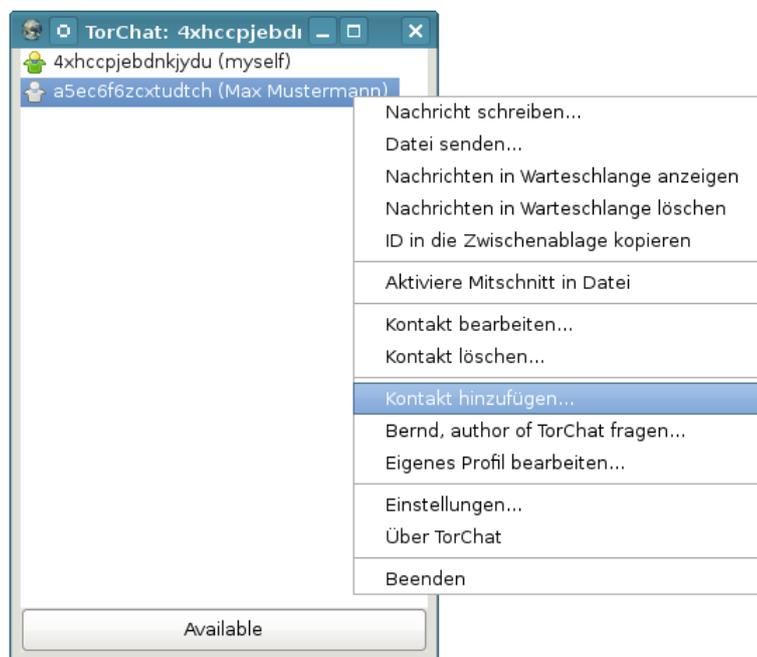


Abbildung 11.19: TorChat Hauptfenster

**WICHTIG:** TorChat ist immer über den Menüpunkt *Beenden* zu schließen. Nur dann wird auch die gestartete Instanz von Tor sauber beendet.

## 11.9 Anonymes Filesharing

Mit der Verbreitung von Three-Strikes-Regelungen bei Urheberrechtsverletzungen in einigen Ländern wie Frankreich, Großbritannien, Irland und bei den ACTA-Verhandlungen wächst der Bedarf für anonymes Filesharing.

### 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 ist <sup>25</sup>.

### Anonymes Filesharing

1-Click-Hoster sind die einfachste Variante. Mit einem Webbrowser kann man anonym via Tor oder JonDonym Daten 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):
  - <http://www.senduit.com>
  - <http://www.wikisend.com> (Passwortschutz möglich)
  - <http://www.turboupload.com> (Löschen der Uploads möglich)
  - <http://www.filefactory.com> (benötigt Javascript)
  - <http://www.share-now.net>
- Für Langzeit-Hosting kann man folgende Dienste verwenden:
  - <http://www.mediafire.com> (Registrierung für Uploads nötig)
  - <http://ompldr.org> (benötigt Cookies für Uploads)

### 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 <http://gnunet.org>.
- **StealthNet:** ist ebenfalls ein anonymes, dezentrales Filesharing Netzwerk. Die aktuelle Client-Software benötigt ein .Net 2.0 Framework. Anleitungen und Downloads gibt es auf der Projektwebsite <http://www.stealthnet.de/>.

<sup>25</sup> <https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea>

- **Anomos:** ist ein relativ junges Projekt. Es kombiniert das BitTorrent Protokoll mit einem Tor-ähnlichem Layer für End-to-End Verschlüsselung und Anonymisierung. Es können normale Torrent-Dateien genutzt werden, die jedoch auf einem Anonos-Tracker bekannt sein müssen. Download und Informationen auf der Projektwebsite <http://anomos.info>.

## 11.10 POND - die bessere E-Mail

POND<sup>26</sup> bietet die Möglichkeit, asynchron Textnachrichten mit Dateianhängen unbeobachtet auszutauschen. Die Kommunikation verläuft ähnlich wie bei E-Mail. Im Gegensatz zu E-Mail bietet POND echte *zero knowledge privacy* und hat folgende Vorteile:

- Der Inhalt der Nachrichten wird mit starker Kryptografie Ende-zu-Ende verschlüsselt. Es wird die von Jabber/XMPP bekannte OTR-Verschlüsselung genutzt.
- Dritte können keine Informationen über Metadaten (Sender, Empfänger) sammeln.
- Auch die beteiligten Server können keine Informationen über Absender und Empfänger auswerten und somit keine Kommunikationsprofile erstellen.
- Die gesamte Kommunikation wird über Tor Hidden Server abgewickelt und ist somit durch Dritte nicht beobachtbar.
- Um Spam zu verhindern, kann man im Gegensatz zu E-Mail keine Nachrichten unaufgefordert an eine bekannte POND-Adresse senden. Beide Kommunikationspartner müssen sich gegenseitig autorisieren, um via POND kommunizieren zu können.
- Nachrichten werden nach 7 Tagen gelöscht. (Digitale Vergesslichkeit)

Das Projekt ist noch in einem frühen Entwicklungsstadium. Das zeigt sich vor allem in den Schwierigkeiten bei der Installation. Außerdem wurde der Source Code bisher nicht durch unabhängige Dritte evaluiert. Im Gegensatz zu BitMessage u.ä. Hypes ist das Konzept von POND aber überzeugend, skaliert für große Nutzerzahlen und ist konsequent umgesetzt. Wenn die Implementierung keine schweren Fehler enthält, ist POND meiner Meinung nach eines der wenigen Tools, die NSA-safe sind.

Wenn die Installation zu kompliziert ist oder kein Linux zur Verfügung steht, kann man die JonDo Live-DVD nutzen, die die Command Line Version (CLI) von POND enthält.

### Installation (Linux)

Voraussetzungen für die Installation:

---

<sup>26</sup> <https://pond.imperialviolet.org/0>

- Da POND die Tor Hidden Services nutzt, braucht man einen Tor Daemon. Man kann das TorBrowserBundle nutzen oder einen Tor Daemon extra installieren. Unter Debian und Ubuntu kann man Tor und das GUI Vidalia aus den repositories installieren:

```
> sudo aptitude install tor vidalia
```

- POND nutzt die relativ neue Programmiersprache Go, die nötigen Tools für diese Programmiersprache und GitHub muss man ebenfalls installieren. Für den grafischen Client von POND (GUI, für Mausschubser) benötigt man Go Version 1.2. Die Command Line Version von POND (CLI) kann auch mit Go Version 1.0 genutzt werden.

```
> sudo aptitude install golang mercurial
```

- Außerdem benötigt POND GUI einige GTK3 Bibliotheken, die nur in aktuellen Distributionen wie Ubuntu ab 13.10 und Debian 8.0 jessie enthalten sind.

```
> sudo aptitude install libgtk-3-dev libgtkspell3-3-dev
```

- In älteren Distributionen wie Debain 7.x wheezy (stable) ist nur POND CLI installierbar. Diese Version benötigt den Editor vim, der ebenfalls mit aptitude installiert werden kann:

```
> sudo aptitude install vim
```

- POND bietet die Möglichkeit, den Master-Key für die Verschlüsselung der Daten im TPM NVRAM des Rechners zu speichern. Damit wird ein zuverlässiges Überschreiben des Master-Key sichergestellt, was bei aktuellen Dateisystemen und SSD-Festplatten nicht immer gewährleistet ist. Die nötigen Bibliotheken sind ebenfalls nur in aktuellen Linux Distributionen enthalten, die Installation ist optional.

```
> sudo aptitude install libtspi-dev trousers
```

Unter Ubuntu 13.10 und neuer sowie Debian jessie kann POND im Terminal mit folgenden Kommandos installiert werden:

```
> cd $HOME
> mkdir gopkg
> export GOPATH=$HOME/gopkg
> go get github.com/agl/pond/client
```

Wenn man nur die CLI Version installieren möchte (z.B. für Debian 7.x wheezy), dann ist das letzte Kommando durch folgende Zeile zu ersetzen:

```
> go get -tags nogui github.com/agl/pond/client
```

Nach der Installation kann man den POND Client mit folgendem Befehl im Terminal starten oder man richtet einen Programmstarter auf dem Desktop oder im Startmenü ein:

```
> $HOME/gopkg/bin/client
```

### POND (grafisches Interface)

Da POND die Tor Hidden Services nutzt, ist zuerst Tor zu starten (via Vidalia). Beim Start mit einer neuen Konfiguration wird automatisch eine neue Identität erstellt. Nach der Eingabe der Passphrase kann man einen POND-Server wählen. Wenn man keinen eigenen POND-Server als Tor Hidden Service betreibt, kann man den Standard übernehmen.

Um mit anderen Nutzern via POND zu kommunizieren, muss ein gegenseitige Authorisierung und ein Austausch der Schlüssel erfolgen. Es ist im Unterschied zur E-Mail nicht möglich, einfach einem anderen Nutzer eine Nachricht zu senden. Die Schlüssel werden durch einen Diffie-Hellman Keyexchange generiert. Als Beispiel soll ein Kontakt zu Beatrice hergestellt werden (Bild: 11.20). Der <name> (im Beispiel: Beatrice) kann frei gewählt werden, er ermöglicht nur eine Zuordnung im eigenen Adressbuch und hat keine Bedeutung als Adresse. Intern erfolgt die Adressierung von Absender und Empfänger über Kryptoschlüssel.

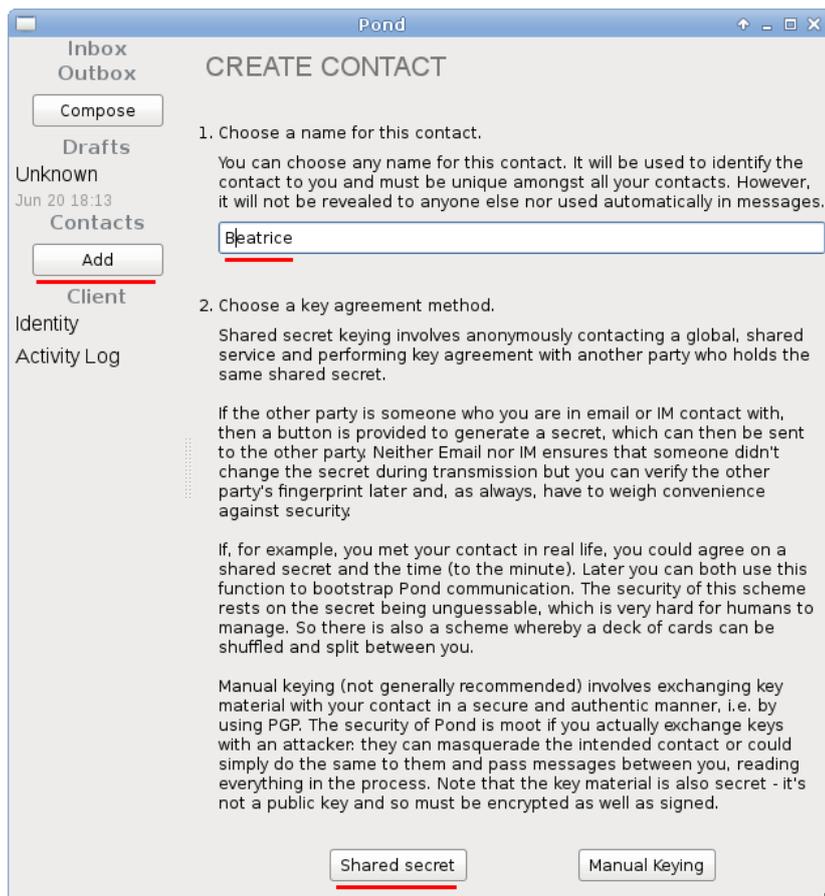


Abbildung 11.20: POND - neuen Kontakt erstellen

Wenn man die empfohlene Option *Shared secret* für den Schlüsseltausch wählt, kann man eine zufällige Passphrase automatisch generieren lassen. Diese Passphrase ist via verschlüsselter E-Mail, Jabber (OTR-verschlüsselt) oder irgendwie anders an den Kommunikationspartner zu senden, der ebenfalls einen neuen Kontakt erstellt und exakt die gleiche Passphrase eingibt. Wenn beide Partner online sind (nicht zwingend notwendig), dauert die gegenseitige Authorisierung und Aushandlung der Krypto-Schlüssel nur eine Minute.

Alternative könnte man bei einem persönlichen Treffen eine individuelle Passphrase austauschen (mit Zeitstempel!) und beide Partner nutzen diese Passphrase für den Keyexchange.

Der Editor der GUI Version (Bild: 11.21) ist wesentlich intuitiver bedienbar, als der Editor *vim* im Comand Line Interface (CLI).

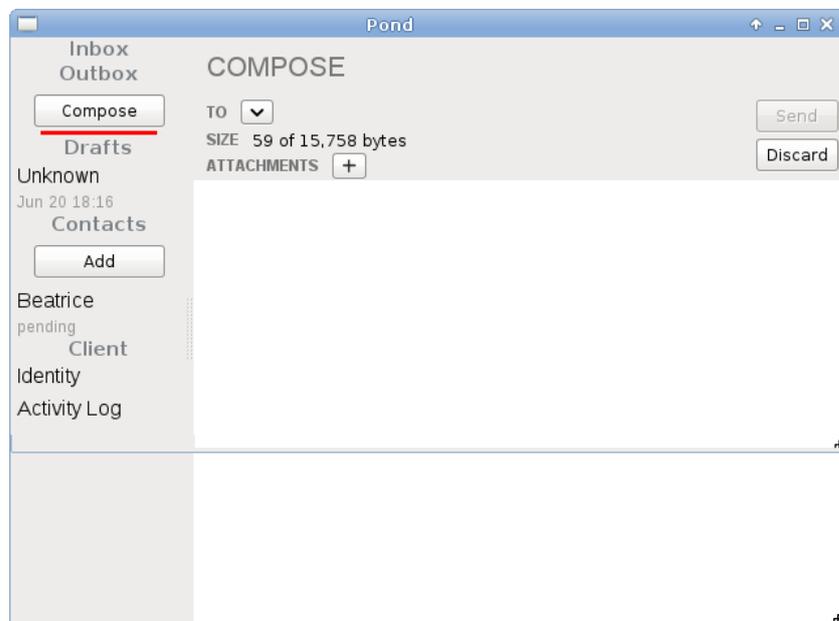


Abbildung 11.21: POND - neue Nachricht erstellen

**Wichtig:** Wenn man im Editor auf *Send* klickt, dann wird die Nachricht in den Postausgang verschoben aber nicht sofort an den den Server des Empfängers versendet. Im Postausgang oder im Activity Log muss man den Button *Transact now* wählen, um die Nachricht wirklich zu versenden.

## 11.11 proxychains für Linux

Für Linux gibt es viele kleine Kommandozeilentools, die irgendwie eine Verbindung ins Internet herstellen (z.B. *ssh*, *scp*, *danetool* oder *wget*), die man in Scripten nutzen kann. Einige Tools können einen Proxy nutzen, andere

muss man dazu zwingen.

Eine generische Lösung, die mit allen Tools funktioniert, bietet *proxychains*. Als erstes ist das Tool mit dem bevorzugten Paketmanager zu installieren:

```
> sudo aptitude install proxychains
```

Dann erstellt man in `$HOME/.proxychains/proxychains.conf` eine eigene Proxy Konfiguration. Mit folgender Konfiguration nutzt man JonDonym:

```
strict_chain
proxy_dns
[ProxyList]
http 127.0.0.1 4001
```

Das TorBrowserBundle kann man mit folgender Konfiguration zur Anonymisierung verwenden:

```
strict_chain
proxy_dns
[ProxyList]
socks5 127.0.0.1 9150
```

Standardmäßig nutzt *proxychains* den Server 4.2.2.2 für die DNS Auflösung. Der Server unterstützt kein DNSSEC und man sollte ihn durch einen zensurfreien DNS Server mit DNSSEC ersetzen. Eine Liste von empfohlenen, unzensurierter DNS-Server mit Support für DNSSEC findet man im allgm. Kapitel *Betriebssysteme*:

- Censurfridns Denmark (91.239.100.100 und 89.233.43.71)
- DNS WATCH (84.200.69.80 und 84.200.70.40)
- Xiala.net (77.109.148.136 und 77.109.148.137)

Den DNS Server für *proxychains* kann man in der Datei `/usr/lib/proxychains3/proxyresolv` (Debian, Ubuntu) oder `/usr/bin/proxyresolv` (SuSE, Redhat) anpassen, indem man den Eintrag für `DNS_SERVER` ändert:

```
DNS_SERVER=91.239.100.100
```

Dann kann man *proxychains* zur Anonymisierung von beliebigen Programmen nutzen:

```
> proxychains ssh user@server.tld (anonyme Server Administration)
> proxychains danetool --check .... (SSL Zertifikate validieren)
> proxychains wget https://server.tld/datei (anonyme Downloads)
```

## 11.12 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.

### 11.12.1 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)*

### 11.12.2 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       |

Einige Webproxys erlauben es, Javascript mit dem Aktivieren einer Option auf der Startseite zu blockieren. Es ist zwingend notwendig, diese Option zu aktivieren, da alle Webproxys mit Javascript ausgetrickst werden können! Außerdem sollte man Javascript im Browser deaktivieren, damit keine Scripte in Bildern, Werbebannern o.ä. durch den Proxy geschmuggelt werden können.

### CTunnel.com

[CTunnel.com](#) ist ein ganz besonderer Web-Proxy, der hier etwas ausführlicher behandelt werden soll. Man verspricht zwar eine anonyme Nutzung des Internet. Die Entwickler haben sich aber große Mühe gegeben, die Nutzung des Dienstes mit deaktiviertem Javascript unmöglich zu machen. Der gesamte Inhalt der Website ist encoded und wird mit Javascript geschrieben.

Die IP-Adressen der Nutzer werden bei aktiviertem Javascript gleich an drei Datensammler verschickt. Neben Google Analytics erhalten auch [xtendmedia.com](#) und [yieldmanager.com](#) diese Information. Google Analytics ist bekannt, die beiden anderen Datensammler sind ebenfalls Anbieter von Werbung. Die Website enthält keinen Hinweis auf die Datenweitergabe. Zumindest im Fall von Google Analytics besteht jedoch eine Informationspflicht.

Die Ereignisse rund um den [Sahra-Palin-Hack](#) zeigen, dass auch der Dienst selbst Informationen über die Nutzer speichert. Die Kommunikationsdaten werden selbst bei kleinen Vergehen an Behörden weitergegeben. Eine seltsame Auffassung von Anonymität.

#### 11.12.3 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 Datensammlern und anderen Gefahren geschützt. Die Free-Version der Software verbindet Sie nach einem Klick auf die Schaltfläche Hide IP mit einem amerikanischen Proxy-Server und vergibt eine neue IP-Adresse für Ihren Rechner.*

Der Dienst erfüllt nicht einmal einfachste Anforderungen. Nutzer können in mehreren Varianten deanonymisiert werden - beispielsweise ganz einfach mit (verborgenen) HTTPS-Links.

Als Tool zur Umgehung von Zensur ist der Dienst auch nicht geeignet. Die amerikanischen Proxy-Server setzen das Filtersystem *Barracuda* ein und es werden die Internetsperren des COICA-Zensurgesetzes umgesetzt.

#### 11.12.4 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.

Die kostenfreie Version hat Jens Kubiziel schon 2014 getestet. Das Ergebnis kann man einfach zusammenfassen: es funktioniert nicht zuverlässig. Insbesondere wenn man ZenMate zur Umgehung regionaler IP-Sperren

verwenden möchte, um Videos zu schauen, die im eigenen Land nicht verfügbar sind, funktioniert die IP-Anonymisierung NICHT.<sup>27</sup>

|                   |  |
|-------------------|--|
| Your IP           | 103.10.107.58<br>88.130.140.38 [Flash] |
| Your location     | Germany undefined                      |
| Your net provider | Versatel Deutschland                   |
| Reverse DNS       | i58828C26.versanet.de                  |

Abbildung 11.22: ZenMate IP-Leak via Flash

Ich habe mir die Premium Version angeschaut:

- Die Registrierung und später der Login in den Premium Dienst erfordern die Angabe einer E-Mail Adresse, was eindeutig ein identifizierendes Merkmal ist. Das gesamte anonymisierte Surfverhalten von Premium Kunden könnte ZenMate eindeutig dem Inhaber einer E-Mail Adresse zugeordnet. Vielleicht protokolliert ZenMate wirklich nichts, technisch wäre es aber einfach möglich.
- Die nächste Überraschung war die Verschmutzung der E-Mails zur Zahlungsbestätigung mit Tracking Wanzen. Wenn man die E-Mails von ZenMate genauer untersucht, findet man ein kleines, nicht sichtbares Bildchen, welches mit einer individuellen URL von einem ZenMate Tracking Server geladen wird.

```

```

ZenMate versucht also, die Empfänger der E-Mails zu verfolgen und jedes Öffnen der Mails soll registriert werden. In der Privacy Policy<sup>28</sup> von ZenMate wird dieses E-Mail Tracking nicht erwähnt.

- Das versprochene Blockieren von Third Party Tracking in der Premium Version funktioniert ebenfalls nicht. Cookies und moderne HTML5 Tracking Features von Drittsiten werden nicht zuverlässig blockiert, wenn man den Tracking Schutz aktiviert.

Schlussfolgerung: Das ist nur Abzocke mit zweifelhafter Werbung.

### 11.12.5 5socks.net

Im Forum der GPF tauchte vor einiger Zeit die Frage auf, was wir von *5socks.net* halten. *5socks.net* ist ein Provider, der die Nutzung von SOCKS-Proxies im Abbo anbietet.

Eine kurze Recherche brachte folgende Ergebnisse:

<sup>27</sup> <https://kubieziel.de/blog/archives/1582-ZenMate-als-Anonymisierungsprogramm.html>

<sup>28</sup> <https://zenmate.com/privacy-policy/>

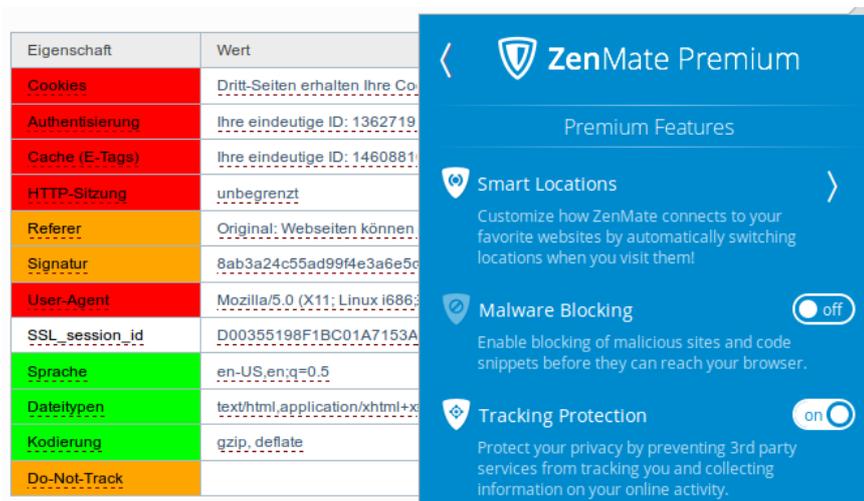


Abbildung 11.23: Tracking Protection in ZenMate funktioniert nicht

## 1. Fragen wir mal nach 5.socks.net:

```
domain: 5socks.net
IPv4-adress: 174.36.202.143
addr-out: s3d.reserver.ru
whois.nic.mil [0] Undefined error: 0
```

```
OrgName: SoftLayer Technologies Inc.
OrgID: SOFTL
Address: 1950 N Stemmons Freeway
City: Dallas
StateProv: TX
PostalCode: 75207
Country: US
```

2. Softlayer Technologies Inc. == Layered Technologies  
<http://seo-mannsgarn.de/proxy-ip-vandalismus.htm>

## 3. Zu dieser Firma findet man bei cryptome.info:

```
Layered Technologies Incorporated
[NSA-affiliated IP range]
Frisco TX US
72.232.0.0 - 72.233.127.255
ns2.layeredtech.com [72.232.210.195]
ns1.layeredtech.com [72.232.23.195]
```

Keiner möchte einen NSA-affiliated Anonymisierungsserver nutzen - oder?

### 11.12.6 BlackBelt Privacy, Cloakfish und JanusVM

Tor Onion Router ist ein populärer Anonymisierungsdienst. Der Hauptnachteil ist die geringe Geschwindigkeit. Die Entwickler von TorProject.org sind sich dieses Problems bewusst und sie arbeiten daran, die Geschwindigkeit ohne Einbußen bei der versprochenen Anonymität zu erhöhen. Daneben gibt es immer wieder ein paar Scharlatane, die mit Voodoo-Methoden eine höhere Geschwindigkeit versprechen. Ich rate davon ab, diese Projekte zu nutzen.

**Tor BlackBelt Privacy** verspricht durch ein bisschen Voodoo in der Konfiguration eine Erhöhung der Geschwindigkeit bei der Nutzung von Tor. Eine Analyse der Änderungen an der Konfiguration durch Tor Entwickler kommt zu dem Schluss, dass minimale Verbesserungen bei der Geschwindigkeit möglich sein könnten. Allerdings verursachen die Modifikationen eine starke Erhöhung der Belastung des Tor Netzwerkes und sie vereinfachen Angriffe zur Reduzierung der Anonymität, wie sie auf der Defcon17 vorgestellt wurden.

Der Maintainer von BlackBelt Privacy versichert, dass die originale Software von Tor und Vidalia ohne Modifikationen am Code genutzt wird. Das kann nicht überprüft werden, da das Projekt nur Binaries für WINDOWS bereitstellt. Die Bereitstellung der *tollen torrc* würde für alle Betriebssysteme ausreichen oder wäre als Ergänzung sinnvoll. Suspect.

**Cloakfish** ist ein Projekt, welches kommerziellen Zugriff auf das kostenfrei zugängliche Tor-Netz bieten möchte. Eine Client-Software, die als Closed-Source zum Download bereitsteht, soll vor allem SEOs ermöglichen, sich über die Tor-Exit-Nodes mit vielen verschiedenen IP-Adressen im Web zu bewegen. (laut Eigen-Werbung bis zu 15.000 verschiedenen Adressen pro Monat)

Durch die Verwendung von nur einem Tor-Node wird die Anonymität der Nutzer stark eingeschränkt und nicht die nächste Stufe der Anonymität erreicht, wie ein schnell aufgezoogenes Werbe-Blog suggerieren möchte.

Die Tor-Entwickler missbilligen diese Nutzung des Tor-Netzwerkes, da die Load-Balancing Algorithmen von Tor durch diese Software gestört werden. Entgegen der Behauptung auf der Projekt-Webseite sind die Entwickler von Cloakfish den Tor Developern unbekannt.

Diskussionen zu Cloakfish und verunglückte Beispiele von Postings, die unter falschem Pseudonym Werbung für die Software machen wollen, findet man bei gulli, im Forum der GPF und im Forum von JonDonym. Die Software wird bei den Black SEO intensiv beworben.

**JanusVM** ist eine VMware Appliance für anonymes Surfen. Die Appliance soll mit openVPN, Tor, Privoxy usw. eine schlüsselfertige Lösung bieten. Roger Dingledine von TorProject.org kommentierte die JanusVM im Dezember 2011 auf der OR-Talk Liste mit folgenden Worten:

*“Probably has been unsafe to use for years.”*

### 11.12.7 Proxy-Listen

In der Anfangszeit des Internets nutzten Cypherpunks die Möglichkeit, ihre IP-Adresse mit mehreren Proxies zu verschleiern. Der Datenverkehr wird über ständig wechselnde Proxies geleitet, so dass der Webserver ständig eine andere IP-Adresse sieht. Es gibt Tools, die diesen Vorgang automatisieren.

Der Vorteil liegt in der im Vergleich zu Mixkaskaden und Onion-Routern höheren Geschwindigkeit. Der offensichtliche Nachteil ist, dass der Datenverkehr zwischen eigenem Rechner und den Proxies meist unverschlüsselt ist.

Inzwischen ist diese Idee häufig pervertiert worden. Im Internet kursierende Proxylisten sind alles andere als anonym. So wurde beispielsweise im Mai 2007 in der Newsgruppe *alt.privacy.anon-server* eine Liste gepostet, die mit verschiedenen DNS-Namen für Proxies gut gefüllt war. Eine Überprüfung der Liste ergab, dass hinter allen die gleiche IP-Adresse und somit derselbe Server steckt. Der Betreiber des Servers erhält eine website-übergreifende Zusammenfassung des Surfverhaltens der Nutzer!

## 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.

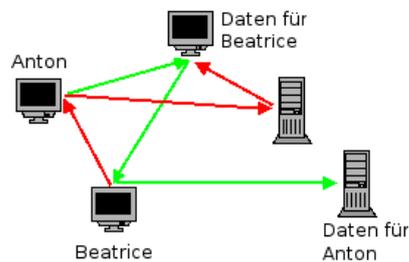


Abbildung 12.1: Prinzip von anonymen Peer-2-Peer Netzen

Hauptverwendungszweck für anonyme Peer-2-Peer Netze ist unbestritten das abmahnsichere 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 Ange-

bote sind nicht lokalisierbar. Wie im normalen Internet sind die meisten Angebote 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 globaler Überwachung ist das Ziel des Projektes. Es stellt die höchsten Anforderungen an die Nutzer und erzielt die langsamsten Downloadraten.

Im Unterschied zu I2P werden die Inhalte im Freenet redundant über alle Peers 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 der Freenet-Knoten bereitstellt.

Unabhängig vom *Open Freenet* kann man mit vertrauenswürdigen Freunden ein eigenes Netz konfigurieren, welches sich vollständig der Beobachtung durch Dritte entzieht.

## 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 *eep-sites*) 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.com](http://www.java.com)<sup>1</sup>. Der Installer möchte unbedingt die *Ask-Toolbar* für alle Browser installieren. Das sollte man deaktivieren, braucht man nicht.

**WICHTIG:** Der Installer aktiviert auch ein Java-Plugin für alle Browser. Dieses Plug-in ist ein Sicherheitsrisiko und muss im Java Control Panel unter *Systemsteuerung - Programme - Java* deaktiviert werden!



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).

<sup>1</sup> <http://www.java.com/de/>

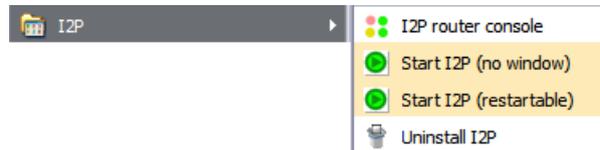


Abbildung 12.2: I2P im Startmenü von Windows

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:** Für Ubuntu kann man das offizielle PPA Repository der I2P Maintainer nutzen. Dieses Repository enthält nur den I2P-Router. Es wird mit folgenden Kommandos aktiviert und danach der I2P-Router installiert:

```
> sudo apt-add-repository ppa:i2p-maintainers/i2p
> sudo apt-get update
> sudo aptitude install i2p
```

**Debian:** Auch für Debian 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 unter der URL [https://geti2p.net/\\_static/debian-repo.pub](https://geti2p.net/_static/debian-repo.pub) herunterzuladen und in den Apt-Keyring einzufügen mit:

```
> wget https://geti2p.net/_static/debian-repo.pub
> sudo apt-key add debian-repo.pub
```

Danach kann man I2P und auch das Paket *i2p-keyring* für spätere Updates des Signaturschlüssels installieren:

```
> sudo apt-get install i2p i2p-keyring
```

**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 Download 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 Ap-pArmor 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 Netzwerkkonfiguration 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)

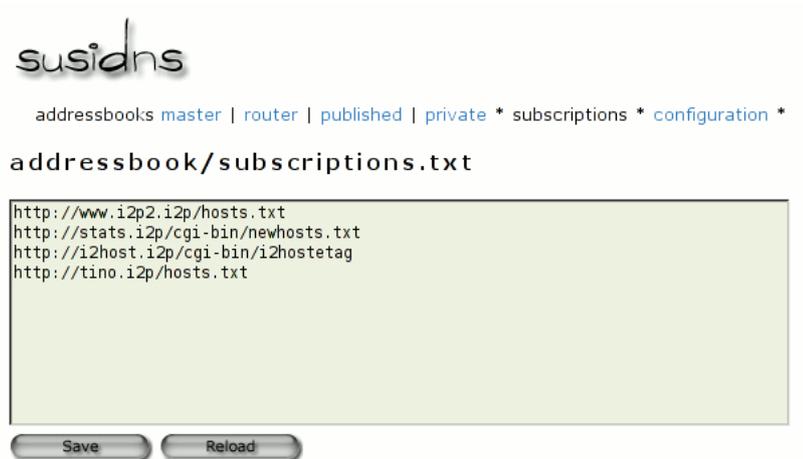


Abbildung 12.3: subscriptions für SusiDNS

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
```

### 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.



Abbildung 12.4: Benutzerdefinierte Proxy Konfiguration im JonDoFox

### 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.



Abbildung 12.5: Firefox Profil-Manager

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.

### 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:



Abbildung 12.6: Firefox Proxy-Einstellungen für I2P

```
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
```

### Suchmaschinen für I2P

Um sich in einem Netzwerk zu orientieren, braucht man eine Suchmaschine. Die Webseite [plugins.i2p](http://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>.

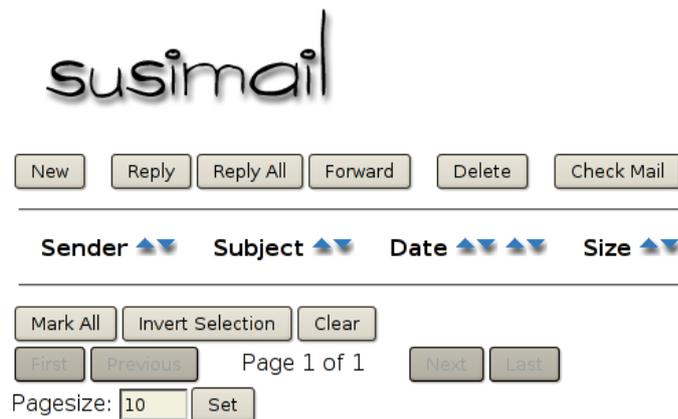


Abbildung 12.7: Webinterface von Susimail

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.
- 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](http://sponge.i2p/files/seedless/01_neodatis.xpi2p)
2. [http://sponge.i2p/files/seedless/02\\_seedless.xpi2p](http://sponge.i2p/files/seedless/02_seedless.xpi2p)
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.



Abbildung 12.8: Installation des Plug-in I2P Bote

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".

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* und weitere Fragen beantworten bestimmt die FAQ von I2P Bote <sup>2</sup>.

### 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
```

<sup>2</sup> <http://i2pbote.net/faq.html>

### 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 smarterer 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 UPnP<sup>3</sup> 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.

<sup>3</sup> <http://heise.de/-1793625>

## Kapitel 13

# 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*, *EncFS* oder *ecryptfs*.
5. Wer eine **Manipulation der Systemdaten** befürchtet, kann seinen Rechner komplett verschlüsseln (z.B. mit *dm-crypt* für Linux).
6. **SDSRDDs** kann man nutzen, wenn Sicherheit absolute Priorität hat, Geld keine Rolle spielt und man sich nicht auf eine Softwarelösung verlassen möchte. SDSRDDs sind SSD Festplatten mit integrierter Verschlüsselung, Token-Authentifizierung (also nicht mit Keyloggern angreifbar) und eingebautem Mechanismus zur Selbstzerstörung, der remote via SMS oder bei unerlaubten Zugriff ausgelöst werden kann.

## 13.1 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 Orgnaldateien sind sicher(!) zu löschen, damit keine Spuren auf der Festplatte bleiben.

**EncFS, Boxcryptor** arbeiten Verzeichnis-basiert. Es werden zwei Verzeichnisse definiert. Das Verzeichnis A mit den verschlüsselten Daten wird auf den Datenträger geschrieben, ein zweites Verzeichnis B oder ein virtuelles Laufwerk bietet den transparenten Zugriff auf die entschlüsselten Daten. Das verschlüsselte Verzeichnis A kann auf externe Datenträger kopiert oder mit einem beliebigen Cloud-Speicher synchronisiert werden.

**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

Veracrypt<sup>1</sup> ist ein Nachfolger des legendären Truecrypt. Es beseitigt einige Schwäche, die bei einem Audit von Truecrypt<sup>2</sup> aufgedeckt wurden und wird nach Open Source Prinzipien weiterentwickelt. Mit Veracrypt neu erstellte Container sind nicht kompatibel mit dem alten Truecrypt Format und können nicht mit tccpplay (für Linux) geöffnet werden. Alte Truecrypt Container können aber mit Veracrypt geöffnet und weiter verwendet werden. Aus Sicherheitsgründen sollte man alle Daten in die neuen Veracrypt Container kopieren.

Ein Feature von Veracrypt und tccpplay 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.

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.

## 13.2 Gedanken zum Passwort

An Stelle von *Passwort* sollte man vielleicht die Bezeichnung *Passphrase* bevorzugen. Sie suggeriert, dass es auch ein wenig länger sein darf und dass Leerzeichen durchaus erlaubt sind.

Eine gute Passphrase sollte leicht merkbar aber schwer zu erraten sein. Außer Buchstaben sollte sie auch Zahlen und Sonderzeichen enthalten und etwa

<sup>1</sup> <https://veracrypt.codeplex.com>

<sup>2</sup> [https://opencrytaudit.org/reports/iSec\\_Final\\_Open\\_Crypto\\_Audit\\_Project\\_TrueCrypt\\_Security\\_Assessment.pdf](https://opencrytaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf)

20 Zeichen lang sein. So etwas schüttelt man nicht einfach aus dem Ärmel. Wie wäre es mit folgender Phrase:

das geht nur %mich% \_AN\_

Zusätzlich zur Passphrase können auch Keyfiles als Schlüssel genutzt werden. Damit ist es möglich, eine Zwei-Faktor-Authentifizierung aufzubauen: eine Passphrase, die man im Kopf hat, und ein Keyfile, welches man in der Hand hat. Ein Angreifer müsste beides erlangen.

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 grundsätzlich keine Passwörter herausgeben.
- Richten sich die Ermittlungen gegen Dritte, kann man die Herausgabe von Keys verweigern, wenn man sich auf das Recht zur Zeugnisverweigerung berufen oder glaubhaft(!) versichern kann, dass man sich damit selbst belasten würde. Im Zweifel sollte man einen Anwalt konsultieren.

In Großbritannien ist es bereits anders. Gemäß dem dort seit Oktober 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 die bösen Terroristen beschränkt ist, kann man bei Heise.de nachlesen. Es wurde als erstes gegen eine Gruppe von Tierschützern angewendet.<sup>3</sup>

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.<sup>4</sup>

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.

<sup>3</sup> <http://www.heise.de/newsticker/meldung/99313>

<sup>4</sup> <https://www.eff.org/wp/defending-privacy-us-border-guide-travelers-carrying-digital-devices>

- Der deutsche Betreiber eines illegalen Waffenhandels im Deep Web konnte bei der Festnahme mit dem Fuß das Stromkabel aus seinem batterie-losen Laptop reißen und die Verschlüsselung damit aktivieren. Das SEK hatte aber zweifellos den Auftrag, bei der Festnahme den Laptop im eingeschalteten Zustand sicherzustellen.<sup>5</sup>

---

<sup>5</sup> <http://motherboard.vice.com/de/read/bis-das-sek-kommt>

## 13.3 Quick and Dirty mit GnuPG

Eine Möglichkeit ist die Verschlüsselung einzelner Dateien mit GnuPG oder PGP. Einfach im bevorzugten Dateimanager mit der rechten Maustaste auf eine Datei klicken und den Menüpunkt *Datei verschlüsseln* wählen. 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* oder anderen Tools in ein Archiv und verschlüsselt dieses Archiv.

Wird die Option *Symmetrisch verschlüsseln* gewählt, erfolgt die Verschlüsselung nicht mit einem Schlüssel sondern nur mit einer Passphrase. Die Entschlüsselung erfordert dann ebenfalls nur die Angabe dieser Passphrase und keinen Key. Diese Variante wird für Backups empfohlen, die man auch nach einem Crash bei totalem Verlust aller Schlüssel wieder herstellen will.

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.

### 13.3.1 GnuPG für WINDOWS

Diese simple Verschlüsselung klappt allerdings unter WINDOWS nicht auf Anhieb. Es ist zuerst die nötige Software zu installieren. Folgende Varianten kann man probieren:

1. Das Programmpaket **gpg4win** enthält eine Erweiterung für den Windows Explorer, die zusätzliche Menüpunkte im Kontextmenü einer Datei bzw. Verzeichnisses einfügt.

Download: <http://www.gpg4win.org>

2. Für Nutzer, die es gern etwas einfacher und übersichtlicher mögen, gibt es die Tools **gpg4usb** <http://gpg4usb.cpunk.de> oder **Portable PGP** <http://ppgp.sourceforge.net> (eine Java-App). Diese kleinen Tools können Texte und Dateien ver- bzw. entschlüsseln und sind auch USB-tauglich. Sie können auf einem USB-Stick mitgenommen werden. Sie speichern die OpenPGP-Keys auf dem Stick und integrieren sich nicht in den Explorer.

## 13.4 EncFS für Windows, Linux, MacOS und BSD

EncFS gibt es für Windows, Linux, MacOS und BSD. Es werden beliebige Verzeichnisse verschlüsselt.

1. Das verschlüsselte Verzeichnis A wird auf den Datenträger geschrieben.
2. Via FUSE ist über ein Verzeichnis B transparenter Zugriff möglich.

Das verschlüsselte Verzeichnis A kann auf externe Datenträger kopiert oder mit einem Cloudspeicher synchronisiert werden. Das Verzeichnis B ist auf dem Datenträger nur als leeres Verzeichnis als Mountpoint für FUSE vorhanden.

Die Installation von EncFS ist einfach:

- Unter Windows kann man `encfs4win` installieren (nicht so einfach). Webseite: <http://members.ferrara.linux.it/freddy77/encfs.html>
- Unter MacOS kann man `encfs` mit dem Paketmanager Homebrew installieren:

```
> brew install encfs
```

- Unter Linux installiert man die Pakete `encfs` und `fuse` mit dem bevorzugten Paketmanager der Distribution. Anschließend müssen alle Nutzer, die EncFS nutzen dürfen, zur Gruppe `fuse` hinzugefügt werden:

```
> sudo addgroup <USERNAME> fuse
```

- Unter BSD installiert man `encfs` aus `pkgsrc` oder als binäres Paket aus den Ports.

Auf der Kommandozeile erstellt man ein neues verschlüsseltes Verzeichnis mit folgendem Kommando:

```
> encfs /home/<user>/encrypted /home/<user>/daten
The directory ".../encrypted" does not exist. Should it be created? (y,n) y
The directory ".../daten" does not exist. Should it be created? (y,n) y
Creating new encrypted volume.
Please choose from one of the following options:
enter "x" for expert configuration mode,
enter "p" for pre-configured paranoia mode,
anything else, or an empty line will select standard mode.
?> p
```

Paranoia configuration selected.

New Encfs Password:

Verify Encfs Password:

Die Verzeichnisse sind mit absoluten Pfaden anzugeben und werden bei Bedarf neu erstellt. Bei der Verschlüsselung kann man zwischen dem Standard-Mode und dem Paranoia-Mode wählen oder alle Parameter selbst

festlegen. Im Paranoia-Mode werden die Dateiinhalte mit AES256 verschlüsselt, die Dateinamen im IV chaining mode codiert und Hardlinks sind nicht möglich. Einige Programme, die mit Hardlinks arbeiten, funktionieren im Paranoia-Mode nicht. Aber das ist bei einfachen Datenverzeichnissen kein Problem.

Ein vorhandenes verschlüsseltes Verzeichnis wird mit dem gleichen Kommando geöffnet:

```
> encfs /home/<user>/encrypted /home/<user>/daten
EncFS Password:
```

In dem Verzeichnis `/home/<user>/daten` kann man ganz normal auf die Dateien zugreifen, die im Verzeichnis `/home/<user>/encrypted` verschlüsselt abgelegt werden. Die Dateinamen werden ebenfalls verschlüsselt. Im Beispiel wurden zwei TXT-Dateien erstellt:

```
> cd /home/<user>/daten
> ls
ersteDatei.txt zweiteDatei.txt

> cd /home/<user>/encrypted
> ls -a
.encfs5 KQPNmIM2Ed0GEoDZvIwzpg-h W2QXuoKGeeudTMEQ2xUWBTAa
```

Das Passwort für das verschlüsselte Verzeichnis kann mit dem Kommando `encfsctl` geändert werden:

```
> encfsctl passwd /home/<user>/encrypted
Enter current Encfs password
EncFS Password:
Enter new Encfs password
New Encfs Password:
Verify Encfs Password:
Volume Key successfully updated.
```

Für Maus-Schubser gibt es mehrere kleine GUI-Tools, die die Arbeit mit EncFS vereinfachen. Unter Linux kann man z.B. `cryptkeeper` installieren. Wenn man `cryptkeeper` startet, findet man in der Taskleiste ein kleines Applet (Bild 13.1), das eine einfache Einrichtung eines neuen EncFS-Verzeichnis ermöglicht oder das Öffnen vorhandener EncFS-Verzeichnisse. Den Programm-Starter findet man in der Menügruppe *System*. `cryptkeeper` verwendet für das verschlüsselte Verzeichnis immer den gleichen Namen wie für das Daten-Verzeichnis, aber beginnend mit einem Punkt (verstecktes Verzeichnis).



Abbildung 13.1: cryptkeeper Taskbar Applet

## 13.5 dm-crypt für Linux

dm-crypt ist seit Version 2.6.4 fester Bestandteil des Linux-Kernels und somit in allen aktuellen Distributionen enthalten. Es nutzt den Device-Mapper. Folgende Software wird außerdem benötigt:

- Das Tool **cryptsetup** (mit LUKS-Support) kann zum Erstellen, Öffnen und Schließen der verschlüsselten Container eingesetzt werden. Aktuelle Distributionen enthalten es: Debian GNU/Linux im Paket *cryptsetup*, SuSE-Linux im Paket *util-linux-crypto*.

Einige Distributionen installieren das Tool unter dem Namen *cryptsetup-luks*. Die im Folgenden beschriebenen Befehle sind dann entsprechend anzupassen. Besser wäre es, einen Link zu erstellen. Dann funktionieren auch die Scripte *mount.crypt* und *umount.crypt* aus der Sammlung *pam-mount*.

```
# ln -s /usr/sbin/cryptsetup-luks /sbin/cryptsetup
```

- Das Paket **pmount** enthält einen Wrapper für das *mount*-Kommando, welcher automatisch verschlüsselte Laufwerke erkennt und vor dem Einbinden das Passwort abfragt. Aktuelle Debian-Distributionen verwenden es standardmäßig.
- Die Sammlung **pam-mount** enthält weitere Scripte, die das Öffnen und Schließen verschlüsselter Container vereinfachen. Die Scripte ermöglichen beispielsweise das Öffnen eines Containers automatisch beim Login. Unter Debian installiert man die Tools wie üblich mit

```
# aptitude install libpam-mount.
```

- Das Kernelmodul **dm\_crypt** muss vor der Verwendung der oben genannten Scripte geladen werden. In Abhängigkeit von der bevorzugten Distribution und der Installationsvariante wird das Modul bereits beim Booten geladen oder ist statisch in *initrd.img* eingebunden. Einfach probieren.

Sollte beim Erstellen oder Öffnen eines verschlüsselten Containers die folgende Fehlermeldung auftreten:

```
Command failed: Failed to setup dm-crypt key mapping.
Check kernel for support for the aes-cbc-essiv:sha256 cipher
```

ist das Kernel-Modul *dm\_crypt* zu laden:

```
# modprobe dm_crypt
```

Außerdem sollte das Modul in die Liste der beim Systemstart zu ladenden Module eingefügt werden. In der Datei */etc/modules* ist die Zeile *dm\_crypt* anzuhängen.

### 13.5.1 Bis zu 8 Passwörter mit LUKS

Die LUKS-Erweiterung von *cryptsetup* erlaubt es, bis zu 8 Passphrasen und Keyfiles zum Öffnen eines Containers zu nutzen. Damit ist es möglich, mehreren Nutzern den Zugriff mit einem eigenen Passwort zu erlauben.

Soll ein verschlüsselter Container mit dem Login eines Nutzers automatisch geöffnet werden, muss eines der 8 möglichen Passwörter mit dem Login-Passwort des Nutzers identisch sein. Login-Manager wie KDM oder GDM können das eingegebene Passwort an das *pam-mount* Modul weiterreichen. Dieses Feature kann beispielsweise für ein verschlüsseltes */home* Verzeichnis genutzt werden.

WICHTIG: bei Änderung des Login-Passwortes muss auch das Passwort für den Container geändert werden. Sie werden nicht automatisch synchronisiert.

### 13.5.2 Verschlüsselten Container erstellen

Alle folgenden Schritte sind als *root* auszuführen. Zum Aufwärmen soll zuerst die Partition */dev/hda4* verschlüsselt werden. Debian und Ubuntu enthalten das Skript `<em>luksformat</em>`, dass alle Aufgaben erledigt.

```
# luksformat -t ext3 /dev/hda4
```

Das ist alles. Der Vorgang dauert ein wenig und es wird 3x die Passphrase abgefragt. Ein Keyfile kann dieses Script nicht nutzen! Um einen USB-Stick komplett zu verschlüsseln, wählt man */dev/sdb1* oder */dev/sda1*. Es ist vor(!) Aufruf des Kommandos zu prüfen, unter welchem Device der Stick zur Verfügung steht.

#### Verschlüsselten Container erstellen für Genießer

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 -c aes-xts-plain64 -s 256 -h sha512
-y /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 luksOpen /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 luksClose <name>
```

8. Die Containerdatei wird ausgehängt:

```
# losetup -d /dev/loop0
```

### 13.5.3 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
```

### 13.5.4 Verschlüsselten Container öffnen/schließen

Aktuelle Linux Distributionen erkennen verschlüsselte Partitionen auf Festplatten und USB-Sticks automatisch und fragen die Passphrase ab, sobald das Gerät erkannt und im Dateimanager geöffnet wird. Einfach Anschließen, im Dateimanager öffnen und auf den Passwort-Dialog wie im Bild [13.2](#) warten.



Abbildung 13.2: Passwort-Abfrage für verschlüsselten USB-Stick

### Auf der Kommandozeile (mit Keyfile)

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>
```

### Containerdatei öffnen

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
```

### Truecrypt und Veracrypt Container öffnen

*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 [Optionen] open --type tcrypt /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.

### 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.

### 13.5.5 Debian GNU/Linux komplett verschlüsseln

In einem komplett verschlüsselten System sind sowohl die Daten als auch die Systemkonfiguration und Software verschlüsselt. Debian ab Version 4.0r1 (etch) bietet bereits beim Installieren die Option, ein komplett verschlüsseltes System unter Ausnutzung der gesamten Festplatte zu installieren. Lediglich für `/boot` bleibt ein kleiner unverschlüsselter Bereich.

Um diese einfache Variante zu nutzen, wählt man im Installations-Dialog *Festplatte partitionieren* die Option *Geführt - gesamte Platte mit verschlüsseltem LVM*. Im folgenden Schritt ist die Passphrase einzugeben, welche das System sichert. Diese Passphrase wird später bei jedem Bootvorgang abgefragt.

Partitionsmethode:

```
Geführt - verwende vollständige Festplatte
Geführt - gesamte Platte verwenden und LVM einrichten
> Geführt - gesamte Platte mit verschlüsseltem LVM
Manuell
```

Ein vollständig verschlüsseltes System macht es böswilligen Buben sehr schwer, bei einem *heimlichen Hausbesuch* die Software zu manipulieren und einen Trojaner zu installieren. Es ist jedoch nicht unmöglich. Wer noch einen Schritt weiter gehen will, erstellt nach der Installation eine bootfähige CD-ROM mit einer Kopie des sauberen Verzeichnis `/boot` und bootet in Zukunft immer von der CD. (Oder man geht zum Psychiater und lässt seine Paranoia behandeln.)

Man sollte nicht aus Zeitgründen auf ein Überschreiben der alten Daten mit Zufallszahlen verzichten. Um die Position verschlüsselter Daten auf der Platte zu verstecken und Daten der alten Installation zu vernichten, bietet

die Installationsroutine die Option, den Datenträger mit Zufallszahlen zu überschreiben. Das dauert zwar einige Zeit, ist aber ein sinnvolles Feature.

### 13.5.6 Ubuntu komplett verschlüsseln

Mit der Version Ubuntu 12.10. ist es nicht mehr nötig, die alternate desktop cd von Ubuntu zu nutzen. Auf Wunsch der EFF.org haben die Entwickler die Full Disc Encryption in den Installer der Desktop-Version integriert. Man kann bei einer **Neuinstallation** nach Auswahl der Sprache im zweiten Schritt die Komplettverschlüsselung der Festplatte aktivieren.

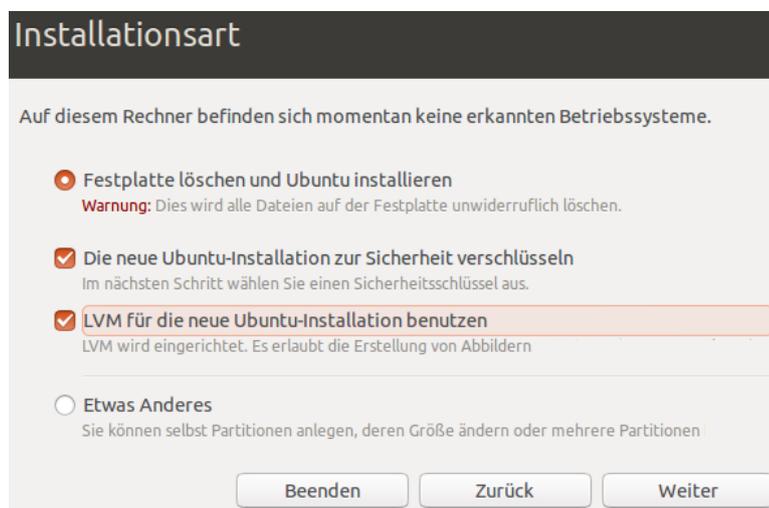


Abbildung 13.3: Full Disk Encryption bei der Installation von Ubuntu wählen

### 13.5.7 HOME-Verzeichnis verschlüsseln

Die Verschlüsselung der persönlichen Daten im \$HOME-Verzeichnis bieten alle Linux-Distributionen bei der Installation an. Wer keine Komplettverschlüsselung nutzen möchte, sollte zumindest diese Option aktivieren. Der Container mit den verschlüsselten Daten wird beim Login automatisch geöffnet. Die Nutzung ist vollständig transparent. Bei Verlust des Laptops sind die Daten jedoch geschützt.

### 13.5.8 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 defaults,size=256m 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
```

## 13.6 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.

### 13.6.1 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-random<sup>6</sup>.

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 öffnen<sup>7</sup>. Viele USB-Sticks mit Verschlüsselung verwenden zwar starke Algorithmen (in der Regel AES256), legen aber einen zweiten Schlüssel zur Sicherheit

<sup>6</sup> <http://true-random.com/homepage/projects/usbsticks/small.html>

<sup>7</sup> <http://heise.de/-270060>

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 eine saubere Implementierung, wie ein Artikel bei Heise<sup>8</sup> zeigt.

### Unison-GTK

Für die Synchronisation der Daten steht z.B. Unison-GTK<sup>9</sup> 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.



Abbildung 13.4: 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 13.4).

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.

**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.

<sup>8</sup> <http://heise.de/-894962>

<sup>9</sup> <http://www.cis.upenn.edu/~bcpierce/unison/>

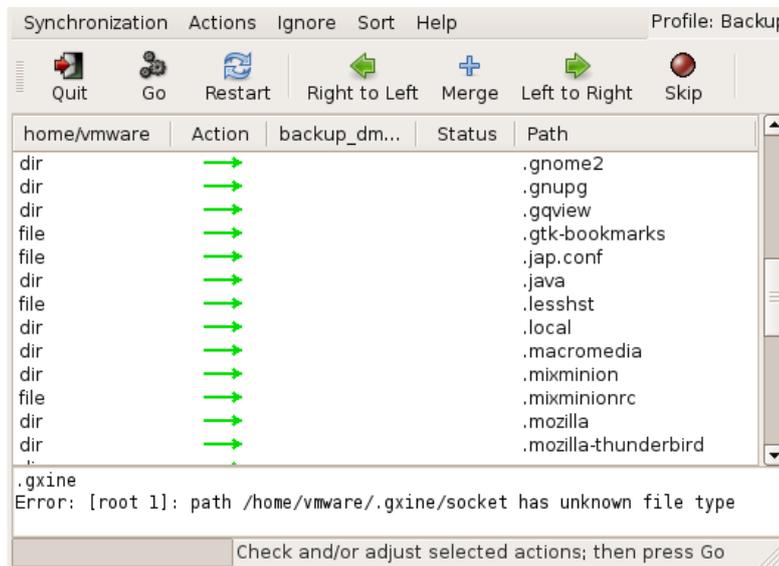


Abbildung 13.5: Hauptfenster von Unison-GTK

### rsync

Das Tool *rsync* ist in allen Linux-Distributionen enthalten und insbesondere für Scripte einfach verwendbar. Es synchronisiert die Dateien eines Zielverzeichnisses mit dem Quellverzeichnis und überträgt dabei nur die Änderungen. Ein Beispiel zeigt das Sichern der E-Mails und Adressbücher von Thunderbird:

```
rsync -av --delete $HOME/.thunderbird /backup_dir/.thunderbird
```

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 einem `-include` angegeben werden. Im Beispiel werden alle versteckten Verzeichnisse und Dateien mit gesichert.

Ein kleines Script, welches alle nötigen Verzeichnisse synchronisiert, ist schnell gestrickt. Eine backup-freundliche Struktur im `$HOME`-Verzeichnis erleichtert dies zusätzlich.

## Grsync

Grsync ist ein grafisches 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 13.6).

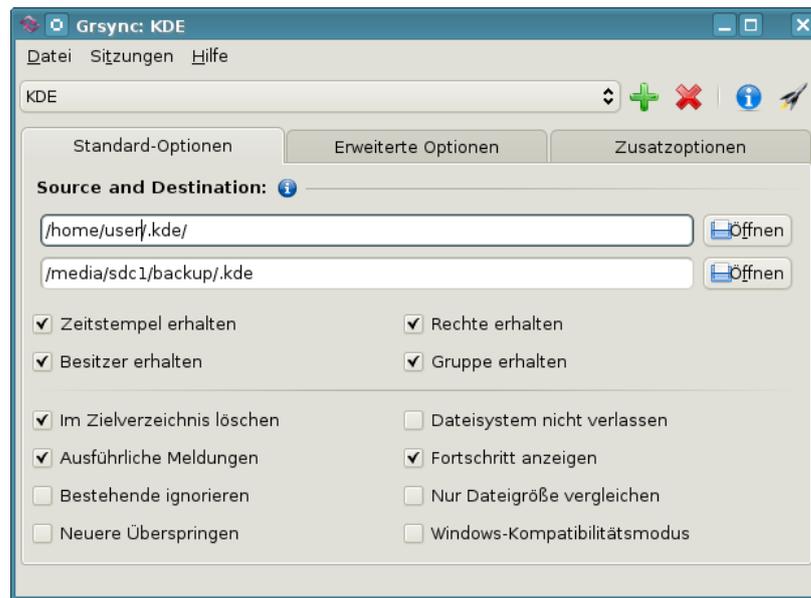


Abbildung 13.6: Hauptfenster von Grsync

### 13.6.2 Online Backups

Neben dem Backup auf einem externen Datenträger kann man auch Online-Speicher nutzen. Als Cloud-Provider kann ich Wuala empfehlen. Bei 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. Mit Ausnahme von Wuala muss man sich um die Verschlüsselung der Daten vor dem Upload 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”<sup>10</sup>. 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

<sup>10</sup> <http://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t>

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.

*Team-Drive* könnte als privacy-freundliche Cloud-Speicher genutzt werden. *duplicity* ist ein kleines Backuptool für Linux, das die Daten lokal ver- und entschlüsselt, bevor sie in einen beliebigen Cloud-Speicher hochgeladen werden. Für unverschlüsselte Cloud-Speicher kann man Verzeichnisse transparent mit EncFS oder Boxcryptor verschlüsseln.

### 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
```

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 Shellscript 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 14

## 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.

### 14.1 Dateien in den Papierkorb werfen

Unter WIN wird diese Variante als *Datei(en) löschen* bezeichnet, was etwas irreführend ist. Es wird überhaupt nichts beseitigt. Die Dateien werden in ein spezielles Verzeichnis verschoben. Sie können jederzeit wiederhergestellt werden. Das ist kein Bug, sondern ein Feature.

Auch beim Löschen der Dateien in dem speziellen Müll-Verzeichnis werden keine Inhalte beseitigt. Lediglich die von den Dateien belegten Bereiche auf dem Datenträger werden als "frei" gekennzeichnet. Falls sie nicht zufällig überschrieben werden, kann ein mittelmäßig begabter User 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.

### 14.2 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 shreddern können.

- Das GpgSX für Windows bietet als Erweiterung für den Explorer die Möglichkeit, Dateien und Verzeichnisse mit einem Mausklick sicher zu löschen: "Wipe..."
- Für WINDOWS gibt es AxCrypt (<http://www.axantum.com/AxCrypt>). Das kleine Tool zur Verschlüsselung und Löschung von Dateien inte-

griert sich in den Dateimanager und stellt 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.

### 14.3 Dateireste nachträglich beseitigen

Mit Bleachbit<sup>1</sup> 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 14.1). 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*.

<sup>1</sup> <http://bleachbit.sourceforge.net/download>

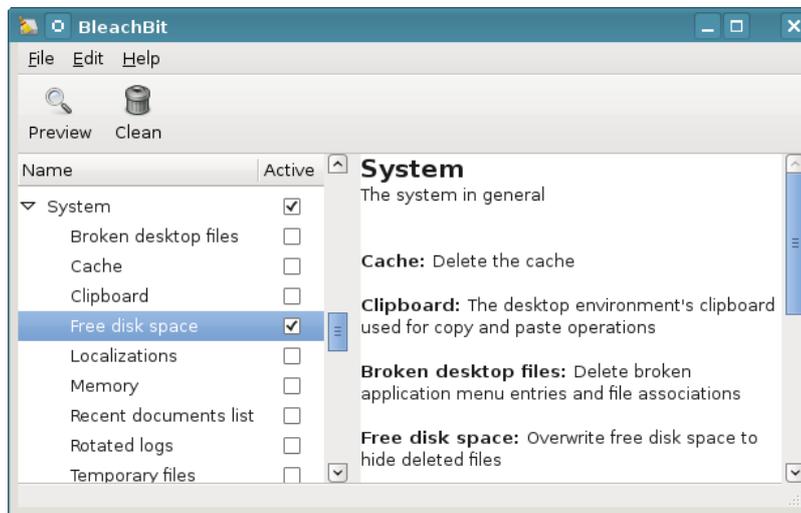


Abbildung 14.1: Bleachbit

Die Säuberung einer größeren Festplatte dauert einige Zeit. Dabei werden nur die als *frei* gekennzeichneten Bereiche überschrieben, das Dateisystem bleibt intakt.

## 14.4 Dateien sicher löschen (SSDs)

Alle oben genannten Tools für Festplatten funktionieren nicht mit Flash basierten Solid State Drives (SSD-Festplatten und USB-Sticks)! 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. Die Auswertung der Raw-Daten der Flash Chips ermöglicht eine Rekonstruktion mit forensischen Mitteln. Mehr Informationen liefert die Publikation *Erasing Data from Flash Drives*<sup>2</sup>.

Für SSDs ist die Trim Funktion zu aktivieren. Dabei werden die Speicherzellen eines Blocks beim Löschen der Datei auf den Ursprungszustand zurück gesetzt. Zusätzliche Maßnahmen zum sicheren Löschen sind dann nicht mehr nötig. Die meisten aktuellen Betriebssystem aktivieren Trim nicht(!) standardmäßig. Folgende Schritte sind nötig, um Trim nach der Installation für SSDs zu aktivieren:

**Windows 7 und neuer** kann TRIM aktivieren. Starten sie das Programm *cmd* als Administrator, um ein Terminal zu öffnen. Im Terminal kann man mit folgendem Kommando den Status der Trim Funktion abfragen:

```
> fsutil behavior query disabledeletenotify
```

<sup>2</sup> [http://www.usenix.org/events/fast11/tech/full\\_papers/Wei.pdf](http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf)

Wenn ein Wert = 0 ausgegeben wird, ist Trim aktiviert. Wird ein Wert = 1 ausgegeben, aktivieren sie die Trim Funktion mit folgendem Kommando:

```
> fsutil behavior set disabledeletenotify 0
```

**Linux** unterstützt seit Kernel 2.6.33 die TRIM Funktionen für SSDs. Das Dateisystem auf der SSD ist mit der Option `discard` zu mounten, um TRIM zu aktivieren.

- Für fest eingebaute Datenträger können die Optionen in der Datei `/etc/fstab` modifiziert und die Option `discard` eingefügt werden:

```
UUID=[NUMS-LETTERS] / ext4 discard,errors=remount-ro 0 1
```

- Die mount-Optionen für USB-Sticks können mit `usbmount` angepasst werden. Nach der Installation des Paketes `usbmount` und `pmount` kann man in `/etc/usbmount/usbmount.conf` die Mount-Optionen anpassen. Folgende Einstellungen funktionieren bei mir unter Ubuntu *precise*:

```
MOUNTOPTIONS="discard,noexec,nodev,noatime,nodiratime"
FS_MOUNTOPTIONS="-fstype=vfat,gid=floppy,dmask=0007,fmask=0117"
```

Alle Nutzer, die unter Windows mit vFAT formatierte USB-Sticks einsetzen wollen, müssen zur Gruppe `floppy` gehören (was standardmäßig unter Ubuntu der Fall ist). Die vFAT formatierten Sticks müssen als `root` ausgehängt werden (mit `pumount`), bevor man den Stick abzieht. Anderenfalls kann es zu Datenverlusten kommen.

Ich werde für mich persönlich weiterhin die vollständige Verschlüsselung der USB-Sticks den Spielereien mit TRIM vorziehen. Damit werden nicht nur gelöschte Dateien geschützt sondern auch die noch vorhandenen Daten. Das Auslesen der RAW-Daten der Speicherzellen durch Forensiker ist dann ebenfalls wenig erfolgreich.

## 14.5 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) <sup>3</sup> 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:

<sup>3</sup> <http://www.dban.org/>

```
> wipe -kq /dev/hda
```

Für SATA- und SCSI-Festplatte:

```
> wipe -kq /dev/sda
```

Wenn die Live-CD 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.)

## 14.6 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/X
```

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
```

Dann kann man ein Passwort setzen und den Datenträger vollständig löschen:

```
> sudo hdparm --user-master u --security-set-pass GEHEIM /dev/X
> sudo hdparm --user-master u --security-erase GEHEIM /dev/X
```

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
```

# Kapitel 15

## 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 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, verwendete Softwareversion und vieles mehr. Diese Angaben sind auch in PDFs enthalten, die mit der Export-Funktion von OpenOffice.org oder Microsoft Office erstellt wurden.

Vor dem Upload der Dateien ins Internet ist es ratsam, diese überflüssigen Informationen zu entfernen. Es gibt mehrere Firmen, die sich auf die Auswertung dieser Metadaten spezialisiert haben. Ein Beispiel ist die Firma Heypic, die die Fotos von Twitter durchsucht und anhand der GPS-Koordinaten auf einer Karte darstellt. Auch Strafverfolger nutzen diese Informationen. Das FBI konnte einen Hacker mit den GPS-Koordinaten im Foto seiner Freundin finden<sup>1</sup>.

Der *StolenCameraFinder*<sup>2</sup> sucht anhand der Kamera ID in den EXIF-Tags alle Fotos, die mit dieser Kamera gemacht wurden. Da die Kamera ID mit hoher Wahrscheinlichkeit eindeutig einer Person zugeordnet werden kann, sind viele Anwendungen für diese Suche denkbar.

### 15.1 Fotos und Bilddateien anonymisieren

- **Irfan View**<sup>3</sup> (Windows) kann in Fotos mit *Öffnen* und *Speichern* die Metatags entfernen. Im Batchmode kann man die Funktion *Konvertieren* nut-

<sup>1</sup> <http://www.tech-review.de/include.php?path=content/news.php&contentid=14968>

<sup>2</sup> <http://www.stolencamerafinder.com>

<sup>3</sup> <http://www.heise.de/download/irfanview.html>

zen, 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.

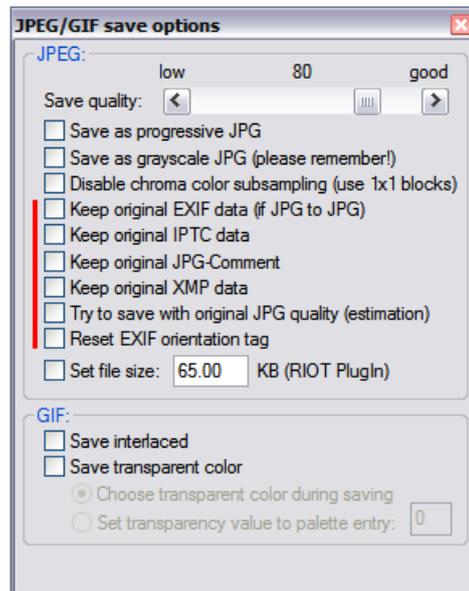


Abbildung 15.1: Informationen in Fotos löschen mit Irfan View

- **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. Nach der Installation kann man z.B. Fotos auf der Kommandozeile säubern:

```
> exiv2 rm foto.jpg
```

## 15.2 PDF-Dokumente säubern

Für Windows gibt es das Tool **BeCyPDFMetaEdit**<sup>4</sup> in einer portablen Version für den USB-Stick oder als Installer. Nach dem Download und evtl. der Installation kann man das Tool starten und die zu säubernden PDF-Dokumente laden. Auf den Reitern *Metadaten* und *Metadaten (XMP)* klickt man auf den Button *Alle Felder löschen* und speichert das gesäuberte Dokument.

## 15.3 Metadata Anonymisation Toolkit (MAT)

Das Metadata Anonymisation Toolkit (MAT)<sup>5</sup> kann PNG und JPEG Bilder, PDF-Dokumente, Microsoft Office Dokumente, OpenOffice Dokumente, MP3 und FLAC Dateien säubern.

<sup>4</sup> [http://www.becyhome.de/download\\_ger.htm](http://www.becyhome.de/download_ger.htm)

<sup>5</sup> <https://mat.boum.org/>

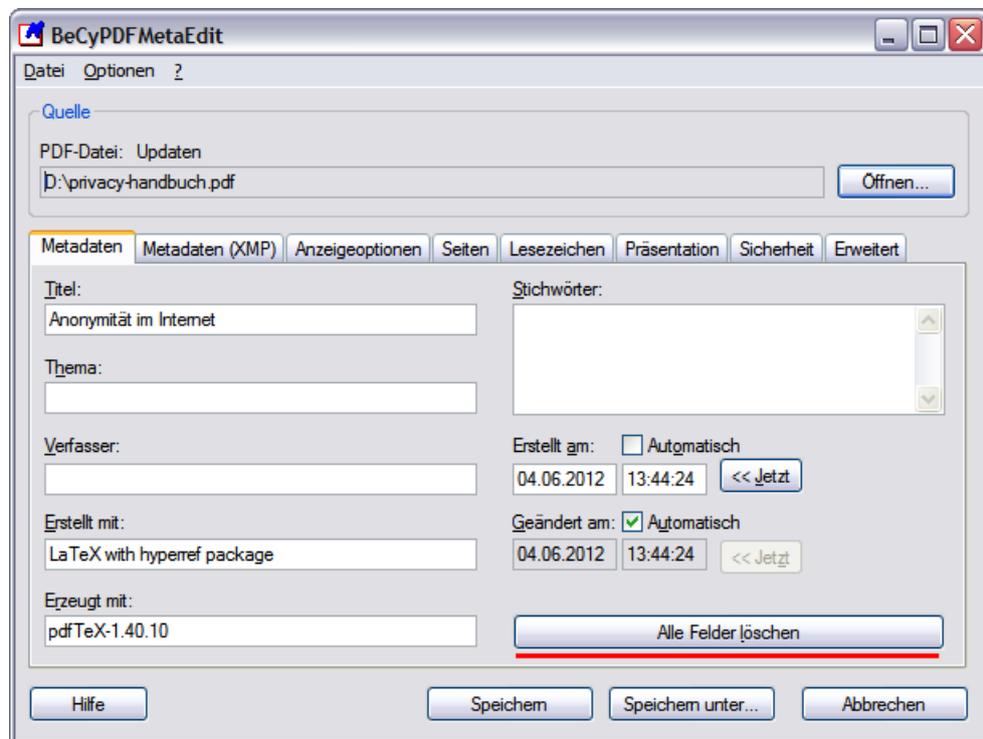


Abbildung 15.2: Metadaten in PDF-Dokumenten löschen

- PDF-Dokumente werden intern als Druckbild gerendert und aus dem Ergebnis wird ein neues Dokument erstellt. Damit werden nicht nur die Metadaten des PDF-Dokumentes entfernt sondern auch die Metadaten aller eingebundenen Bilder. Formulare, Inhaltsverzeichnis, anklickbare Links usw. gehen dabei verloren.
- Bei Office Dokumenten werden nur die Metadaten des Masterdokumentes gelöscht. Um evtl. eingebundene Bilder usw. muss man sich selbst kümmern. Am einfachsten benennt man das Dokument in eine ZIP-Datei um und behandelt es als Archiv.
- Archive werden entpackt, alle unterstützten Dateien werden gereinigt und das Archiv wird neu zusammengestellt. Man kann in den Einstellungen angeben, ob nicht unterstützte Dateien wieder ins Archiv gepackt werden sollen oder nicht.

Das Tool ist in Python geschrieben und braucht einige Bibliotheken. Unter Debian, Ubuntu usw. installiert man zuerst die nötigen Bibliotheken mit:

```
> sudo aptitude install libimage-exiftool-perl python-hachoir-core
python-hachoir-parser python-mutagen python-pdfrw python-gi
python-gi-cairo gir1.2-poppler-0.18 python-distutils-extra
gir1.2-gtk-3.0 python-setuptools python-pdfminer python-pdftools
python-poppler curl
```

Danach entpackt man das heruntergeladene Archiv, wechselt in das neu erstellte Verzeichnis und kann das Programm starten. Es gibt eine Version für die Kommandozeile und eine Version mit grafischer Oberfläche (GUI). Auf der Kommandozeile säubert man Dateien mit:

```
> mat /path/to/datei.ext
```

Die GUI-Version startet man mit:

```
> mat-gui
```

Alternativ kann man MAT auch für alle User installieren mit:

```
> sudo python setup.py install
```

In der Programmgruppe *Zubehör* findet man den Starter für das GUI von MAT. Mit dem + kann man Dateien der Liste hinzufügen und mit dem Besen-Icon daneben säubern. Live-CDs sind eine Alternative, wenn man das Metadata Anonymisation Toolkit als Windows Anwender nutzen möchte. MAT ist in TAILS und in der JonDo Live-CD installiert.

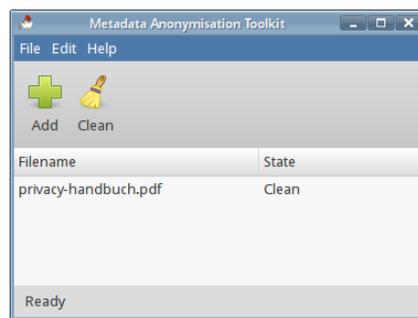


Abbildung 15.3: Dateien säubern mit MAT

## Kapitel 16

# Daten verstecken

Geheimdienste orakeln seit Jahren immer wieder, das *Terroristen* über versteckte Botschaften in Bildern kommunizieren. Telepolis berichtete 2001 und 2008 kritisch-ironisch über Meldungen von Scotland Yard, wonach islamische Terroristen ihre Kommunikation in pornografischen Bildern verstecken würden. Stichhaltige Belege für die Nutzung von **Steganografie** konnten bisher nicht geliefert werden. Andere Journalisten hinterfragten die Meldungen weniger kritisch:

*“Bislang ist zwar noch nicht bewiesen, ob die Terrorverdächtigen die Bilder - bei einem Verdächtigen wurden 40.000 Stück gefunden - nur zum persönlichen Vergnügen heruntergeladen haben oder ob tatsächlich ein Kommunikationsnetzwerk aufgebaut wurde.”* (Welt Online<sup>1</sup>, 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

<sup>1</sup> <http://www.welt.de/politik/article2591337/>

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.

## 16.1 Allgemeine Hinweise

Das Beispiel verdeutlicht, welche Voraussetzungen für die Nutzung von Steganografie zum Austausch von versteckten Botschaften gegeben sein müssen:

- Sender und Empfänger müssen sich darüber verständigt haben, wie die Nutzdaten versteckt werden.
- Das Passwort für die Verschlüsselung muss ausgetauscht werden.
- Die Modalitäten für den Austausch der Trägermedien müssen geklärt werden. Wo kann der Empfänger die Fotos mit den versteckten Botschaften finden?

### Wenn diese Voraussetzungen geklärt sind, kann es losgehen

1. Der Absender schreibt seine Botschaft mit einem einfachen Texteditor.
2. Die Textdatei wird in einem (anonymisierten) Foto oder in einer Audiodatei mit Steganografie Tools wie z.B. *DIIT* oder *steghide* versteckt und gleichzeitig mit dem Passwort verschlüsselt.
3. Das Foto könnte man dem Empfänger per E-Mail senden. Das ist aber nicht unbedingt die beste Idee, da dabei die Metadaten der Kommunikation ausgewertet werden können (A hat B eine Mail geschrieben, Stichwort: Kommunikationsanalyse). Um auch die Metadaten der Kommunikation zu verstecken, könnte der Absender das Foto in seinem (anonymen) Blog veröffentlichen, man könnte es bei Flickr oder Twitpic hochladen oder an eine öffentliche Newsgruppe im Usenet senden. Wichtig ist, dass es öffentlich publiziert wird und der Empfänger nicht erkennbar ist. Außerdem kann der Absender verschiedene Maßnahmen ergreifen, um selbst anonym zu bleiben.
4. Der Empfänger muss wissen, wo er aktuelle Nachrichten finden kann. Fotos oder Audiodateien, in denen der Empfänger eine Botschaft vermutet, sind herunterzuladen.
5. Danach kann der Empfänger versuchen, die geheime Botschaft aus dem Trägermedium zu extrahieren. Dabei ist das gleiche Tool wie beim Verstecken zu verwenden. Wenn er alles richtig macht und das korrekte Passwort verwendet, wird die Textdatei extrahiert und kann mit einem einfachen Texteditor gelesen werden.

### Unsichtbare Markierungen, Wasserzeichen

Man kann Steganografie Tools auch nutzen, um unsichtbare Wasserzeichen an Bildern oder Audiodateien anzubringen.

Wenn Fotos oder Videos nur einem kleinen Kreis von Personen zugänglich gemacht werden sollen, dann können individuelle Wasserzeichen steganografisch in den Dateien versteckt werden. Sollten diese Fotos oder Videos in der Öffentlichkeit auftauchen, kann das Leck anhand des unsichtbaren steganografischen Wasserzeichens ermittelt werden.

## 16.2 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
```

## 16.3 stegdetect

Auch die Gegenseite ist nicht wehrlos. Manipulationen von steghide, F5, outguess, jphide usw. können z.B. mit *stegdetect*<sup>2</sup> 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:

```
> 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.

<sup>2</sup> <http://www.outguess.org/download.php>

# Kapitel 17

## 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.

### 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 und besser personalisieren.

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.
- Mit der digitalen Assistentin *Cortana* wird in der Standardkonfiguration eine Art Abhörzentrale eingerichtet, die das Wohnzimmer direkt mit Microsoft verbindet.
- Das Schreibverhalten wird analysiert und an Microsoft gesendet. Das Profil der typischen Tastenanschläge könnte zukünftig für die Identifikation bei Texteingaben in Webformularen oder Chats genutzt werden (Stichwort: Keystroke Biometrics<sup>1</sup>).
- Als besonderes Highlight gehören auch die automatisch Recovery Keys der Festplattenverschlüsselung Bitlocker zu den Daten, die MS in seiner Cloud sammelt und NSA/FBI/CIA zur Verfügung stellt.

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.<sup>2</sup>

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...

<sup>1</sup> <https://de.wikipedia.org/wiki/Tippverhalten/>

<sup>2</sup> <http://arstechnica.com/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft>

Mit der immer wieder beschworenen Installation eines Virencanners gibt der Nutzer praktisch die Hoheit über die Installation von Software teilweise auf. Es ist die Aufgabe eines Virencanners, Software zu entfernen, die der Hersteller der Software für unpassend hält. Außerdem entstehen durch Antiviresoftware neue Lücken, die durch Angreifer gezielt ausgenutzt werden können. Da Virencanner sehr tief im System sitzen, sind diese Lücken besonders gefährlich.

Können kommerzielle Virencanner gegen staatliche Trojaner schützen? Wer die Veröffentlichungen um die NSA-Cyberwaffe *Regin* genauer verfolgt hat, der muss diese Frage wohl mit *Nein* beantworten.

1. 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.*

2. Dann wurde der Trojaner *Regin* von Symantec analysiert. Auch Symantec veröffentlichte nichts. Vikram 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.*

3. Erst nachdem The Intercept ankündigte, über *Regin* zu berichten, haben die Anti-Virus Firmen reagiert und sind ebenfalls an die Öffentlichkeit gegangen.
4. 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 diesen weiteren Fall von NSA-Spionage anfangs nicht kommentieren und dementierte halbherzig.

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.

## MacOS

Wenn man die Apple Datenschutzrichtlinie liest, dann erkennt man, das MacOS sich nicht als Betriebssystem eignet, wenn man seine Privatsphäre nicht mit Apple teilen möchte:

*Wir erheben Daten wie namentlich Beruf, Sprache, Postleitzahl, Vorwahl, individuelle Geräteidentifizierungsmerkmale, Weiterleitungs-URL sowie Ort und Zeitzone, wo Apple Produkte verwendet werden, damit wir das Verhalten unserer Kunden besser verstehen und unsere Produkte, Dienste und Werbung verbessern können.*

Für diese Datensammlungen wurde Apple mit dem BigBrother Award 2011 geehrt. Apple ist seit Oktober 2012 Partner im PRISM Programm der NSA.

## Linux

Es gibt eine Vielzahl von Linux Distributionen, so dass man als potentieller Anwender erst einmal vor der Qual der Wahl steht: Debian und Derivate, Open-SuSE, Mandrive, Fedora, Gentoo für Bastler, Minidistributionen wie Puppy oder Fortress Linux als besonders gehärtete Variante... Ich kenne längst nicht alle Distributionen daher nur einige Gedanken:

- **Debian** ist ein robustes Arbeitstier unter den Linux Distributionen. Die Maintainer legen vor allem Wert auf Stabilität und weniger auf 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. Debian hatte als erste Distribution Full-Disc-Encryption bei der Installation angeboten.
- **Ubuntu** ist angetreten, um das bessere Debian zu sein und mit aktueller Software auch neueste Hardware gut zu unterstützen. In letzter Zeit geht das Projekt oft eigene Wege und die Übertragung sämtlicher Suchanfragen auf dem Desktop an kommerzielle Dritte wie z.B. Amazon ist ein Fiasko für die Privatsphäre. Man kann diese Probleme aber beseitigen, siehe FixUbuntu.com.<sup>3</sup>

1. Das Unity Tweak Tool installieren und starten. Auf der Kommandozeile:

```
> sudo apt-get install unity-tweak-tool
> unity-tweak-tool
```

2. Auf dem Reiter *Suche* ist das *Durchsuchen von Online Quellen* sowie *Mehr Empfehlungen anzeigen* zu deaktivieren.

Ubuntu gibt es in einer häufig aktualisierten Version, die man komplett alle 6 Minate aktualisieren muss, oder als LTS Version (Long Term Support), die man nur alle zwei Jahre komplett aktualisieren muss.

- **Xubuntu** (LTS) gefällt mir eigentlich am besten. Die gute Hardware Unterstützung für neue Technik kombiniert mit einfacher Installation, klarem Bedienkonzept des XFCE Desktop ohne irgendwelchen Cloud Anbindungen oder Übertragung von Daten an Dritte sowie Full-Disc-Encryption bei der Installation mag ich.

---

<sup>3</sup> <https://fixubuntu.com/>

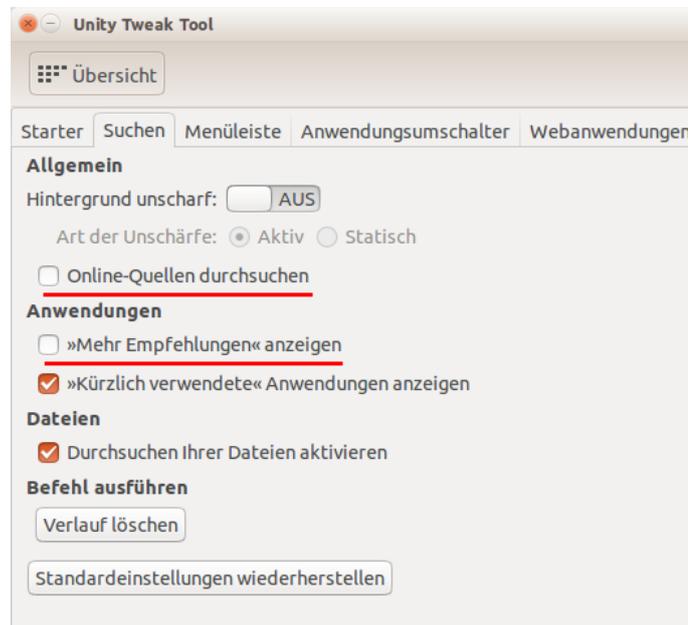


Abbildung 17.1: Privacy Einstellungen im Unity Tweak Tool

- **Mint Linux** möchte das bessere Ubuntu sein und bietet vor allem einen anderen Desktop, der auch sehr hübsch ist. Allerdings ist Mint keine komplett selbständige Distribution sondern schmarrotzt bei Ubuntu, was schon öfters für Verstimmung bei Canonical sorgte. Mit Mint Debian Edition gibt es auch eine Variante, die auf Debian (unstable) basiert.

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. Ich habe nichts vermisst.

### NetBSD und OpenBSD

Diese beiden BSDs sind konsequent und ohne Kompromisse hinsichtlich Benutzbarkeit auf Sicherheit optimiert. Wenn man mehrere Jahre Erfahrung mit mit einem UNIX-artigen System (z.B. Linux) gesammelt hat und hinreichend leidensfähig ist, dann kann man auch diese beiden Betriebssystem 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 Allocieren 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
```

## 17.1 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.

Auf der Blackhat 2014 haben K. Nohl und J. Lell von SRLabs im Vortrag *BadUSB - On Accessories that Turn Evil*<sup>4</sup> gezeigt, wie man modifizierte USB-Geräte für viele böse Dinge nutzen kann, da kaum Sicherheitshürden überwunden werden müssen. USB-Geräte (z.B. USB-Sticks von Fremden) können neben der offen sichtbaren Funktion (z.B. als Speichermedium) verdeckte Funktionen enthalten, die man nicht bemerkt. Sie können sich als USB-Tastatur ausgeben und Kommandos senden, sie können sich als Netzwerkkarten ausgeben und den Datenverkehr umleiten oder einfach einen Virus/Trojaner installieren.

Wenn man es einmal ausprobieren möchte, kann man sich das Script *BadAndroid-v0.1.zip*<sup>5</sup> 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 der Internettraffic für bestimmte Webseiten wird umgeleitet, ohne das der User etwas merkt - eine nette Demo.

Ein besonderes Risiko sind USB-Sticks oder USB-Festplatten, die man bedenkenlos an unterschiedlichen Computern in verschiedenen Netzen nutzt.

- Ein Beispiel aus der Praxis: In den 90ziger Jahren des letzten Jahrhunderts war ich 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 schlampig gewarteten 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

<sup>4</sup> <https://www.youtube.com/watch?v=nuruzFqMgIw>

<sup>5</sup> <https://srlabs.de/blog/wp-content/uploads/2014/07/BadAndroid-v0.1.zip>

transportieren. Dabei kann der USB-Stick extra präpariert werden oder man greift die schlecht gesicherten Rechner mehrere Tagets 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 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 Spoinage-Trojaner der NSA. Dieser Trojaner konnte 2014 vom schlecht gesicherten, heimischen PC einer Mitarbeiterin ins Bundeskanzleramt gelangen und dann dort seine Aufgaben ausführen, weil die Mitarbeiterin dienstliche Dokumente zuhause bearbeitete und mit einem USB-Stick ins Bundeskanzleramt brachte.

Bei **Firewire** (IEEE 1394) und **Thunderbolt** Schnittstellen ist das Risiko noch größer. Im Gegensatz zu USB wird bei diesen Schnittstellen keine Master-Slave Kommunikation genutzt. Über Firewire und Thunderbolt haben angeschlossene Geräte via DMA (Direct Memory Access) vollen Zugriff auf den Hauptspeicher des PC und können z.B. eine Kopie auslesen.

- 2008 wurde demonstriert, wie man den Windows Login mit einem Firewire Gerät umgehen kann. Microsoft sah keinen Handlungsbedarf, da die Funktionalität der Firewire Spezifikation entspricht. Es ist also kein Bug sondern ein Feature.
- Gegen Aples I/O-Technik Thunderbolt gabe es von Anfang an Sicherheitsbedenken<sup>6</sup>. 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 unbekanntem 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 Firma nehmen will.

<sup>6</sup> <http://heise.de/-1198049>

3. Zum Aufladen von Geräten kann man USB-Ladegeräte nutzen. Man muss nicht alles, was wie ein USB-Stecker aussieht, in den Computer einführen.
4. Es gibt zahlreiche Freeware Tools, um USB-Schnittstellen unter Windows zu sperren. (z.B. den USB-Blocker<sup>7</sup> von securityXploded.com)
5. 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.*<sup>8</sup>
  - 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
```

## 17.2 Linux Firewall konfigurieren

Die Firewall des Linux Kernels wird mit dem Tool *iptables* konfiguriert. Es gibt einige GUIs für die Konfiguration, die irgendwelche Regeln zusammenstellen und eine Firewall verwalten können. Volle Kontrolle über die Firewall hat man aber nur, wenn man es selbst macht. Eine Firewall mit *iptables* selbst zu konfigurieren, ist nicht so schwer. Einfache Dinge sind einfach und Kompliziertes ist möglich.

Man kann für alle Distributionen Shell-Script mit der Firewall Konfiguration im Verzeichnis */etc/network/if-up.d* speichern. Das Script wird dann nach dem Herstellen einer Netzwerkverbindung ausgeführt und aktiviert die Firewall Regeln. Eine einfache Firewall Basis-Konfiguration für Desktop Rechner oder Laptops blockiert alle Verbindungsversuche von außen und erlaubt es allen Nutzern und Daemonen, Verbindungen ins Internet herzustellen:

```
#!/bin/sh
set -e
```

<sup>7</sup> <http://securityxploded.com/windows-usb-blocker.php>

<sup>8</sup> <https://support.microsoft.com/kb/2516445/de>

```

# Nichts tun, wenn loopback aktiviert wird
[ "$IFACE" != "lo" ] || exit 0

# alte Konfiguration löschen
/sbin/iptables --flush
/sbin/iptables --delete-chain
/sbin/iptables -t mangle --flush
/sbin/iptables -t mangle --delete-chain
/sbin/iptables -t nat --flush
/sbin/iptables -t nat --delete-chain

# forwarding deaktivieren
echo 0 > /proc/sys/net/ipv4/ip_forward

# Default-Policies setzen
/sbin/iptables -P INPUT DROP
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT ACCEPT

# loopback freischalten
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -i lo -j ACCEPT

# Antworten auf bestehende Verbindungen erlauben
/sbin/iptables -A INPUT -i $IFACE -m state --state ESTABLISHED,RELATED -j ACCEPT

```

Das Script kann man von meiner Webseite herunter laden. Nach dem Download ist das Script in das Verzeichnis `/etc/network/if-up.d` zu kopieren (1) und als *ausführbar* zu markieren (2). Für beide Schritte sind root Rechte erforderlich.

- (1) > `sudo cp Downloads/zzz-firewall.sh /etc/network/if-up.d`
- (2) > `sudo chmod +x /etc/network/if-up.d/zzz-firewall.sh`

Diese Firewall Konfiguration ist stealth. Der Rechner beantwortet keine Pings und ist nicht mit Portscans im lokalen Netz auffindbar.

### Erweiterungen der Basiskonfiguration - Teil 1

Wenn Dienste auf dem Rechner von außen erreichbar sein sollen, dann kann man weitere Regeln anfügen, um einzeln Ports zu öffnen. Als Beispiel soll der Port 8888 (für den I2P-Router) für eingehenden TCP und UDP Traffic geöffnet werden:

```

/sbin/iptables -A INPUT -i $IFACE -p tcp --dport 8888 -j ACCEPT
/sbin/iptables -A INPUT -i $IFACE -p udp --dport 8888 -j ACCEPT

```

### Erweiterungen der Basiskonfiguration - Teil 2

Wenn nur bestimmte User und Daemons Verbindungen ins Internet herstellen dürfen, kann man zusätzliche OUTPUT Regeln einfügen, die diesen UIDs den Aufbau von Verbindungen ins Internet ausdrücklich erlaubt und dann alle

anderen Verbindungsversuche abweisen. Zuerst muss man das Kernelmodul *ipt\_owner* laden:

```
modprobe ipt_owner
```

Die Regeln werden nach folgendem Muster definiert:

```
# Freigabe definieren
/sbin/iptables -A OUTPUT -o $IFACE -m owner --uid-owner <user> -j ACCEPT

# den Rest blockieren
/sbin/iptables -t filter -A OUTPUT -j REJECT
```

Dafür sollte man sein System aber gut kennen und wissen, welche Dienste man benötigt. Ein kleines Beispiel als Anregung für eigene Experimente:

- Es soll nur dem Nutzer *inetuser* gestattet werden, im Internet zu surfen und Tor bzw. JonDo zu verwenden. Dafür reicht es, die Ports 80 und 443 für ausgehende TCP Verbindungen zu öffnen.
- Der DNSCrypt-proxy kümmert sich um die Auflösung der DNS-Namen beim Surfen ohne Tor oder JonDo und läuft unter der UID *dnscrypt*.
- Alle weiteren Tools zur Kommunikation werden mit Tor oder JonDo (Premium) anonymisiert, beide Anon-Dienste können Port 443 verwenden.

Dafür sind folgende Regeln nötig:

```
# Freigaben
/sbin/iptables -A OUTPUT -o $IFACE -m owner --uid-owner inetuser \
-p tcp --dport 80 -j ACCEPT
/sbin/iptables -A OUTPUT -o $IFACE -m owner --uid-owner inetuser \
-p tcp --dport 443 -j ACCEPT
/sbin/iptables -A OUTPUT -o $IFACE -m owner --uid-owner dnscrypt \
-p udp --dport 443 -j ACCEPT

# den Rest blockieren
/sbin/iptables -t filter -A OUTPUT -j REJECT
```

Was passiert, wenn man als *root* die Software aktualisieren will oder Software aus den Repositories installieren will? *root* kann keine Verbindungen ins Internet aufbauen. Entweder man nutzt Tor bzw. JonDo dafür, oder man fügt temporär eine weitere Regel für *root* hinzu. Viele Spielchen sind möglich.

### Erweiterungen der Basiskonfiguration - Teil 3

Mit der Option *-d* (*--destination*) kann man zulässige IP-Adressen oder Netzwerkbereiche für ausgehenden Traffic definieren. Man könnte im Beispiel oben z.B. eine OUTPUT Regel vor der letzten REJECT Regel einfügen, die Verbindungen zu einem CUPS Netzwerkdrucker erlaubt. Die IP-Adresse des Netzwerkdrucker ist in diesem Beispiel 192.168.1.30.

```
# Verbindungen zum Netzwerkdrucker erlauben
/sbin/iptables -A OUTPUT -o $IFACE -p tcp -d 192.168.1.30 \
--dport 631 -j ACCEPT
```

In Firmen könnte man pauschal Verbindungen zu allen Netzwerkdruckern im lokalen Netz erlauben, indem man den gesamten Netzwerkbereich 192.168.1.\* freigibt:

```
# Verbindungen zu allen Netzwerkdruckern im LAN erlauben
/sbin/iptables -A OUTPUT -o $IFACE -p tcp -d 192.168.1.0/24 \
--dport 631 -j ACCEPT
```

Prinzipiell kann man auch Hostnamen statt IP-Adressen verwenden. Die DNS-Auflösung der Hostnamen erfolgt aber nur einmalig vor der Übergabe der Regeln an den Kernel.

### Logging

Zur Erkennung von Angriffsversuchen oder um Probleme mit eigenen, restriktiven Konfigurationen zu erkennen, kann man Logging in *iptables* aktivieren.

```
# Logging aktivieren
/sbin/iptables -N LOGGING
/sbin/iptables -A INPUT -j LOGGING
/sbin/iptables -A OUTPUT -j LOGGING
/sbin/iptables -A LOGGING -m limit --limit 2/min -j LOG \
--log-prefix "IPTables-Dropped: " --log-level 4
/sbin/iptables -A LOGGING -j DROP
```

Dieses Beispiel schreibt die Logs über gedropte Paket nach */var/log/syslog*. Die Zeilen beginnen mit *IPTables-Dropped:*, so dass man mit schnell filtern kann.

## 17.3 Privacy Leaks mit DHCP

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 übermittelt. Damit hinterlässt man auf dem DHCP-Server Spuren, die C. Huitema von der IETF in der Studie *Unique Identifiers in DHCP options enable device tracking*<sup>9</sup> 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).
2. Die UUID/GUID des Intel Preboot eXecution Environment (PXE) wird an den DHCP-Server übermittelt, wenn PXE in den BIOS Einstellungen aktiv ist.
3. Der konfigurierte Hostname und die DNS-Domain des Rechners wird an den DHCP-Server übermittelt.

<sup>9</sup> <https://tools.ietf.org/html/draft-huitema-perpass-dhcp-identifiers-00>

Um keine eindeutigen Spuren als Road-Warrior in Internet Cafe's oder am Flughafen zu hinterlassen, sollte man die MAC-Adresse des WLAN-Modul faken, PXE im BIOS deaktivieren und nichtssagenden Hostnamen und DNS-Domain für den eigenen Rechner nutzen.

Wenn man Windows oder MacOS verwendet, dann lohnt es sich nicht, weiter darüber nachzudenken. Windows und MacOS teilen Microsoft bzw. Apple nach dem Herstellen der Netzwerkverbindung viele Details mit, bei MacOS auch den aktuellen Standort. Deshalb gibt es im folgenden nur Hinweise für Linux.

### 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. Die anonymen Live-CDs JonDo-Live und TAILS nutzen folgende nichts aussagende Werte:

```
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
```

### MAC-Adresse ändern unter Linux

Die MAC-Adresse ist eine weltweit eindeutige Kennung der Netzwerkschnittstelle. Jede Netzwerkkarte und jedes WLAN-Modul hat eine eindeutige Kennung.

- In IPv4 Netzen wird diese Kennung nur bis zum Router/Gateway übertragen. Im eigenen Home-Netz braucht man sich keine Gedanken machen, wenn man vom DSL-Provider eine IPv4 Adresse zugeteilt bekommt. In fremden WLANs (Internetcafe', Flughafen, Hotel) ist davon auszugehen, dass die MAC-Adressen protokolliert werden können.

- 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 eindeutig personenbezogenen Merkmal.

Unter Linux gibt es das Tool *macchanger*, das man mit dem bevorzugten Paketmanager der Distribution installieren kann. Um bei Bedarf die MAC-Adresse des WLAN-Moduls zu ändern, ist als root zuerst der NetworkManager zu stoppen, dann die MAC-Adresse zu ändern und danach der NetworkManager wieder zu starten.

```
> sudo su
# service network-manager stop
# macchanger -a wlan0
# service network-manager start
# exit
```

Man kann die MAC-Adresse auch beim Booten automatisch ändern lassen. Für Debian, Ubuntu und Mint werden die Netzwerkschnittstellen durch Init-Scripte initialisiert. Man kann folgendes Sys-V-Init Script *macchanger-boot* nutzen, um die MAC-Adresse der WLAN-Schnittstelle zu ändern.

```
#!/bin/bash

### BEGIN INIT INFO
# Provides: macchanger
# Required-Start: networking
# Required-Stop:
# Should-Start:
# Default-Start: S
# Default-Stop:
# Short-Description: Change MAC address of WLAN interface
### END INIT INFO

PATH=/sbin:/bin:/usr/bin
. /lib/lsb/init-functions

case $1 in
  restart|reload|force-reload|start)
    log_action_begin_msg "Change MAC address of wlan0"
    /usr/bin/macchanger -a wlan0 > /dev/null
    log_action_end_msg 0
    ;;

  stop)
    ;;
esac
exit 0
```

Nach dem Download kopiert man das Script nach */etc/init.d*, setzt die Rechte auf ausführbar und fügt es in den Startprozess ein. Im Terminal sind dafür folgende Befehle auszuführen:

```
> sudo su
# cp macchanger-boot /etc/init.d/
# chmod +x /etc/init.d/macchanger-boot
# insserv macchanger-boot
# exit
```

Unter Suse Linux kann man den Befehl zum Ändern der MAC-Adresse am Ende des Scriptes */etc/init.d/boot.local* einfügen. Die Datei kann man mit einem Texteditor bearbeiten und die folgende Zeile einfügen:

```
macchanger -a wlan0
```

Möchte man statt der MAC-Adresse des WLAN-Moduls die MAC-Adresse der Ethernetschnittstelle ändern, dann ist *wlan0* durch *eth0* zu ersetzen.

# Kapitel 18

## Live-DVDs

Es gibt einige Projekte, die fertig konfigurierte Live-DVDs bereitstellen. Bei der Nutzung einer Live-DVD erhält man ein sinnvoll vorkonfiguriertes und garantiert sauberes System ohne Trojaner. Da man keine Updates einspielen kann, sollte man regelmäßig eine aktuelle Version des ISO-Images von der Webseite herunterladen.

**JonDo Live-DVD** basiert auf Debian *wheezy* und bietet JonDonym, Tor und Mixmaster als Anonymisierungsdienste. Mit dem JonDoFox und dem originalen TorBrowserBundle sind sichere Browser installiert. Der E-Mail Client Icedove ist für anonyme Nutzung vorbereitet. Außerdem sind POND, Pidgin, Jitsi, Skype, der Parole Media Player, MAT und weitere Anwendungen enthalten.

Die Live-DVD gibt es mit deutscher Lokalisierung. Sie kann sowohl mit Intel i686 als auch mit AMD64 Computern genutzt werden.

Download: <https://www.anonym-surfen.de/jondo-live-cd.html>

**TAILS** *The Amnesic Incognito Live System* ist die offizielle Live-DVD von Torproject.org. Der gesamte Datenverkehr ins Internet wird in der Standardkonfiguration durch Tor geschickt. TAILS bietet die Anonymisierungsdienste Tor und I2P. Diese Live-CD kann nur mit Intel i686 Computern genutzt werden.

Download: <https://tails.boum.org/>

**Bankix** ist speziell für sicheres Online Banking optimiert. Es wird vom Heise Verlag gepflegt. Das Live System basiert auf Ubuntu LTS. Bankix unterstützt UEFI und *Secure Boot*. Es sind keine Anpassungen der BIOS Einstellungen auf Win 8 kompatiblen Computern nötig, um die Live-DVD zu nutzen.

**Ubuntu Privacy Remix** soll an dieser Stelle auch erwähnt werden. Es ist eine Live-CD ganz ohne Netzwerkverbindungen. Diese Live-CD ermöglicht ein sicheres Bearbeiten von Dokumenten in einer garantiert sauberen Umgebung, eine Lösung für spezielle Fälle.

## 18.1 USB-Sticks als Bootmedium vorbereiten

Für die JonDo Live-DVD und TAILS wird alle 3-6 Wochen eine aktualisierte Version zum Download freigegeben. Deshalb verwende ich USB-Sticks als Boot Medium statt DVDs. Regelmäßige Aktualisierung ist (nicht nur) für sicherheitsrelevante Software ein Muss.

**Windows:** Mit dem *Easy Universal USB Installer* von Pendrivelinux.com kann man einfach einen bootfähigen USB-Stick aus einem Linux ISO-Image erstellen. Mit dem *YUMI Multiboot USB Creator* von Pendrivelinux.com kann man mehrere Live-Systeme auf einen USB-Stick packen.



Abbildung 18.1: Easy Universal USB Installer

Nach dem Download ist die EXE-Datei zu starten (keine Installation nötig). Man wählt die Option *Try unlisted Linux ISO image*, das herunter geladene ISO-Image und außerdem den USB-Stick, der verwendet werden soll.

**Linux:** Man kann auf der Kommandozeile das Tool *dd* verwenden, um das ISO-Image auf den USB-Stick zu schieben. Nach dem Anschließen des USB-Stick benötigt man die die Device Kennung, die man Quick-and-Dirty mit IIsärmitteln 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 mit dem Tool *dd* das ISO-Image von TAILS oder die JonDo Live-DVD auf den USB-Stick. Dabei werden alle(!) Daten und Partitionen auf dem Stick gelöscht.

```
> dd if=jondo-live-dvd.iso of=/dev/sdc
```

Wenn man eine Fortschrittsanzeige für den Kopiervorgang sehen will, dann kann man das Tool *buffer* verwenden:

```
> dd if=jondo-live-dvd.iso | buffer -s 64k -S 10m >/dev/sdc
```

Man kann diese Methode auch in den Live-DVDs nutzen, wenn man zwei USB-Sticks im Wechsel verwendet.

## 18.2 BIOS-Einstellungen für Win8 Rechner

TAILS unterstützt kein Secure Boot und die JonDo Live-DVD unterstützt kein UEFI. Um diese Live-DVDs mit modernen Windows 8 kompatiblen Rechnern zu nutzen, sind Anpassungen an den BIOS-Einstellungen nötig. Sonst erhält man beim Booten des Live-Systems den Fehler:

```
Image Authorization Fail  
System can not boot this device due to Security Violation.
```

Wie man die BIOS-Einstellungen öffnet, ist von Rechner zu Rechner unterschiedlich. Üblicherweise muss man in den ersten 1-2 Sekunden beim Booten des Rechners die Taste F1, F2 oder ENTF drücken. Mein Laptop hat eine extra Taste dafür. Das Handbuch zur Hardware liefert konkrete Antworten.

In der Sektion *Boot* im BIOS muss man folgendes anpassen:

- TAILS: Die Option *Secure Boot* ist zu deaktivieren. Bei einigen Computern versteckt sich diese Option hinter *OS Selection* und man muss *WIN 7/others OS* wählen.
- JonDo Live-DVD: Da kein UEFI unterstützt wird, muss man das *Compatibility Support Module* (CSM) laden bzw. *Legacy Support* beim *Boot Mode* aktivieren. Secure Boot wird damit automatisch deaktiviert.

Außerdem sollte man *PXE-Boot* deaktivieren (siehe: DHCP Privacy).

Zur Vereinfachung in der täglichen Nutzung kann man die Bootreihenfolge im BIOS ändern. Standardmäßig bootet der Computer das OS vom DVD-Laufwerk oder der ersten Festplatte. Man kann den USB-Stick als erstes Boot Medium setzen. Dann bootet das installierte OS nur, wenn der USB-Stick nicht angesteckt ist.

Alternativ kann man das beim Starten des Rechners das *BIOS Boot Select Menü* aufrufen (bei PCs üblicherweise mit den Tasten F8, F10 oder F12, bei Macs die ALT-Taste gedrückt halten), wenn man den USB-Stick nutzen will. Das Handbuch zur Hardware liefert wieder konkrete Antworten.

## Kapitel 19

# 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.*

Ob ich ein Smartphone nutze, werde ich manchmal gefragt. Gegenfrage: Braucht man das Ding wirklich oder ist nur ein nettes Lifestyle Gadget? Ich denke, Jakob Appelbaum hat recht:

*Benutzt am besten gar keine Mobiltelefone. Oder wir müssen die Mobilfunktechnik so grundlegend neu entwickeln, dass sie keine Spionagetechnik mehr ist.*

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.*

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 beschreibt 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.*

Man sollte sich darüber im Klaren sein, dass es gegen die Lokalisierung und Beobachtung von Bewegungsprofilen keinen technischen Schutz gibt.

## 19.1 Kommerzielle Datensammlungen

Die Auswertung der Standortdaten schafft einen neuen Markt für Werbung, der den bisherigen Markt für personenbezogene Werbung im Internet weit übertreffen soll. Bei den damit möglichen Gewinnen wundert es nicht, dass viele Teilnehmer aggressiv dabei sind, Daten zu sammeln:

- In Apples Datenschutzbestimmungen für das iPhone räumt der Konzern sich das Recht ein, den Standort des Nutzers laufend an Apple zu senden. Apple wird diese Daten Dritten zur Verfügung stellen. Für diese Datensammlungen 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.*

- Mit der Software Carrier IQ, die auf über 140 Mio. Android Handys und auf einigen Apples iPhone installiert war, sammelten verschiedene Mobil Provider Informationen über die Nutzer. Die Software konnte nicht auf normalen Weg durch den Nutzer deinstalliert werden.
- Tausende Apps sammeln überflüssigerweise Standortdaten der Nutzer und übertragen sie an die Entwickler der Apps. Der Bundesdatenschutzbeauftragte erwähnt beispielsweise eine App, die das Smartphone zur Taschenlampe macht und dabei den Standort an den Entwickler der App sendet. Einige Spiele der Hersteller iApps7 Inc, Ogre Games und redmi-capps gehen in ihrer Sammelwut so weit, dass sie von Symantec als Malware eingestuft werden. Die Spiele-Apps fordern folgende Rechte um Werbung einzublenden:
  - ungefährender (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.

- Einige Apps beschränken sich nicht auf die Übertragung der Standortdaten und Einblendung von Werbung. Die folgenden Apps haben auch das Adressbuch der Nutzer ausgelesen und ohne Freigabe durch den Nutzer an den Service-Betreiber gesendet:
  - die Social Networks *Facebook*, *Twitter* und *Path*
  - die Location Dienste *Foursquare*, *Hipster* und *Foodspotting*

- die Fotosharing App *Instagram*

Besonders brisant wird diese Datensammlung, wenn Twitter alle Daten von Wikileaks Unterstützern an die US-Behörden herausgeben muss.

- Die App von Facebook fordert außerdem folgende Rechte:
  - Lesender Zugriff auf alle SMS und MMS
  - Zugriff auf Kalendertermine sowie vertrauliche Informationen
  - ohne das Wissen der Eigentümer Kalendertermine hinzufügen oder ändern
  - E-Mails an Gäste senden

Ein Entwickler von Facebook versicherte, dass man diese Rechte nie voll ausnutzen wird. Die Facebook-App braucht diese Rechte nur für die Authentifizierung und um einen Kalender-Feed anzulegen. Ich bin mir ganz sicher: *Niemand hat vor...* Aber wer würde einem Mitglied der PRISM-Gruppe diese Rechte einräumen?

- Die Security-Suites von Avira, Bitdefender und AVG werben mit einer einfachen Lokalisierung des Smartphone bei Diebstahl. Dafür werden die Standortdaten ständig an die Firmen übertragen, auch wenn man den Diebstahlschutz deaktiviert hat.

## 19.2 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.<sup>1</sup>

<sup>1</sup> <http://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims/>

- 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 Middle East.

Auch in Deutschland wird die Lokalisierung von Handys und 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.<sup>2</sup>
- 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.<sup>3</sup> Die Überwachung Handys der Aktivisten begann bereits zwei Jahre vor dem G8-Gipfel in Heiligendamm.
- Die breite Funkzellenauswertung in Berlin zur Aufklärung von Sachbeschädigungen wird als gängige Ermittlungsmethode beschrieben. Auf Anfrage musste die Polizei zugeben, dass diese Methode bisher NULL Erfolge gebracht hat.
- Die Nutzung der Stillen SMS zur Lokalisierung von Personen boomt gerade beim Verfassungsschutz:
  - 1. Halbjahr 2013: 28.500 Stille SMS versendet
  - 1. Halbjahr 2014: 53.000 Stille SMS versendet
  - 2. Halbjahr 2014: 142.000 Stille SMS versendet

Gleichzeitig stagniert die Nutzung der Stillen SMS bei Strafverfolgern (Polizei, BKA usw.) oder geht zurück. Man kann jetzt darüber spekulieren, was die Gründe für diese Aktivitäten des 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.

<sup>2</sup> <http://www.heise.de/tp/artikel/34/34973/1.html>

<sup>3</sup> <http://www.heise.de/tp/artikel/35/35043/1.html>



Die Nutzung des Systems gegen Protestler wird ausdrücklich beworben:

*Bei Protestcamps, Besetzungen u. ä. werden üblicherweise in größerem 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.

#### **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<sup>4</sup>. Bereits 2007 hat das BSI deshalb empfohlen, bei Gesprächen mit sensiblen Inhalten keine Handys mitzuführen.

*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.*

### **19.3 Stille SMS ind IMSI-Catcher erkennen**

Die App **Android-IMSI-Catcher-Detector** (AIMSICD) tut, was der Name sagt. Sie ist auf allen Androids einsetzbar und erfordert kein Rooten des

<sup>4</sup> <http://news.cnet.com/2100-1029-6140191.html>

Smartphones. Die Entwickler setzen den Open Source Gedanken konsequent um. Die App ist nicht(!) im Google PlayStore verfügbar sondern im F-Droid Store, der nur Open Source Projekte anbietet.

Die App **SnoopSnitch** von SRLabs steht seit Januar 2015 für Android im F-droid Store und im PlayStore bereit. Die App erkennt IMSI-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.

Die App **Darshak** von R. Borgaonka (SecT, TU Berlin) kann Alarm auslösen, wenn der Standort des Smartphone mit sogenannten *Stillen SMS* getrackt wird, und kann außerdem die Sicherheitseinstellungen der Funkzelle sichtbar machen, um den Einsatz eines IMSI-Catchers zu erkennen. Die App steht auf Github zum Download bereit.<sup>5</sup> Sie ist derzeit nur auf dem Samsung Galaxy S3 einsetzbar und erfordert ein Rooten des Smartphone. Die Installation ist auf der Webseite beschrieben.

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 Botchaften 18 IMSI-Catcher aufgespürt<sup>6</sup>.

*I would bet money that there are governments that are spying in DC. (C. Soghoian, ACLU)*

Washington DC ist kein Einzelfall. Auch in Oslo wurden IMSI-Catcher im Regierungsviertel gefunden. Leider mussten die Journalister einer Zeitung mit einem GSMK CryptoPhone erst darauf aufmerksam machen. Die norwegische Spionageabwehr ist genauso verschlafen wie in Berlin.<sup>7</sup>

*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!

## 19.4 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

<sup>5</sup> <https://github.com/darshakframework/darshak>

<sup>6</sup> <http://rt.com/usa/189116-washington-dc-spying-phone>

<sup>7</sup> <http://www.zeit.de/digital/datenschutz/2014-12/norwegen-spionage-oslo>

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.<sup>8</sup>

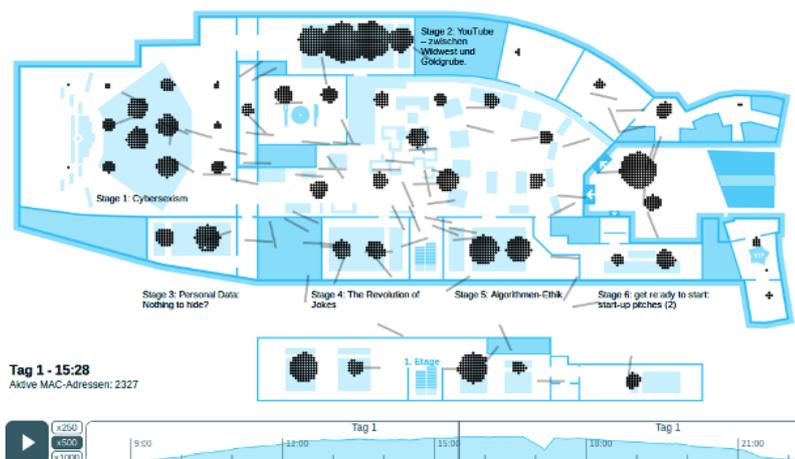


Abbildung 19.1: WLAN Tracking auf der re:publica 2013

2. Forscher der Università di Roma sind mit der Studie *Signals from the Crowd: Uncovering Social Relationships through Smartphone Probes*<sup>9</sup> 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.).

<sup>8</sup> <http://apps.opendatacity.de/relog/>

<sup>9</sup> <http://conferences.sigcomm.org/imc/2013/papers/imc148-barberaSP106.pdf>

3. Die Security Firma Sensepost ging noch einen Schritt weiter. Auf der Blackhat Asia 2014 wurde die *Drohne Snoopy*<sup>10</sup> 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. abreifen konnte, Name und Wohnort der Nutzer ermitteln konnte und die Smartphones über einen längeren Zeitraum tracken konnte. Auf Github 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 WiFi 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.<sup>11</sup>

*We will cookie the street.* (K. Memari, chief executive of Renew)

- Die Firma AdNear experimentiert mit Drohen, welche die Wi-Fi und Baseband Signale der Smartphones auswerten. Anhand der MAC Adresse der WLAN Module der Smartphones werden die Bewegungen der Nutzer verfolgt.<sup>12</sup>

*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.

<sup>10</sup> <http://www.sensepost.com/blog/7557.html>

<sup>11</sup> <http://rt.com/news/trash-bin-surveillance-wifi-402/>

<sup>12</sup> <https://adnear.com/february2015/experimenting-with-drones-for-data-collection.php>

## 19.5 WhatsApp Alternative

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.

Das die NSA die Whatsapp Kommunikation belauschen kann und die Daten an befreundete Geheimdienste weitergibt, überrascht mich nicht. Für den BND und Verfassungsschutz sind diese Daten wahrscheinlich eine Bezahlung für ihre breitwillige Kooperation.<sup>13</sup>

### Anforderungen an einen guten Messenger

Unter Berücksichtigung des Crypto War 3.0 ergeben sich für mich folgende Anforderungen an ein guten Messenger:

1. Sichere Verschlüsselung nach dem aktuellen Stand der Technik:
  - *Forward Secrecy* für die Ende-zu-Ende Verschlüsselung, damit die Geheimdienste bei Kompromittierung des Schlüssels nicht den gesamten, gespeicherten Datenverkehr entschlüsseln können.
  - Sichere Transportverschlüsselung (SSL/TLS) für die notwendige Kommunikation der Apps mit den Servern.
2. Prüfung der Crypto sollte durch unabhängige Experten möglich sein.
3. Keine unerwünschten Uploads von Daten ohne ausdrückliche Bestätigung durch den Nutzer (kein Adressbuch Upload oder ähnliches).
4. Google-freie Installation (via F-Droid) und Google-freier Betrieb sollten möglich sein.
5. Die Server Komponente sollte ebenfalls verfügbar sein (nicht unbedingt kostenlos), damit man einen eigenen Server unabhängig vom Entwickler aufsetzen kann, um Kompromittierung des Dienstes zu erschweren.
6. Benutzbarkeit sollte zumindest brauchbar sein, ist aber kein Hauptkriterium für mich.

### Diskussion der Alternativen (Stand: Sept. 2015)

**TextSecure, Signal 2.0** von WhisperSystems wird von Security-Experten aufgrund der guten Ende-zu-Ende Verschlüsselung empfohlen.

*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. They further added IM like functionality (using IP rather than SMS). (Collin R. Mulliner)*

<sup>13</sup> <http://heise.de/-2687028>

*For the record - @moxie writes crypto software that blinds the #NSA & #GCHQ. He is their nightmare. Usable crypto developer with a backbone!* (Jakob Appelbaum)

Es gibt aber Nachteile, weshalb ich TextSecure nicht mehr empfehle:

- Die Telefonnummern aus dem Adressbuch werden bei der Installation als Hash ungefragt hochgeladen. In einem Blogartikel erklärt M. Marlspike, dass die Hashes der Telefonnummern nur geringen Schutz gegen Angriffe bieten.<sup>14</sup>
- Google-freie Installation und Betrieb sind nicht mehr möglich, da TextSecure die Google Cloud Services (GCS) nutzt und nur im Google Play Store verfügbar ist.
- Nutzung eigener Server ist nicht mehr möglich, seit die Google Cloud Services für den Betrieb genutzt werden.

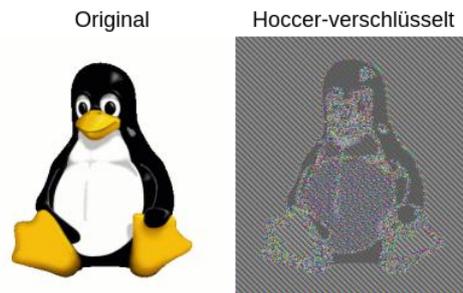
**Threma** ist ein Schweizer Messenger Dienst. Der Upload des Adressbuches erfolgt ausdrücklich nur auf Wunsch des Nutzers. Die Software ist aber nicht Open Source und der Betreiber kontrolliert die Infrastruktur vollständig. Threma könnte zukünftig wie Skype 2004 zur Implementierung von Backdoors verpflichtet werden.

**Hoccer** ist ein deutscher Dienst und der Testsieger 2015 bei der Stiftung Warentest. Die Server stehen alle in Deutschland. Hoccer respektiert die Privatsphäre der Nutzer und schnüffelt nicht in den Adressbüchern rum. Die Software ist ebenfalls nicht Open Source und der Betreiber kontrolliert die Infrastruktur und Software Entwicklung vollständig, was den Dienst ebenfalls anfällig für staatliche Backdoors macht.

Laut Beschreibung auf der Webseite ist die Crypto beschissen schlecht.

- Die Ende-zu-Ende Verschlüsselung ist ohne Forward Secrecy implementiert. Dieses Feature ist heutzutage notwendig, weil man davon ausgehen muss, dass ein Angreifer die gesamte Kommunikation speichern könnte, um sie später zu entschlüsseln, wenn er den private Key in die Hände bekommt. Andere Messenger zeigen, dass Ende-zu-Ende Verschlüsselung mit Forward Secrecy möglich ist.
- Außerdem wird AES256 ohne Block Cipher Mode genutzt. Wenn man ein Bitmap Bild so verschlüsselt, wie die Crypto auf der Webseite von Hoccer beschrieben ist, dann ist das Ergebnis nicht zufriedenstellend.

<sup>14</sup> <https://whispersystems.org/blog/contact-discovery/>



Vielleicht ist Beschreibung auf der Webseite nur buzz word bingo der PR-Abteilung und die Entwickler haben es besser implementiert? Andererseits gab es das schon bei anderen Projekten. BitMessage hat bspw. im Protokoll 1.x die gleichen Fehler bei der AES Implementierung gemacht.

**iMessage** von Apple bietet eine starke Ende-zu-Ende Verschlüsselung, die Apple PR-mäßig laut schreiend vermarktet und selbst auf Anforderung von US-Behörden zur Drogen- und Verbrechensbekämpfung und nicht in Echtzeit knacken kann. Allerdings speicherte der iMessage Backups der Protokolle der Kommunikation unverschlüsselt in der iCloud. Auf diese Daten hat Apple Zugriff und kann sie den Behörden zur Verfügung stellen<sup>15</sup>. Die Speicherung unverschlüsselter Protokolle von verschlüsselter Kommunikation ist ein schwerer Security Bug. Wenn man diese Protokolle auch noch in der eigenen Cloud speichern lässt, dann muss man schon von einer Backdoor sprechen.

Der Security Experte Cyril Cattiaux hat die Verschlüsselung von iMessage en Detail analysiert und weitere Schwächen gefunden. Die Transportverschlüsselung (SSL/TLS) zwischen der App und den Servern arbeitet ohne Certificate Pinning. Das erlaubt man-in-the-middle Angriffe mit gültigen Zertifikaten einer beliebigen Certification Authority wie z.B. Verisign. Certificate Pinning ist heutzutage eine Anforderung für qualitativ starke SSL-Verschlüsselung mit A+ Rating.

**E-Mail** ist das am häufigsten genutzte Medium für Textnachrichten. Als Realitätscheck ein Vergleich mit den genannten Messenger Diensten:

- 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.

*Google has most of my emails, because it has all of yours.*

- Die zusätzliche Installation und Konfiguration von OpenPGP für die Ende-zu-Ende Verschlüsselung ist kompliziert. Es gibt keine Ende-zu-Ende Verschlüsselung mit *Forward Secrecy* für E-Mails.
- Der Austausch von Schlüsseln für OpenPGP oder S/MIME muss per Hand erfolgen, es gibt keinen vertrauenswürdigen Automatismus. Außerdem müssen die Schlüssel per Hand verifiziert werden.

<sup>15</sup> <http://heise.de/-2807703>

- 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 und 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 TextSecure, Threema oder Hoccer erhebliche Vorteile gegenüber E-Mails.

### Meine Empfehlung für Messenger auf dem Smartphone

Ich würde Jabber (XMPP) mit der App **Conversations** empfehlen. Jabber bietet eine dezentrale Infrastruktur, die Software ist Open Source und mit OTR bzw. PGP stehen gute Verfahren für Ende-zu-Ende Verschlüsselung zur Verfügung. Man kann OpenPGP mit OpenKeychain in Kombination mit dem Yubikey NEO für hohe Sicherheitsanforderungen nutzen, um den privaten Schlüssel nicht auf dem unsicheren Smartphone zu speichern (siehe unten).

Die Jabber (XMPP) App **ChatSecure** kann kein OpenPGP verwenden, nur OTR ist für die Ende-zu-Ende Verschlüsselung enthalten. Dafür kann man Tor (OrBot) als Anonymisierungsdienst mit der App nutzen.

## 19.6 Crypto-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 der Nutzer die volle Kontrolle hat. Bei Smartphones kann man nicht davon ausgehen, dass der Nutzer volle Kontrolle über die installierte Software hat.

1. Mit dem Kill Switch hat Google die Möglichkeit, auf Android Handys beliebige Apps zu deinstallieren, zu installieren oder auszutauschen. Auch alternative Mods auf Basis von Android wie cyanogenmod enthalten den Kill Switch, da er nicht im Open Source Teil von Android implementiert ist. Das iPhone<sup>16</sup>, Windows Phone<sup>17</sup> und Amazons Kindle<sup>18</sup> 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.

Hinweis: Die App **SecDroid** deaktiviert den Killswitch auf Android Smartphones. Sie kann aus dem F-Droid Store installiert werden.

2. Jede Crypto-Anwendung benötigt gute Zufallszahlen. Der Zufallszahlengenerator der Android Java VM ist so besch... schlecht, dass man als Angreifer nicht die Kompetenz und Rechenleistung der Crypto-City von

<sup>16</sup> <http://www.engadget.com/2008/08/07/iphone-hacker-says-the-device-calls-home-to-apple-allows-apps/>

<sup>17</sup> <http://heise.de/-1131297>

<sup>18</sup> <http://heise.de/-6887>

Fort Meade braucht. Ganz gewöhnliche Hacker konnten die Schwächen der Android Implementierung im Sommer 2013 nutzen, um Geldbörsen von Bitcoin Nutzern leer zu räumen<sup>19</sup>.

### 3. 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).

### Einige Crypto-Apps

Wer trotzdem ein besseres Gefühl im Bauch hat, wenn die Kommunikation verschlüsselt wird, kann folgende Apps nutzen:

- **CSipSimple** und **Redphone** sind VoIP-Softphones mit ZRTP-Verschlüsselung der Gespräche (siehe Kapitel: VoIP) und für verschlüsselte Textnachrichten.
- **Groundwire** ist ein VoIP-Softphones mit ZRTP-Verschlüsselung und OSTN-Support für das iPhone.
- **Silent Circle** ist ein kommerzielles Projekt von Phil Zimmermann, dass für iPhone und Windows verschlüsselte Internettelefonie bietet.<sup>20</sup>

### 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)*

<sup>19</sup> <http://heise.de/-1933714>

<sup>20</sup> <https://silentcircle.com>

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 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 in das GUI.
  - Der Jabber/XMPP Client **Conversations** kann in Kombination mit OpenKeychain die Chats mit OpenPGP verschlüsseln. (OTR-Verschlüsselung ist auch möglich, der private Key liegt dabei aber auf dem Smartphone.)
2. Den Yubikey NEO bereitet man am einfachsten mit Enigmail auf einem PC vor (siehe: Smartcards). Die OpenPGP Smartcard Funktion ist freizuschalten, die PIN und Admin-PIN ist zu ändern und die Schlüssel sind zu generieren. Man kann diese Schritte aber auch mit OpenKeychain erledigen.
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.

### Anonymisierungsdienste nutzen

Eine allgemeine Einführung zu den JonDonym und Tor Onion Router findet man im Abschnitt Anonymisierungsdienste. An dieser Stelle geht es nur um Besonderheiten für Smartphones. JonDonym und Tor stellen Proxy Clients für Android im Market zur Installation bereit:

- **ANONdroid** wird von der TU Dresden unter Leitung von Dr. Stefan Köpsell für JonDonym entwickelt. Der Client ermöglicht auch die Nutzung der Premium-Dienste von JonDonym mit einem Coupon Code, den man im Webshop von JonDos kaufen kann. Die zu anonymisierenden Internet-Apps müssen die Nutzung eines Proxy unterstützen, da ANONdroid nur einen Proxy bereit stellt, ohne das System zu modifizieren.
- **Orbot** ist ein Tor Client für Android. Er kann anonyme Verbindungen via Tor für alle oder einzelne Internet-Apps erzwingen.
- **Firefox Mobile** kann mit folgenden Add-ons aufgewertet werden:
  - *NoScript anywhere* ist ein Add-on mit vielen Sicherheitsfeatures.<sup>21</sup>
  - *AdBlock Plus für Android* ist kein Add-on für Firefox Mobile, sondern eine separate App, die Werbung und Trackingdienste blockiert.<sup>22</sup>
  - *ProxyMob* ist ein Add-on zur Modifikation der Proxy-Einstellungen von Firefox Mobile.<sup>23</sup>

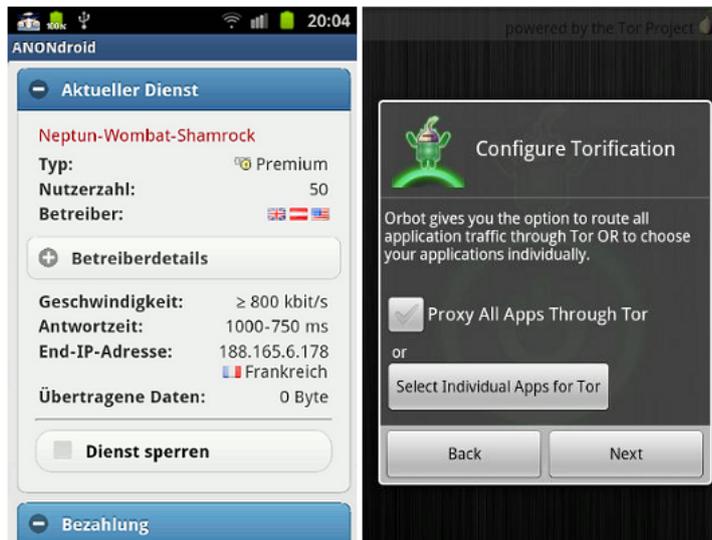


Abbildung 19.2: ANONdroid und Orbot

Die Warnung zu Crypto-Apps aus den Markets gilt auch für Orbot und ANONdroid. Um eine remote Kompromittierung der Proxy Clients zu verhindern, muss die Software außerhalb der Zugriffsmöglichkeiten des Kill Switch installiert werden.

Eine Möglichkeit bietet **Lil'Debi**. Die Software installiert ein minimales Debian GNU/Linux in einer chroot Umgebung. In dieser Linux-Umgebung hat der Nutzer die volle Kontrolle über die installierten Anwendungen<sup>24</sup>.

<sup>21</sup> <http://noscript.net/nsa/>

<sup>22</sup> <https://adblockplus.org/en/android-about>

<sup>23</sup> <https://guardianproject.info/apps/proxymob-firefox-add-on>

<sup>24</sup> <https://guardianproject.info/code/lildebi/>

Da keine grafische Oberfläche zur Verfügung steht, ist man auf die Kommandozeile angewiesen, für Neulinge sicher etwas gewöhnungsbedürftig.

Da im chroot ein vollständiges Debian Linux zur Verfügung steht, kann man die Software aus den Repositories nutzen und wie üblich installieren:

- **Tor** installiert man mit:

```
# aptitude install tor
```

- Für JonDonym kann man den GUI-less **JonDoDaemon** nutzen. Die Installation und Nutzung ist auf der Webseite beschrieben <sup>25</sup>.

---

<sup>25</sup> [https://anonymous-proxy-servers.net/wiki/index.php/JonDoDaemon\\_für\\_Debian](https://anonymous-proxy-servers.net/wiki/index.php/JonDoDaemon_für_Debian)