

Privacy-Handbuch

<https://www.awxcnx.de/handbuch.htm>
Spurenarm Surfen mit Mozilla Firefox,
E-Mails verschlüsseln mit Thunderbird,
Anonymisierungsdienste nutzen
und Daten verschlüsseln
für WINDOWS + Linux

5. November 2012

Inhaltsverzeichnis

1	Scroogled	7
2	Angriffe auf die Privatsphäre	20
2.1	Big Data - Kunde ist der, der bezahlt	21
2.1.1	Google	21
2.1.2	Datenhändler	28
2.2	User-Tracking	29
2.3	Geotagging	31
2.4	Kommunikationsanalyse	33
2.5	Überwachungen im Internet	36
2.6	Rechtsstaatliche Grundlagen	41
2.7	Bundesamt für Verfassungsschutz auflösen	42
2.8	Ich habe doch nichts zu verbergen	44
3	Digitales Aikido	47
3.1	Nachdenken	48
3.2	Ein Beispiel	51
4	Spurenarm Surfen	54
4.1	Auswahl des Webbrowsers	55
4.2	Datensparsame Suchmaschinen	55
4.2.1	Firefox konfigurieren	59
4.3	Cookies	60
4.3.1	Mozilla Firefox konfigurieren	62
4.3.2	Super-Cookies in Firefox	64
4.3.3	Flash-Cookies verwalten	64
4.4	EverCookies	65
4.5	JavaScript	67
4.5.1	NoScript für Mozilla Firefox	68
4.6	Werbung, HTML-Wanzen und Social Media	70
4.6.1	Adblock für Mozilla Firefox	71
4.7	History Sniffing	72
4.8	Risiko Plugins	73
4.8.1	PDF Reader Plugins	73
4.8.2	Weitere Anwendungen	75
4.8.3	Java-Applets	75
4.8.4	Flash und Silverlight	76
4.9	HTTPS nutzen	77

4.10	Vertrauenswürdigkeit von HTTPS	78
4.10.1	Firefox Add-ons	81
4.11	HTTPS Tracking	85
4.12	Starke Passwörter nutzen	86
4.13	HTTP-Header filtern	87
4.14	Snakeoil für Firefox (überflüssiges)	92
5	Bezahlen im Netz	94
5.1	Paysafecard, UKash, Liberty Reserve, Pecunix	95
5.1.1	Anonyme Online-Zahlungen vor dem Aus?	97
5.2	Bitcoin	98
5.2.1	Exchanger / Marktplätze	99
5.2.2	Anonymität von Bitcoin	100
6	Allgemeine Hinweise zur E-Mail Nutzung	103
6.1	Mozilla Thunderbird	103
6.1.1	Mehrere E-Mail Adressen nutzen	104
6.1.2	Wörterbücher installieren	105
6.1.3	Spam-Filter aktivieren	106
6.1.4	Gesicherte Verbindungen zum Mail-Server	106
6.1.5	Sichere Konfiguration des E-Mail Client	108
6.1.6	Datenverluste vermeiden	111
6.1.7	X-Mailer Kennung modifizieren	112
6.1.8	Spam-Schutz	113
6.1.9	Private Note	116
6.1.10	Filelink	117
7	E-Mails verschlüsseln	119
7.1	GnuPG und Thunderbird	121
7.1.1	Installation von GnuPG	121
7.1.2	Installation der Enigmail-Erweiterung	122
7.1.3	Schlüsselverwaltung	123
7.1.4	Signieren und Verschlüsseln erstellter E-Mails	125
7.1.5	Adele - der freundliche OpenPGP E-Mail-Roboter	126
7.1.6	Verschlüsselung in Webformularen	128
7.1.7	GnuPG SmartCard nutzen	129
7.1.8	Web des Vertrauens	133
7.1.9	Schlüssel zurückrufen	135
7.2	S/MIME mit Thunderbird	137
7.2.1	Kostenfreie Certification Authorities	137
7.2.2	Erzeugen eines Zertifikates	138
7.2.3	S/MIME-Krypto-Funktionen aktivieren	139
7.2.4	Zertifikate der Partner und der CA importieren	140
7.2.5	Nachrichten verschlüsseln und signieren	141
7.3	Root-Zertifikate importieren	142
7.3.1	Webbrowser Firefox	143
7.3.2	E-Mail-Client Thunderbird	143
7.4	Eine eigene Certification Authority	144
7.5	Ist S/MIME-Verschlüsselung unsicher?	146
7.6	Eine Bemerkung zum Abschluß	149

8	E-Mail jenseits der Überwachung	151
8.1	Anonyme E-Mail Accounts	151
8.2	alt.anonymous.messages	152
8.3	Mixmaster Remailer	152
8.3.1	Remailer-Webinterface nutzen	153
8.4	Fake Mailer	153
8.5	PrivacyBox der GPF	154
9	Im Usenet spurenarm posten	155
9.1	News-Server	156
9.2	Thunderbird konfigurieren	157
10	Anonymisierungsdienste	158
10.1	Warum sollte man diese Dienste nutzen?	158
10.2	Tor, I2P, Freenet und JonDonym	160
10.2.1	Testergebnisse von Computer-Zeitschriften	164
10.2.2	Finanzierung der Anonymisierungsdienste	165
10.2.3	Security Notes	166
10.3	JonDonym nutzen	168
10.3.1	JonDonym Premium Account einrichten	170
10.3.2	Anonym Surfen mit dem JonDoFox	172
10.4	Tor Onion Router nutzen	175
10.4.1	TorBrowserBundle	176
10.4.2	Anonym Surfen mit Tor	177
10.4.3	Tor Bad Exit Nodes	180
10.4.4	Tor Good Exit Nodes	182
10.4.5	Tor Hidden Services	184
10.5	Anonymous Live-CDs für JonDo und Tor	186
10.6	Anonyme E-Mails mit Thunderbird	188
10.7	Anonym Bloggen	192
10.8	Anonymes Instant-Messaging mit Pidgin	193
10.9	Anonymes Filesharing	194
10.10	Invisible Internet Project	197
10.10.1	Installation des I2P-Routers	197
10.10.2	Konfiguration des I2P-Router	200
10.10.3	Anonym Surfen mit I2P	201
10.10.4	I2P Mail 1 (Susimail)	202
10.10.5	I2P Mail 2 (Bote)	205
10.10.6	I2P IRC	209
10.10.7	I2P BitTorrent	210
10.11	Finger weg von unserösen Angeboten	212
10.11.1	Web-Proxys	212
10.11.2	Free Hide IP	213
10.11.3	5socks.net	213
10.11.4	BlackBelt Privacy, Cloakfish und JanusVM	214
10.11.5	Proxy-Listen	215

11 Daten verschlüsseln	216
11.1 Quick and Dirty mit GnuPG	218
11.1.1 GnuPG für WINDOWS	218
11.2 Truecrypt für WINDOWS	220
11.2.1 Truecrypt installieren	221
11.2.2 Gedanken zum Schlüssel	221
11.2.3 Verschlüsselten Container erstellen	222
11.2.4 Verschlüsselten Container öffnen	223
11.2.5 Verschlüsselten Container schließen	224
11.2.6 WINDOWS komplett verschlüsseln	225
11.2.7 Traveller Disk erstellen	227
11.3 DM-Crypt für Linux	228
11.3.1 Gedanken zum Passwort	229
11.3.2 Verschlüsselten Container erstellen	229
11.3.3 Passwörter verwalten	231
11.3.4 Verschlüsselten Container öffnen/schließen	231
11.3.5 Debian GNU/Linux komplett verschlüsseln	234
11.3.6 HOME-Verzeichnis verschlüsseln	234
11.3.7 SWAP und /tmp verschlüsseln	235
11.4 Backups verschlüsseln	236
11.4.1 Schnell mal auf den USB-Stick	236
11.4.2 Backups mit aespipe verschlüsseln	239
11.4.3 Verschlüsselte Backups mit dar	241
11.4.4 Online Backups	242
12 Daten löschen	245
12.1 Dateien in den Papierkorb werfen	245
12.2 Dateien sicher löschen (Festplatten)	245
12.3 Dateireste nachträglich beseitigen	246
12.4 Dateien sicher löschen (SSDs)	247
12.5 Gesamten Datenträger säubern (Festplatten)	248
12.6 Gesamten Datenträger säubern (SSDs)	249
13 Daten anonymisieren	250
13.1 Fotos und Bilddateien anonymisieren	250
13.2 PDF-Dokumente säubern	251
13.3 Metadata Anonymisation Toolkit (MAT)	251
14 Daten verstecken	254
14.1 steghide	256
14.2 stegdetect	256
15 Internettelefonie (VoIP)	258
15.1 Open Secure Telephony Network (OSTN)	259
16 Smartphones	263
16.0.1 Crypto-Apps	265
16.0.2 Anonymisierungsdienste nutzen	266

17 Umgehung von Zensur	268
17.1 Strafverfolgung von Kinderpornografie	272
17.2 Die Medien-Kampagne der Zensursula	274
17.3 Löschen statt Sperren ist funktioniert	275
17.4 Simple Tricks	276
17.5 Unzensierte DNS-Server nutzen	278
17.5.1 WINDOWS konfigurieren	280
17.5.2 Linux konfigurieren	281
17.5.3 DNS-Server testen	283
18 Lizenz und Spenden	285
18.1 Spenden	285

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 einzuschießen. Es geht ja auch nicht um P.I.I." - persönlich identifizierende Information, der toxische Smog der Informationsära - "sondern bloß um Metadaten. Also ist es bloß ein bisschen böse."

"Warum dann all die Heimlichtuerei?"

Maya seufzte und umarmte den Labrador, dessen gewaltiger Kopf auf ihrem Knie ruhte. "Die Schlapphüte sind wie Läuse - die sind überall. Tauchen sogar in unseren Konferenzen auf, als wären wir in irgendeinem Sowjet-Ministerium. Und dann die Sicherheitseinstufungen - das spaltet uns in zwei Lager: solche mit Bescheinigung und solche ohne. Jeder von uns weiß, wer keine Freigabe hat, aber niemand weiß, warum. Ich bin als sicher eingestuft - zum Glück fällt man als Lesbe nicht mehr gleich automatisch durch. Keine sichere Person würde sich herablassen, mit jemandem essen zu gehen, der keine Freigabe hat."

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

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

"Was ist denn?"

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

"Ähm, du bist nicht zufällig in einer terroristischen Vereinigung?"

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

"Sagtest du nicht, die Gerichte würden das nicht erlauben?"

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

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

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

Sie schwiegen eine Minute lang.

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

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

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

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

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

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

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

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

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

“... verraten und vergoogelt.”

“Voll und ganz”, nickte sie.

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

“Ich kann die Sache in Ordnung bringen”, presste sie flüsternd hervor. “Als die Chinesen mit den Verhaftungen 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 schnüffelt in Gmail-Konten?"

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

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

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

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

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

“Über den Googleputzer?”

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

“Jesus.”

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

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

“Wir müssen jetzt los”, beharrte sie.

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

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

“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 erwischte - 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 keiner 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...

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.

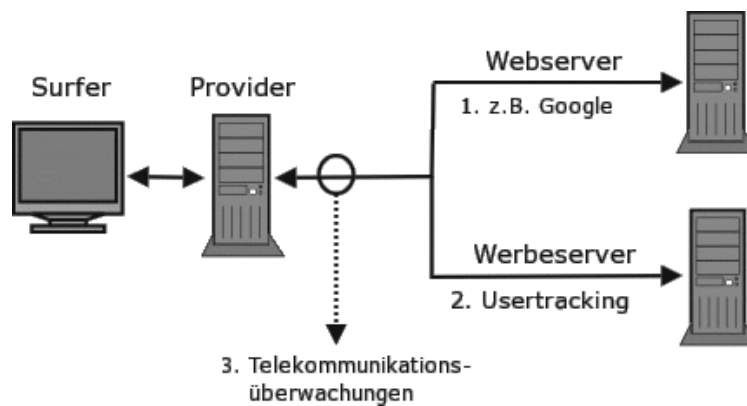


Abbildung 2.1: Möglichkeiten zur Überwachung im WWW

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 Bild 2.2 zur Besucherstatistik wurde vom Google Ad-Planner für eine (hier nicht genannte) Website erstellt. Man erkennt, dass der überwiegende

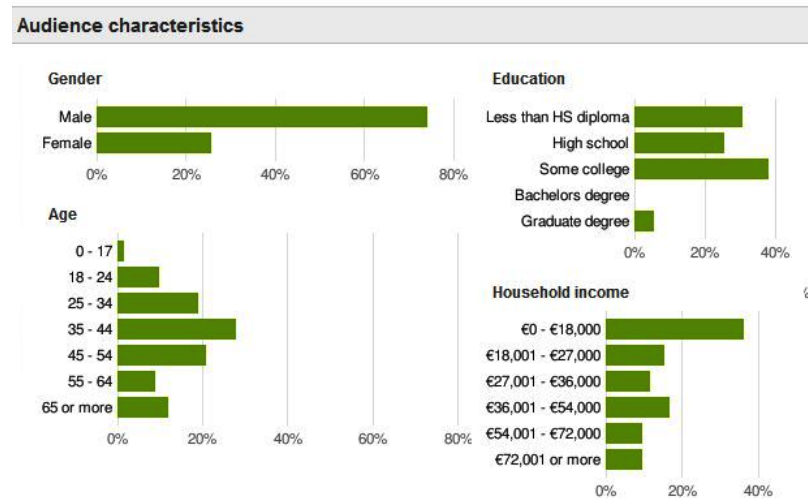


Abbildung 2.2: Ad-Planner Besucherstatistik (Beispiel)

gende Anteil der Besucher männlich und zwischen 35-44 Jahre alt ist. (Die Informationen zu Bildung und Haushaltseinkommen müssen im Vergleich zu allgm. 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 unsicher 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 sucht mit dem Smartphone Betriebssystem Android auf dem Markt der mobilen Kommunikation ähnliche Erfolge wie im Web.

Das erste Google Handy *G1* war ein in Hardware gegossenes Pendant zum Webbrowser Google Chrome. Bei der Markteinführung versuchte Google die Nutzer mit dem ersten Einschalten zu überreden, einen Google-Account anzulegen. Ohne Account bei Google ging fast nichts mit dem Hightech-Spielzeug, nur Telefonieren war möglich. Dieses Feature wurde auf Druck der Nutzer deaktiviert.

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).

Inzwischen ist die feste Bindung an Google-Dienste unter Android etwas gelockert. Aber nach wie vor sind diese als Standard voreingestellt und werden aus Bequemlichkeit sicher von der Mehrzahl der Nutzer verwendet.

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:

- Google ist die einzige allgemeine Suchmaschine, die unbedarften Nutzern zur Verfügung steht. Alternativen sind standardmäßig nicht vorhanden und müssen von den Nutzer aktiv gesucht und installiert werden.
- Die Default-Startseite ermöglicht es Google, ein langlebiges Cookie zu setzen und den Browser damit praktisch zu personalisieren.
- Sollte die Startseite modifiziert werden (z.B. bei der Variante *Icetweasel* von Debian GNU/Linux), 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 erfolgreiche 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 von 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 Behörden und Geheimdiensten

Es wäre verwunderlich, wenn die gesammelten Datenbestände nicht das Interesse der Behörden und Geheimdienste wecken würden. Google kooperiert auf zwei Ebenen:

1. 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

2. Außerdem kooperiert Google mit der CIA bei der Auswertung der Datenbestände im Rahmen des Projektes *Future of Web Monitoring*, um Trends und Gruppen zu erkennen und für die Geheimdienste der USA zu erschließen. Es besteht der Verdacht, dass Google auch mit der NSA kooperiert. Das EPIC bemüht sich, Licht in diese Kooperation zu bringen. Anfragen wurden bisher nicht beantwortet. Nach Informationen des Whistleblowers W. Binney, der 30 Jahre in führenden Positionen der NSA gearbeitet hat, wird Google ab Herbst 2012 Kopien des gesamten E-Mail Verkehrs von Gmail und sämtliche Suchanfragen dem neuen Datacenter der NSA in Bluffdale zur Verfügung stellen.

It will store all Google search queries, e-mail and fax traffic and so on.

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 (selbständigen?) 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 Mikrossoft 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. Im Rahmen der Zusammenarbeit mit FBI und CIA führten die Daten von Acxiom mehrfach zu Anklagen und Abschiebungen (nach Aussage eines leitenden Mitarbeiters).

Acxiom prahlt damit, präzise Daten über 96% der amerikanischen Bevölkerung zu haben. Jeder Datensatz hat 1.500 Datenpunkte (Stand 2010). Neben Daten zur Internetnutzung verarbeitet Acxiom auch Kreditkartenrechnungen, Apothekenrechnungen und andere Daten aus der realen Welt.

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

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, verarbeitet aber auch 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
- ...

Eine Analyse des Wall Street Journal hat sich näher mit den Datensammlungen Firma beschäftigt ¹.

2.2 User-Tracking

Viele Dienste im Web nutzen die Möglichkeiten, das Surfverhalten zu verfolgen, zu analysieren und die gesammelten Daten zu versilbern. Die dabei entstehenden Nutzerprofile sind inzwischen sehr aussagekräftig. Wie das Wall Street Journal in einer Analyse beschreibt, können das Einkommen, Alter, politische Orientierung und weitere persönliche Daten der Surfer eingeschätzt werden oder die Wahrscheinlichkeit einer Kreditrückzahlung. Hauptsächlich werden diese Daten für Werbung genutzt. Ein Online-Versand von Brautkleidern möchte Frauen im Alter von 24-30 Jahren ansprechen, die verlobt sind. Das ist heute möglich.

Es geht aber längst nicht nur um die Einblendung von Werbung. Sarah Downey warnt ² 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 der Windows Nutzern angeboten werden.³.

Häufig werden *Werbeeinblendungen* für das User-Tracking genutzt. Die in Webseiten dargestellte Werbung wird nur von wenigen Anbietern zur Verfügung gestellt. Diese verwenden verschiedene Möglichkeiten, um Surfer zu erkennen, das Surfverhalten Website-übergreifend zu erfassen und anhand dieser Daten Nutzerprofile zu generieren. Für die Auswertung werden nicht nur die besuchten Websites genutzt. Besonders aussagekräftig sind die Klicks auf Werbung. S. Guha von Microsoft und B. Cheng sowie P. Francis vom Max-Planck-Institut für Software Systeme beschreiben in einer wiss. Veröffentlichung, wie man homosexuelle Männer anhand der Klicks auf Werbung

¹ <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html>

² <http://heise.de/-1628313>

³ <http://heise.de/-1626368>

erkennen kann. Das Verfahren kann für verschiedene Fragestellungen angepasst werden.

Neben Werbung und Cookies werden auch *HTML-Wanzen* (sogenannte *Webbugs*) für das Tracking eingesetzt. Dabei 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, werden beim Betrachten einer Webseite oder Öffnen der E-Mail vom externen Server geladen und hinterlassen in den Logs des Servers Spuren für eine Verfolgung des Surfverhaltens.

Außerdem gibt es spezielle Tracking-Dienste wie Google Analytics, die Javascript und *EverCookie* Techniken nutzen.

Gesetzliche Schranken scheint man großflächig zu ignorieren. Die Universität Karlsruhe hat eine Studie veröffentlicht, die zu dem Ergebnis kommt, dass nur 5 von 100 Unternehmen im Internet geltende Gesetze zum Datenschutz respektieren. Der Nutzer ist also auf Selbstschutz angewiesen.

Tracking von Dokumenten

Die Firma ReadNotify bietet einen Service, der E-Mails, Office-Dokumente und PDF-Dateien mit speziellen unsichtbaren Elementen versieht. Diese werden beim Öffnen einer E-Mail oder eines 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.

Die Markierung von E-Mail Newslettern ist relativ weit verbreitet, aber nicht immer legal. Es wird nicht nur im kommerziellen Bereich verwendet. Auch die CDU Brandenburg markierte ihre Newsletter über einen längeren Zeitraum, um zu überprüfen, wann und wo sie gelesen wurden.

Nutzen der Informationen für Angriffe

Neben der unerwünschten Protokollierung der Daten besteht die Gefahr, dass böswillige Betreiber von Websites die Informationen über die verwendeten Versionen der Software gezielt ausnutzen, um mittels bekannter Exploits (Sicherheitslücken) Schadensroutinen einzuschleusen und damit die Kontrolle über den Rechner zu erlangen.

Derartig übernommene Rechner werden häufig als Spamschleuder missbraucht oder nach sensiblen Informationen (z.B. Kontodaten) durchsucht. Es sind auch gezielte Anwendungen zur Spionage bekannt. Das von chinesischen Hackern mit manipulierten PDF-Dokumenten aufgebaute Ghostnet konnte 2008 erfolgreich die Computersysteme von westlichen Regierungen und des Dalai Lama infizieren. Eine Analyse des Kontrollzentrums Ghost RAT zeigte die umfangreichen Möglichkeiten der Malware. Es konnten Keylogger installiert werden, um an Bankdaten und Passwörter zu gelangen, das Mikrofon konnte für die Raumüberwachung genutzt werden.....

2.3 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, das sie sich häufig im Umkreis von xx aufhalten. Gezielte 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*⁴.

Das Magazin Wired berichtete im Danger Room (Oktober 2011), dass das FBI Smartphones bereits seit Jahren mit der Zielstellung der "Durchleuchtung der Gesellschaft" trackt. Muslimisch 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*⁵.

Datensammlung

Die Daten werden mit verschiedenen Methoden gesammelt:

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

⁴ <http://www.heise.de/tr/artikel/Immer-im-Visier-276659.html>

⁵ <http://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims>

- 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 spezifiziert⁶.

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.

- 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.)



Abbildung 2.3: Lokalisierung eines Smartphone durch Facebook

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

- Lokalisierungsdienste wie *Gowalla* oder *Foursquare* bieten öffentlich einsehbare Standortdaten und versuchen, durch spielartigen Charakter

⁶ <http://www.apple.com/chde/legal/privacy/>

neue Nutzer zu gewinnen. Im Gegensatz zu den oben genannten Datensammlungen kann man bei Gowalla oder Foursquare aber gut kontrollieren, welche Daten man veröffentlicht oder die Dienste nicht nutzen.

Nichts zu verbergen?

Wer ein praktisches Beispiel braucht: 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.⁷

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.⁸

2.4 Kommunikationsanalyse

Geheimdienste verwenden seit Jahren die Kommunikations-Analyse (wer mit wem kommuniziert), um die Struktur von Organisationen aufzudecken. Teilweise gelingt es damit, die Verschlüsselung von Inhalten der Kommunikation auszuhebeln und umfangreiche Informationen zu beschaffen.

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

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

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

⁷ <http://www.magnus.de/news/krankengeld-gestrichen-wegen-verfaenglichen-facebook-bildern-208271.html>

⁸ http://www.unwatched.org/20120601_Unachtsamer_Umgang_mit_Facebook_kann_unangenehme_Folgen_haben

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 *Schulenfalle*, 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...

Für unser Beispiel geben wir der Gruppe den 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 2.4). Dabei wird nicht nur einfache Anzahl der Kommunikationsprozesse ausgewertet, es wird auch die zeitliche Korrelation einbezogen.

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

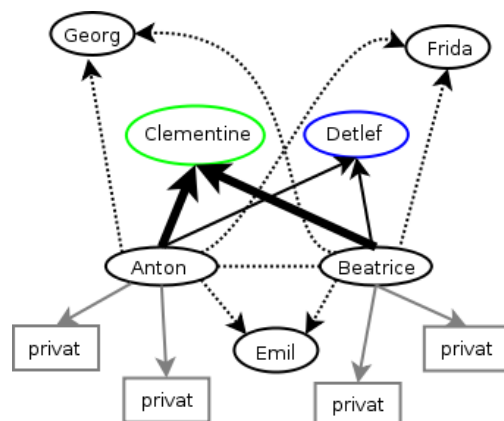


Abbildung 2.4: Soziales Netz von Anton und Beatrice

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

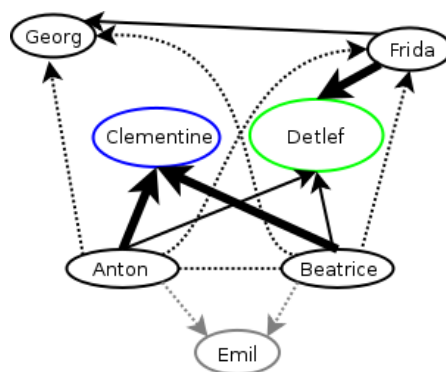
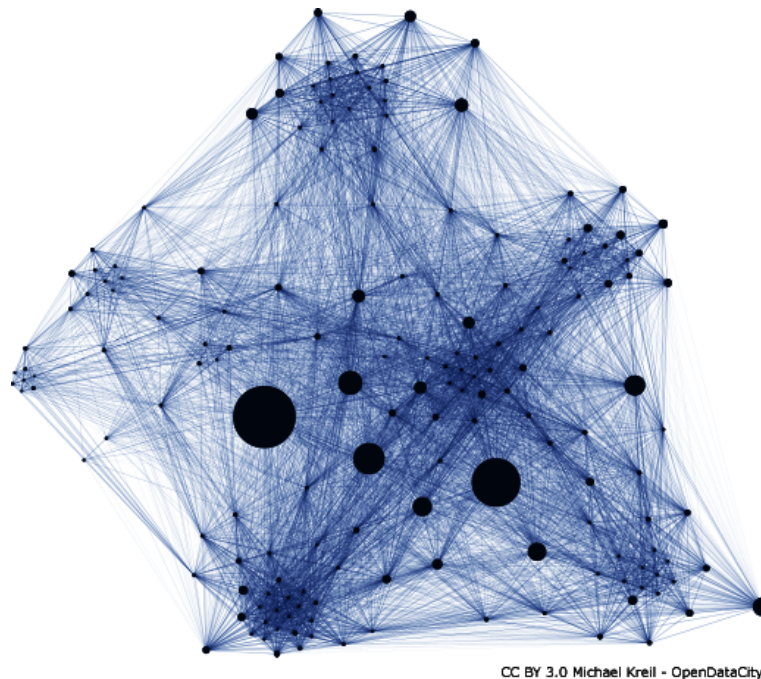


Abbildung 2.5: Präzisierte Struktur der "mg"

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 2.6 erstellt.



CC BY 3.0 Michael Kreil - OpenDataCity

Abbildung 2.6: Kommunikationsnetzwerk von Malte Spitz

2.5 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!**⁹

Vorratsdatenspeicherung oder Mindestspeicherfrist: 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

⁹ <http://www.dubistterrorist.de>

ein Rechtsgutachten mit schweren Bedenken gegen die VDS vorgelegt.

Ein Vergleich der Zahlen der Kriminalitätsstatistik des BKA für die Jahre 2007, 2008 und 2009 zeigt, dass die VDS im Jahr 2009 nicht zur einer Verbesserung der Aufklärungsrate von Straftaten im Internet führte und dass die Aufklärungsrate der Straftaten mit Internetbezug deutlich höher als der Durchschnitt ist.

	2007 (o. VDS)	2008 (o. VDS)	2009 (mit VDS)
Gesamtzahl der Straftaten	6.284.661	6.114.128	6.054.330
Aufklärungsrate (gesamt)	55.0%	54.8%	55.6%
Straftaten im Internet	179.026	167.451	206.909
Aufklärungsrate (Internet)	82.9%	79.8%	75.7

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.

Wie schlecht die Sicherheit der Datenberge von den Providern gewährleistet wird, zeigt ein Beispiel aus Dortmund. Eine rechtsextremistische Aktivistin arbeitete in einem Call-Center eines Mobilfunk Anbieters als Telefonistin. Scheinbar ist es recht üblich, dass Call-Center-Mitarbeiter Zugriff auf Stammdaten der Kunden und teilweise auf Verbindungsdaten haben. Die Telefonistin besorgte Informationen über alternative Jugendliche, die dann zusammengeschlagen wurden.

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 überprüft und für falsch befunden¹⁰.

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 *Zugangerschwerernsgesetz* verabschiedet. Alle Provider mit mehr als 10.000 Kunden sollen

¹⁰ <http://blog.odem.org/2009/05/quellenanalyse.html>

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 ¹¹.
5. Die Auswertung des eco Verband zeigt, dass Webseiten mit dokumentiertem Missbrauch effektiv gelöscht werden können. 2010 wurden 99,4% der gemeldeten Webseiten gelöscht ¹².
6. Im Herbst 2011 wurde das Gesetz offiziell beerdigt.

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

Die verfassungsrechtlichen Bedenken gegen die Zensur hat der wissenschaftliche Dienst des Bundestages in einem Gutachten zusammengefasst ¹³. Auch eine Abschätzung der EU-Kommision kommt zu dem Schluss, dass diese Sperrmaßnahmen **notwendigerweise eine Einschränkung der Menschenrechte voraussetzen**, beispielsweise der freien Meinungsäußerung.

BKA Gesetz: Mit dem BKA Gesetz wurde eine Polizei mit den Kompetenzen eines Geheimdienstes geschaffen. Zu diesen Kompetenzen gehören neben der heimlichen Online-Durchsuchung von Computern der Lauschangriff außerhalb und innerhalb der Wohnung (incl. Video), Raster- und Schleierfahndung, weitgehende Abhörungsbefugnisse, 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.

¹¹ <http://ak-zensur.de/2010/08/kapitulation.html>

¹² http://www.eco.de/verband/202_8727.htm

¹³ http://netzpolitik.org/wp-upload/bundestag_filter-gutachten.pdf

Damit wird sich das BKA bis zu einem gewissen Grad jeglicher Kontrolle, der justiziellen und erst recht der parlamentarischen, entziehen können ¹⁴.

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.)

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...

¹⁴ <http://www.berlinonline.de/berliner-zeitung/print/politik/725127.html>

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 umfassen 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.

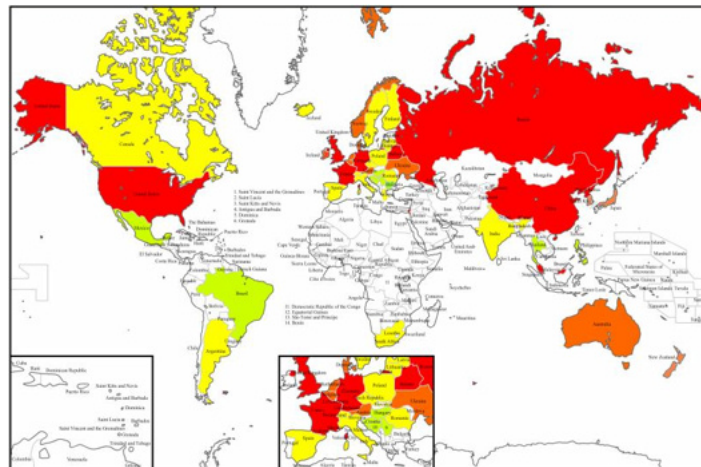


Abbildung 2.7: Vergleich der elektronischen Polizeistaaten

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 Kinderpornografie...* (05.03.2009)

2.6 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 und das Gutachten des Bundesdatenschutzbeauftragten zum *Staatstrojaner* zeigen deutlich die gesellschaftlichen Defizite bei der Begrenzung der Überwachung.

Der teilweise erfolgreiche Widerstand der Zivilgesellschaft gegen Vorratsdatenspeicherung, Zugangserschwerenissetz, Online Durchsuchung, Großer Lauschangriff usw. reicht nicht aus. Die gesellschaftlich ausgehandelten Normen (Gesetze, Urteile des BVerfG...) zur Begrenzung der Überwachung werden nicht respektiert und scheinbar 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, das wir unser Ok 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 scheinbar in einem "rechtsfreien Raum". Übertretungen der zulässigen Grenzen haben keine oder (bei starkem öffentlichen Druck) harmlose Konsequenzen.
3. 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?

4. 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 ¹⁵
- Razzien im Vorfeld des G8-Gipfels waren rechtswidrig ¹⁶
- Konstruieren und schnüffeln mit §129a ¹⁷
- Durchsuchung beim LabourNet waren rechtswidrig ¹⁸

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

2.7 Bundesamt für Verfassungsschutz auflösen

Es wird Zeit, das Bundesamt für Verfassungsschutz aufzulösen. Die Humanistische Union fordert bereits seit 20 Jahren die Auflösung dieses Inlandgeheimdienstes. 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 der Polizei.

V-Leute sind keine Lösung, sondern das Problem

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)

- V-Leute des Verfassungsschutz 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 Entarnung vom Verfassungsschutz ins Ausland gebracht wurde. ¹⁹
- 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. ²⁰

¹⁵ <http://de.indymedia.org/2008/10/228421.shtml>

¹⁶ <http://www.ag-friedensforschung.de/themen/Globalisierung/g8-2007/bgh.html>

¹⁷ <http://www.neues-deutschland.de/artikel/175230.konstruieren-und-schnueffeln-mit-s-129a.html>

¹⁸ <http://www.labournet.de/ueberuns/beschlagnahme/index.html>

¹⁹ <http://www.heise.de/tp/blogs/8/151641>

²⁰ <http://www.heise.de/tp/artikel/31/31120/1.html>

- Der Verfassungsschutz hat die rechtsradikale Szene nicht unterwandert, sondern finanziell unterstützt und vor Strafverfolgung geschützt.
 - Laut einem BKA-Report ²¹ 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 wurde zu spät an die Polizei weitergeleitet, so dass rechtsradikale Aktionen nicht mehr verhindert werden konnten.
 - 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:²²

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. Auf Veranlassung des Innenministers Dr. Ingo Wolff wurden auch Anklagen gegen die Mitarbeiter des Verfassungsschutz wegen Geheimnisverrats und Strafvereitelung eingestellt.²³

Das ist seit mehreren Jahren bekannt. Konsequenzen? Keine!

- Die mit viel Brimborium verurteilte *Sauerländer Terrorzelle* wurde vom V-Mann Mevlüt Kar gegründet und für die Vorbereitung *gigantischer Terroranschläge* mit Sprengzündern usw. versorgt. Die Sauerlandgruppe war der dritte Versuch von Mevlüt Kar, eine Terrorzelle aufzubauen und an die Behörden zu verraten. M. Kar wurde nie angeklagt.²⁴
 - 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.
- Ein weiterer V-Mann des Verfassungsschutz 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 Erstarben salafitischer Gruppen beigetragen.²⁵

²¹ <http://www.spiegel.de/panorama/justiz/verfassungsschutz-soll-rechte-v-leute-vor-straftverfolgung-geschuetzt-haben-a-865154.html>

²² <https://www.taz.de/Neonazi-Ermittlungen/!103340/>

²³ <http://www.nadir.org/nadir/initiativ/azzoncao/donazi3.html>

²⁴ <http://www.heise.de/tp/artikel/35/35986/1.html>

²⁵ <http://www.heise.de/tp/blogs/8/150854>

- 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 P. soll monatlich 2.500 - 3.000 Euro vom Verfassungsschutz erhalten haben. Gegen den V-Mann wurde ebenfalls keine Anklage erhoben.²⁶
- Die Rolle des Verfassungsschutz bei den systematischen Pannen im Rahmen der Ermittlungen zur *rechtsradikalen NSU Terrorzelle* wird sicher nicht vollständig aufgeklärt werden.

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

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 überwacht²⁷
- Verfassungsschutz in Bayern überwacht die linke Szene²⁸
- Überwachung einer linken Gruppe durch Verfassungsschutz²⁹
- Verfassungsschutz bespitzelt linke Abgeordnete³⁰
- Gegner von Stuttgart21 vom Verfassungsschutz überwacht³¹
- mg-Überwachung durch den Verfassungsschutz war illegal³²
- Ohne demokratische Kontrolle (BfV in Bayern)³³

2.8 Ich habe doch nichts zu verbergen

Dies Argument hört man oft. Haben wir wirklich nichts zu verbergen? Einige Beispiele sollen exemplarisch zeigen, wie willkürlich gesammelte Daten unser Leben gravierend beeinflussen können:

- Im Rahmen der Zulässigkeitsprüfung für Piloten wurde Herr J. Schreiber mit den vom Verfassungsschutz gesammelten Fakten konfrontiert³⁴:
 1. Er wurde 1994 auf einer Demonstration kontrolliert. Er wurde nicht angezeigt, angeklagt oder einer Straftat verdächtigt, sondern nur als Teilnehmer registriert.

²⁶ <http://www.heise.de/tp/blogs/8/150854>

²⁷ <http://heise.de/-217246>

²⁸ <http://www.heise.de/tp/artikel/35/35942/1.html>

²⁹ <http://www.heise.de/tp/blogs/8/151499>

³⁰ <http://www.heise.de/tp/artikel/36/36316/1.html>

³¹ <http://www.bei-abriss-aufstand.de/2012/02/25/>

³² <http://annalist.noblogs.org/post/2012/03/03/>

³³ <http://www.heise.de/tp/artikel/35/35942/1.html>

³⁴ <http://www.pilotundflugzeug.de/artikel/2006-02-10/Spitzelstaat>

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.³⁵
- 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.³⁶

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.³⁷

- "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.

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.

³⁵ <http://blog.kairaven.de/archives/998-Datenstigmaanekdote.html>

³⁶ <http://www.lawblog.de/index.php/archives/2008/03/11/>

³⁷ http://en.wikipedia.org/wiki/Operation_Ore

Politische Aktivisten

Wer sich politisch engagiert und auf gerne vertuschte Mißstände hinweist, hat besonders unter der Sammelwut staatlicher Stellen zu leiden. Wir möchte jetzt nicht an Staaten wie Iran oder China mäkeln. 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”*³⁸ 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.

³⁸ <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:** Zensur umgehen. Immer mehr Länder führen Zensurmaßnahmen ein, um den Zugriff auf unerwünschte Inhalte zu sperren. Mit den *Simple Tricks* oder unzensierten DNS-Servern können diese Sperren umgangen werden.
- **2. 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...)
- **3. Grad:** Anhand der IP-Adresse ist ein Nutzer eindeutig identifizierbar. Im Rahmen der Vorratsdatenspeicherung werden diese Daten für 6 Monate gespeichert. Mixkaskaden (JonDonym) oder Onion Router (Tor) bieten eine dem realen Leben vergleichbare Anonymität. Remailer bieten die Möglichkeit, den Absender einer E-Mail zu verschleiern.
- **4. Grad:** Eine noch höhere Anonymität bietet 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 bei einem Provider, der die Vorratsdatenspeicherung (VDS) umsetzt.
3. Eine anonyme/pseudonyme E-Mail Adresse bei einem ausländischen Provider, der nicht zur Vorratsdatenspeicherung verpflichtet ist.
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.)

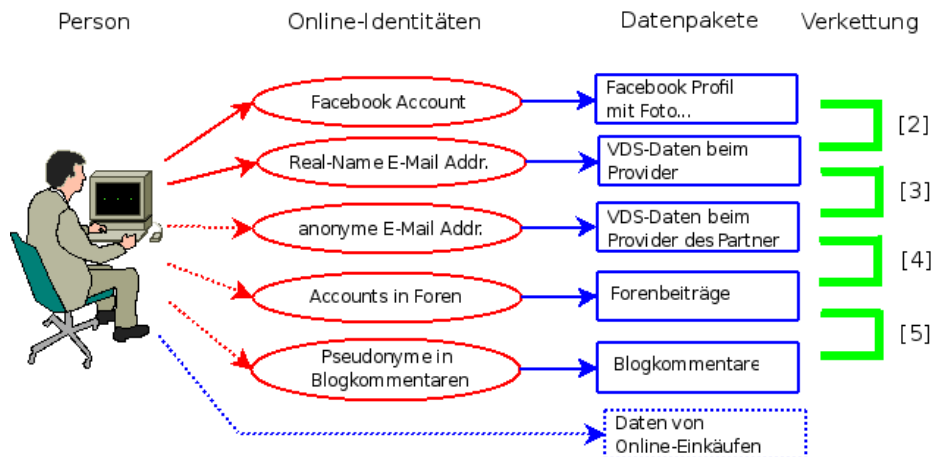


Abbildung 3.1: Datenverknüpfung

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 kann mit anderen Einträgen von Cookies oder User-Tracking-Systemen zeitlich korreliert werden und so können den Profilen die Mail-Adressen und reale Namen zugeordnet werden.
- Von dem anonymen E-Mail Postfach findet man VDS-Daten bei den Empfängern der E-Mails. Diese Datenpakete enthalten einen Zeitstempel sowie die IP-Adresse und E-Mail Adresse des Absenders und können mit weiteren Daten 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-Einkäufeln erfordern in der Regel 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 Freundschaftbeziehungen gibt es auch viele Fotos. Dieser Datenpool ist schon sehr umfangreich:
 - Wirtschaftswissenschaftler haben eine Methode vorgestellt, um Meinungsmacher und kreative Köpfe in Online-Communities zu identifizieren ¹.
 - MIT-Studenten erkennen homosexuelle Neigungen ihrer Kommilitonen anhand der Informationen über Freundschaften in den Facebook-Profilen ².
 - Der Grünen-Vorsitzende Özdemir pflegte eine Freundschaft mit dem Intensivstraftäter Muhlis Ari, ist in seinem Facebook-Profil erkennbar ³.
2. Dem Facebook Profil kann man durch Kombination mit anderen Datenkrümel 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

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

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

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

Person zugeordnet werden. Ein einzelner passender Datensatz reicht aus. (Wenn nicht konsequent Anonymisierungsdienste für das anonyme Postfach verwendet werden.)

4. Die Verbindung zwischen anonymer E-Mail Adresse und Foren Account ergibt sich durch die Nutzung der E-Mail Adresse bei Anmeldung.
5. Durch Vergleiche von Aussagen und Wortwahl lassen sich Korrelationen zwischen verschiedenen Nicknamen in Foren und Blogs herstellen. Dem Autor sind solche Korrelationen schon mehrfach offensichtlich ins Auge gesprungen und konnten durch Nachfrage verifiziert werden.
6. Durch Datenschutzpannen können Informationen über Online-Einkäufe mit anderen Daten verknüpft werden. Dabei schützt es auch nicht, wenn man sich auf das Gütesiegel des TÜV Süd verlässt und bei einem Händler einkauft, der bisher nicht negativ aufgefallen ist. Eine kleine Zusammenfassung vom 29.10.09 bis 04.11.09:
 - Die Bücher der Anderen (500.000 Rechnungen online einsehbar ⁴)
 - Die Libris Shops (Zugang zu Bestellungen von 1000 Buchshops ⁵)
 - Sparkassen-Shops (350.000 Rechnung online einsehbar ⁶)
 - Acht Millionen Adressen von Quelle-Kunden sollen verkauft werden ⁷)

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

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

- Die Datensammlungen werden mit kommerziellen Zielen ausgewertet, um uns zu manipulieren und unsere Kauf-Entscheidungen 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?*

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

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

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

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

– Personalchef: *Die Fotos in ihrem Facebook-Profil ...*

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

- Von der israelischen Armee ist bekannt, dass sie die Profile in sozialen Netzen überprüfen, wenn Frauen den Wehrdienst aus religiösen Gründen verweigern. Zur Zeit verweigern in Israel 35% der Frauen den Wehrdienst. Anhand der sozialen Netze wird der Lebenswandel dieser Frauen überprüft. Es werden Urlaubsfotos in freizügiger Bekleidung gesucht oder Anhaltspunkte für Essen in einem nicht-koscheren Restaurant. Auch aktiv wird dabei gehandelt und Fake-Einladungen zu einer Party während des Sabbats verschickt.
- Firmen verschaffen sich unrechtmäßig Zugang zu Verbindungs- und Bankdaten, um ihrer Mitarbeiter auszuforschen. (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 ⁸.
- Mit dem Projekt INDECT hat die EU ein Forschungsprojekt gestartet und mit 14,8 Mio Euro ausgestattet, um unsere Daten-Spuren für Geheimdienste zu erschließen ⁹.

Ich habe doch nichts zu verbergen...

...oder habe ich nur zu wenig Fantasie, um mir die Möglichkeiten der Datensammler 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

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

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

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

Bedeutung der Pseudonyme

Die Suche nach Informationen über F. fiel relativ leicht. Sie verwendete die gleichen Pseudonyme mehrfach und die Pseudonyme waren eindeutig und einfach zu googeln. Damit ergeben sich viele Verknüpfungen von einzelnen Informationshäppchen. Als Verteidigung gegen diese Recherche kann man viele unterschiedliche Pseudonyme verwenden oder zumindest schwer googelbare Pseudonyme, wenn man wiedererkannt werden möchte.

Die Wiedererkennbarkeit lässt sich messen. Auf der Website *How unique are your usernames?* ¹⁰ kann man den Entropiewert seiner bevorzugten Pseudonyme berechnen lassen. Gute und schwer googelbare Pseudonyme haben Entropiewerte < 20. Werte über 40 sind sehr eindeutig und die damit verbunden Informationen somit leicht verknüpfbar.

¹⁰ <http://planete.inrialpes.fr/projects/how-unique-are-your-usernames>

Kapitel 4

Spurenarm Surfen

Bild 4.1 zeigt ein Konzept für anonymes Surfen:

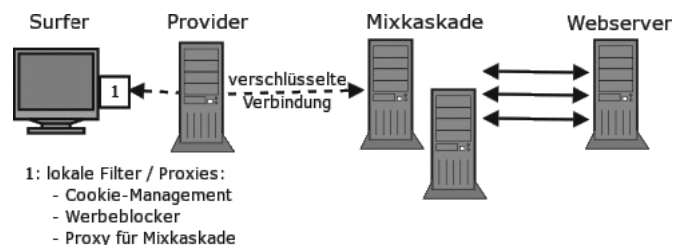


Abbildung 4.1: Konzept für anonymes Surfen

1. Die Nutzung datensammelnder Webangebote kann man vermeiden.
2. Die Annahme von Cookies und die Ausführung von JavaScript wird auf vertrauenswürdige Websites eingeschränkt.
3. Werbung, HTML-Wanzen und die Like-Buttons (mit den Social Networks Daten sammeln) werden durch Filter blockiert.
4. Verräterische Informationen des Browsers werden entfernt.
5. Risikoreiche und Privacy-unfreundliche Features wie PDF-Reader Plug-Ins, Browser History, Geolocation usw. werden deaktiviert.
6. HTTPS-Zertifikate werden zusätzlich validiert, um Man-in-middle Angriffe zu erschweren.
7. Der Datenverkehr kann über einen Anonymisierungsdienst geleitet werden. Die verschlüsselte Kommunikation verhindert auch die Auswertung des Internetverkehrs durch mitlesende Dritte wie z.B. unsichere WLAN-Hotspots oder TKÜV. (siehe *Anonymisierungsdienste nutzen*)

Mit diesen Maßnahmen kann es vorkommen, dass Websites nicht wie erwartet funktionieren. Gute Webdesigner verzichten auf suspekte 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 hilft kann man Javascript gezielt für einzelne Server freigeben. 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 ¹ für fast alle Betriebssysteme zum Download bereit. Linux-Distributionen enthalten den Browser in der Regel.

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 separaten Repository ² bereit.

Firefox kann durch viele von der Community entwickelte Add-ons und Anpassungen in der Konfiguration zu einem sicheren und privacy-freundlichen Browser aufgewertet werden. Ich beschränke mich im folgenden auf diesen einen Browser. Das ist schon sehr umfangreich, wenn man es gut machen will.

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.

¹ <http://www.mozilla-europe.org/de/firefox>

² <http://mozilla.debian.net>

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, die auch SSL-Verschlüsselung bietet. Sie legt nicht so starken Wert auf neueste Trends wie Google. Die Ergebnisse sind oft älter. Damit ist DuckDuckGo vor allem für trend-unabhängige Fragen geeignet.
- Neben der eigentlichen Suche bietet DuckDuckGo viele nette Erweiterungen ³. 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.
- **Blekko** (<https://blekko.com>)
Blekko hatte als erste Suchmaschine eine gute Lösung gegen Spam. Allerdings bietet sie keine Einschränkung auf bestimmte Sprachen. In den Ergebnissen dominieren englische Seiten. Die IP-Adressen der Nutzer werden nach 48h gelöscht.
- **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.

Beide Suchmaschinen bieten gute Ergebnisse bei einfachen Suchanfragen. Komplexe Suchanfragen mit mehreren Begriffen beantwortet Google oder die als Google-Proxy nutzbare Suchmaschine **Startpage** besser.

Meta-Suchmaschinen

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

- **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*:

³ <https://duckduckgo.com/goodies.html>

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](#)

- **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 ideale Ergänzung zu Ixquick.com. Einen Proxy zum anonymen Aufruf der Webseiten aus den Ergebnissen bietet Startpage auch.
- **Metager2.de** (<http://www.metager2.de>)
 ist ein 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.

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

Yacy⁴ 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 Oracle⁵ 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 Repository⁶ 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:8080> 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.

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.

⁴ <http://yacy.net>

⁵ <http://java.sun.com>

⁶ <http://www.yacy-websuche.de/wiki/index.php/De:DebianInstall>

Google ???

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

Einsatz von EverCookies: Der Surfer wird offenbar mit EverCookie Techniken markiert, wenn Cookies deaktiviert sind. 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, kann aber auch als Cookie-Ersatz missbraucht werden.

Beim Browser Mozilla Firefox erfolgt keine Markierung, da bei Firefox mit einer Sperrung von Cookies auch der DOMStorage gesperrt wird.

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/.....`

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 Werten werden als Parameter *biw* und *bih* in der Google-URL übergeben. Sie haben aber keinen Einfluss auch die Bildschirmdarstellung. Auch wenn das Browserfenster zu klein ist und die



Abbildung 4.2: Suchmaschinen verwalten

Darstellung nicht passt, bleiben die festen Größen der HTML-Elemente erhalten.

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

Auf der Webseite der Google-Suche kann man dem Tracking kaum entgehen. Wer unbedingt die Ergebnisse von Google braucht, kann die Suchmaschine *Startpage.com* als anonymisierenden Proxy nutzen. Sie ist mit dem Datenschutzsiegel EuroPriSe zertifiziert. Andere Suchmaschinen bieten eine andere Sicht auf das Netz - auch nicht schlecht, erfordert manchmal etwas Umgewöhnung.

4.2.1 Firefox konfigurieren

Für viele Suchdienste gibt es Plug-Ins zur Integration in die Suchleiste von Firefox. Die Website Mycroft ⁷ bietet ein Suchformular, mit dem man die

⁷ <http://mycroft.mozdev.org/>

passenden Plug-Ins nach Eingabe des Namens der Suchmaschine schnell findet. Die Installation funktioniert nur, wenn JavaScript für diese Website freigegeben wurde.

Für viele Suchmaschinen gibt es eine Variante mit SSL-Verschlüsselung. Diese Varianten sollten (wenn angeboten) bevorzugt genutzt werden. SSL-Verschlüsselung gibt es für Ixquick, Google, Wikipédia, Startpage u.a.m.

Außerdem kann die Generierung von Suchvorschlägen deaktiviert werden. Die Vorschläge kommen von dem gewählten Suchdienst, verlangsamen aber die Reaktion auf Eingaben deutlich. Ich weiss selber, was ich suche! Den Dialog findet man unter *Suchmaschinen verwalten* in der Liste der Suchmaschinen.

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 auch für das Tracking von Nutzern verwendet.

Der Screenshot Bild 4.3 zeigt die Liste der Cookies, die bei einem einmaligen Aufruf der Seite *www.spiegel.de* gesetzt wurden. Neben den Cookies von *spiegel.de* zur Zählung der Leser setzen gleich mehrere datensammelnde Werbeserver Cookies und außerdem Zähldienste (*quality-channel.de*, *ivwbox.de*), welche die Reichweiten von Online-Publikationen auswerten.

Es ist nicht ungewöhnlich, dass populäre Webseiten mehrere Datensammler einbinden. Eine Studie der Universität Berkeley ⁸ 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 Daten wurden an mehr als 600 Server übermittelt. Spitzenreiter unter den Datensammlern ist Google, 97% der populären Webseiten setzen Google-Cookies.

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 Erreichung der vollen Funktion benötigen, werden Ausnahmen zugelassen.
3. Die für den Zugriff auf personalisierte Inhalte gespeicherten Cookies sollten beim Schließen des Browsers automatisch gelöscht werden. Einige Websites verwenden diese Cookies auch nach dem Logout für das User-Tracking.

Fast alle Login-Seiten, welche Cookies zur Identifizierung des Surfers verwenden, weisen mit einem kleinen Satz auf die notwendigen Freigaben

⁸ <http://heise.de/-1288914>

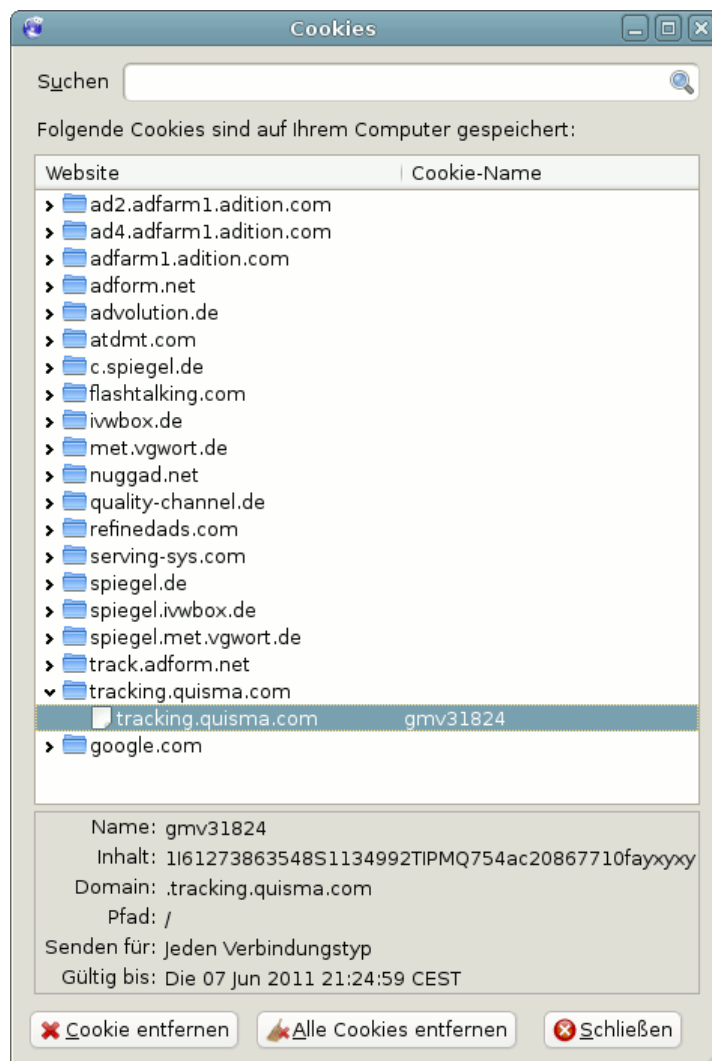


Abbildung 4.3: Liste der Cookies beim Besuch von Spiegel-Online

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.

4.3.1 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 Fremd-Cookies standardmäßig deaktiviert werden.

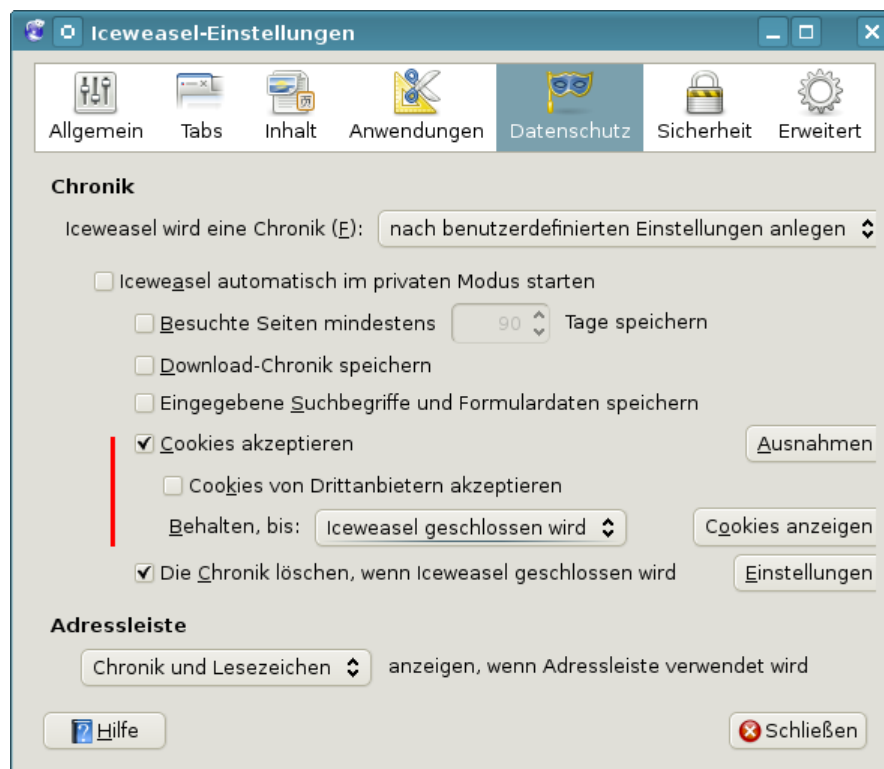


Abbildung 4.4: Cookies-Einstellungen in Firefox

Mit einem Klick auf den Button *Ausnahmen* kann man Server konfigurieren, die Cookies setzen dürfen oder grundsätzlich blockiert werden. Um von Google nicht beim Besuch der meisten deutschen Websites verfolgt zu werden, ist es nötig, diesen Dienst ausdrücklich zu blockieren.

Anderenfalls wird der Browser beim Start durch den Aufruf der Default-Seite oder beim Laden der Phishing-Datenbank mit einem Google-Cookie

“personalisiert”. Durch eingebettete Werbung und Google-Analytics auf vielen Websites kann Google unbedarfte Surfer effektiv beobachten.

Zusätzliche Add-ons für Firefox

Die Firefox Addon Sammlung bietet viele Add-ons um die Verwaltung von Cookies zu erleichtern. Nicht alle werden noch gepflegt und sind mit aktuellen Versionen von Firefox kompatibel. Das Add-on **CookieMonster**⁹ 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. Nach dem Neustart von Firefox ist in der Statusleiste ein zusätzliches Symbol vorhanden. Ein Klick mit der linken(!) Maustaste auf das blau-schwarze “CM” öffnet das in Bild 4.5 dargestellte Menü (nur wenn die Website Cookies nutzen möchte).

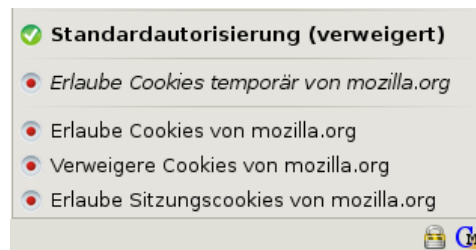


Abbildung 4.5: CookieMonster Menü

Erlaube Cookies temporär erlaubt es dem aktuellen Server, nur für diese Sitzung Cookies zu setzen. Mit dem Schließen des Browsers werden die Cookies und die Ausnahmereglung gelöscht.

Erlaube Cookies erlaubt es dem aktuellen Server, unbegrenzt gültige Cookies zu setzen. Diese Variante wird nur benötigt, wenn man bei einem späteren Besuch der Website automatisch wieder angemeldet werden möchte.

Verweigere Cookies erlaubt es dem aktuellen Server nicht, Cookies zu setzen.

Erlaube Sessioncookies erlaubt es dem aktuellen Server, Cookies zu setzen. Mit dem Schließen des Browsers werden diese Cookies wieder gelöscht. Bei folgenden Besuchen dürfen wieder neue Cookies gesetzt werden.

Nach der Installation von CookieMonster muss man das Standardverhalten auf *Alle Cookies blockieren* umschalten. Das ist sicherer, als nur die Cookies von Dritt-Seiten zu blockieren. Die Einstellungen werden im Add-ons-Manager unter *Extras -> Add-ons* in der Sektion *Erweiterungen* konfiguriert.

⁹ <https://addons.mozilla.org/de/firefox/addon/cookie-monster/>

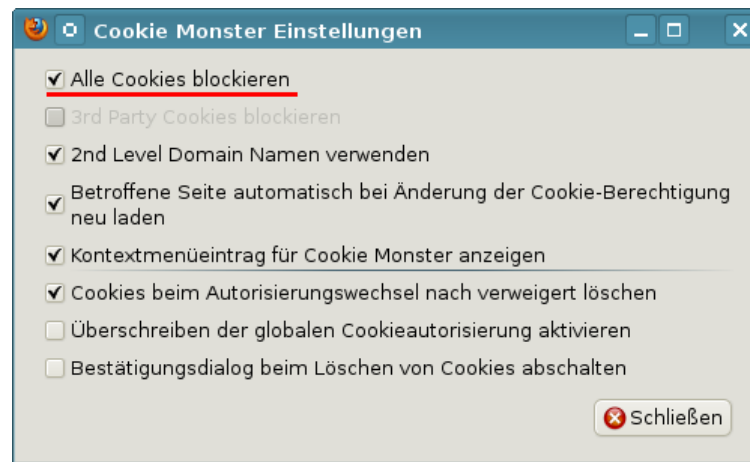


Abbildung 4.6: CookieMonster Einstellungen

4.3.2 Super-Cookies in Firefox

Mozilla Firefox bietet auch die clientseitige Datenspeicherung. Dieser DOM-Storage 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.

Diese parallele Anwendung der Einstellung für Cookies auf DOMStorage gilt nur für Firefox. Andere Browser verhalten sich bezüglich der clientseitigen Datenspeicherung anders! Bei Opera habe ich noch keine Möglichkeit gefunden, die lokale Speicherung von Daten gezielt zu deaktivieren.

4.3.3 Flash-Cookies verwalten

Auch Flash-Applikationen können Cookies setzen, sogenannte *Local Shared Objects (LSO)*. Diese Datenkrümel können bis zu 100kByte Daten fassen und ignorieren die Einstellungen des Browsers. Sie werden neben der Speicherung von Einstellungen auch zum Nutzertracking verwendet von Youtube, Ebay, Hulu...

Aktuelle Browser (mit Ausnahme von Opera) verwalten die Flash-Cookies nach den gleichen Regeln wie normale Cookies. Zusätzliche Add-ons zum Löschen der Flash Cookies sind nicht mehr nötig. Außerdem bieten Flash-Player unterschiedliche Möglichkeiten, diese Datenspeicherung zu deaktivieren:

1. Wer den **Adobe Flash-Player** nutzt, kann mit einer Flash-Anwendung

auf der Webseite von Macromedia ¹⁰ die Einstellungen für das Speichern und Auslesen von Informationen sowie Nutzung von Mikrofon und Kamera anpassen.

Auf der Seite *Globale Speichereinstellungen* ist die Datenspeicherung zu deaktivieren (Bild 4.7). Anschließend sind auf der Seite *Webseiten Speichereinstellungen* die bisher gespeicherten Cookies zu löschen.

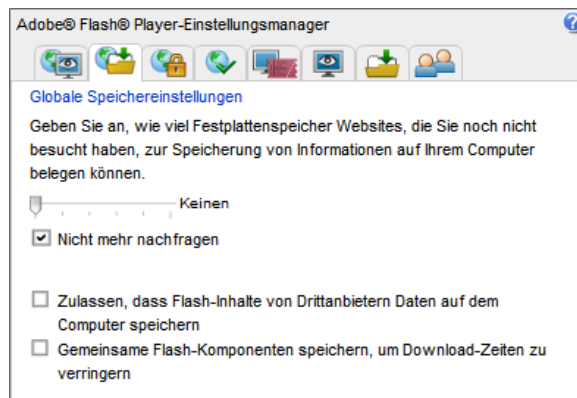


Abbildung 4.7: Einstellungsmanager für Adobe Flash-Player

Wer das Add-on NoScript nutzt, muss zusätzlich zur aktuellen Webseite dem Server *wwwimages.adobe.com* das Ausführen von Javascript erlauben. Anderenfalls funktioniert die Flash-Applikation nicht.

2. Der freie Flash-Player **Gnash** bietet die Möglichkeit, die Speicherung von Cookies zu konfigurieren. Man klickt mit der rechten Maustaste auf ein Flash-Movie und wählt den Punkt *Bearbeiten - Einstellungen* im Kontextmenü und schickt man alle Shared Objects nach `/dev/null`.

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 ¹¹ 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-Profil erstellen.

¹⁰ http://www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager.html

¹¹ <http://smorgasbork.com/component/content/article/84-a-study-of-internet-users-cookie-and-javascript-settings>

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.

Nach empirischen Untersuchungen der Universität Berkeley¹² nutzen ca. 40% der Tracking-Dienste EverCookie Techniken (Stand 2011). Besonders häufig werden seit 2008 Flash-Cookies bzw. LSOs parallel zu normalen Cookies eingesetzt (37%), dann folgen die sogenannten SuperCookies (DOMStorage oder IE-userData mit 7%) und ETags (2%). Teilweise werden mehrere Techniken kombiniert.

- Die *Google-Suche* nutzt DOMStorage, was eine Markierung von Nutzern auch bei deaktivierten Cookies ermöglicht.
- Die Firma *Clearspring* protzt damit, präzise Daten von 250 Mio. Internetnutzern 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 Demonstration¹³ 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

¹² http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390

¹³ <http://samy.pl/evercookie/>

- window.name auswerten
- Internet Explorer userData Storage
- Internet Explorer userData Storage
- HTML5 Database Storage via SQLite
- HTTP-Auth speichern (zukünftig)

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.
3. Ein EverCookie-sicherer Browser kann nur mit Konfigurationseinstellungen nicht erreicht werden. Der Datenverkehr ist durch zusätzliche Maßnahmen zu reinigen. Bisher kann nur der **JonDoFox** alle von Samy Kamkar vorgestellten Techniken im Browser blockieren.
(siehe Kapitel *Anonymisierungsdienste*)

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 Plugins und Hilfs-Applikationen.... Die Website <http://browserspy.dk> zeigt eine umfangreiche Liste.

Diese Informationen können zu einem individuellen Fingerabdruck verrechnet werden. Anhand dieses Fingerabdruck kann der Surfer wiedererkannt werden, auch wenn er die IP-Adresse mit VPNs oder Anonymisierungsdiensten verschleiert. Die EFF geht davon aus, dass diese Methode von vielen Datensammlern genutzt wird.

- *Yahoo! Web Analytics* nutzt Javascript Tracking Code, wenn Cookies blockiert werden.

*In case Yahoo! Web Analytics cannot set a cookie, the system can still retrieve information from the JavaScript tracking code, the IP address and the web browser user agent.*¹⁴

¹⁴ http://help.yahoo.com/l/us/yahoo/ywa/documentation/install_guide/ig_get_started.html

- Ein weiteres Beispiel ist die Firma *bluecave* ¹⁵. Das Trackingscript *BCAL5.js* sammelt Informationen zur verwendeten Software, installierte Schriftarten, Bildschirmgröße, Browser Plug-ins und ein paar mehr Daten, um daraus einen individuellen Fingerprint zu berechnen. *bluecave* protzt damit, 99% der Surfer zu erkennen.
 - Der Trackingdienst Multicounter ¹⁶ und die Google Suche speichern die per Javascript ausgelesene Bildschirmgröße als besonderes individuelles Merkmal.
2. Einige EverCookie Techniken nutzen Javascript, um zusätzliche Markierungen im Browser zu hinterlegen und gelöschte Tracking Cookies wiederherzustellen.
 3. Durch Einschleusen von Schadcode können Sicherheitslücken ausgenutzt und der Rechner kann kompromittiert werden. Das Einschleusen von Schadcode erfolgt dabei auch über vertrauenswürdige Webseiten, beispielsweise mit Cross Site Scripting, wenn diese Websites nachlässig programmiert wurden.

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.

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 ¹⁷ installiert werden. Ein einfacher Klick auf das Download-Symbol startet die Installation. Im Anschluss ist Firefox neu zu starten.

Nach dem Neustart von Firefox ist in der Statusleiste ein zusätzliches Symbol vorhanden, welches den Status der Freigabe von JavaScript anzeigt. Ein Klick auf das Symbol öffnet das im Bild 4.8 gezeigte Menü, welches JavaScript für die aktuellen Sites generell oder nur temporär freigibt.

Einige Webseiten verwenden *Captchas* als Spamschutz. Die Captchas werden von Drittseiten eingebunden (Recaptcha.com, Nucaptcha.com...) und funktionieren nur, wenn Javascript für den Captcha-Provider freigegeben ist. Wenn das Captcha auf einer Webseite nicht funktioniert, schauen sie in der NoScript-Liste nach, ob evtl. ein Captcha-Provider dabei ist und geben sie Javascript temporär für diese Domain frei.

Weitere Skripte von Drittanbietern werden üblicherweise nur zum Spionieren verwendet und sind für die Funktionalität selten notwendig.

¹⁵ <http://www.bluecava.com>

¹⁶ <http://www.multicounter.de/features.html>

¹⁷ <https://addons.mozilla.org/de/firefox/addon/noscript>

eines Info-Balkens hilfreich bei der Suche nach den Ursachen sein.

NoScript dient nicht nur der Steuerung von Javascript, es bieten **Schutz gegen vielfältige Angriffe** aus dem Netz. (XSS-Angriffe, Webbugs, Click-Hijacking...). Außerdem blockiert es auch Ping-Attribute und kann für eine Liste von Webseiten SSL-Verschlüsselung erzwingen.

4.6 Werbung, HTML-Wanzen und Social Media

Die auf vielen Websites eingeblendete **Werbung** wird von wenigen Servern bereitgestellt. Diese nutzen häufig die Möglichkeit, das Surfverhalten websiteübergreifend zu erfassen. Mit Hilfe von listen- und patternbasierten Filtern kann der Zugriff auf Werbung unterbunden werden. Für den Browser Firefox gibt es die Adblock Plug-Ins, Nutzer anderer Browser können Content-Filter zum Blockieren von Werbung nutzen.

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 Statement¹⁸ zu Werbung auf Heise online veröffentlicht und erklärt, wie sie einzelne Webangebote durch Freigaben im Werblocker 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 METIS¹⁹ 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 deutschen Datenschutzrecht vereinbar. Deutsche Webseitenbetreiber sind aufgefordert, die Facebook Buttons von ihren Seiten zu entfernen²⁰. Mit dem Aufruf einer Webseite, die den Like Button enthält, werden Daten an Facebook übertragen und dort ausgewertet.

Als Schutz vor dieser Datensammlung kann man diese Elemente mit geeigneten Filterlisten blockieren. Eine passende Liste stellt MonztA bereit²¹.

¹⁸ <http://www.heise.de/Adblocker-auf-heise-online-1164703.html>

¹⁹ <http://www.vgwort.de/metis.php>

²⁰ <https://www.datenschutzzentrum.de/facebook>

²¹ <http://www.camp-firefox.de/forum/viewtopic.php?f=4&t=82797>

4.6.1 Adblock für Mozilla Firefox

Für Mozilla Firefox steht mit **Adblock Plus**²² 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.

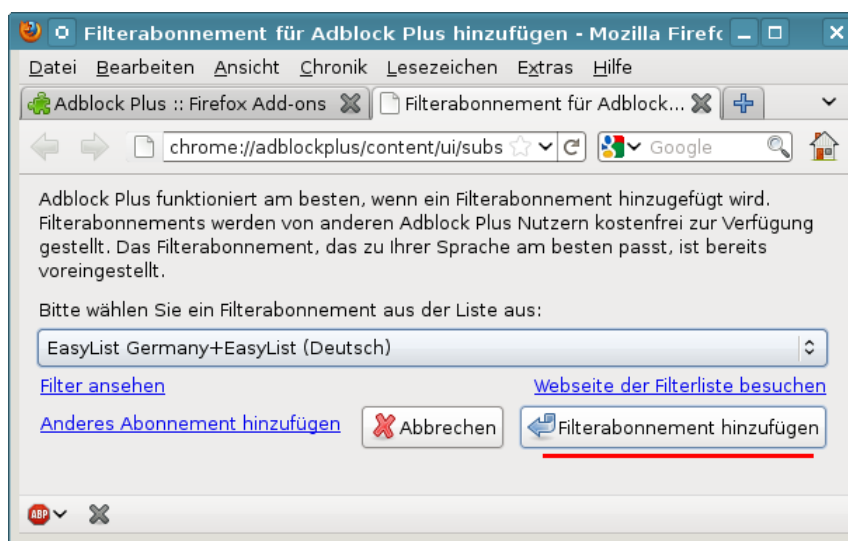


Abbildung 4.10: Auswahl einer Liste nach der Installation von Adblock Plus

Zusätzliche Filterlisten abonnieren

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 können 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, da sie bereits vorhanden ist.
- **SocialMediaBlock** ist eine Liste zum Blockieren der verschiedenen Social Media Tracking Features wie Facebook Like Buttons u.ä. Zur

²² <https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/>

Installation kopiert man folgende URL in die Adressleiste von Firefox:

abp://subscribe/?location=http://monzta.maltekraus.de/adbblock_social.txt&title=SocialMediaBlock

Whitelisting von Websites

Mit der Version 2.0 hat Adblock eine Whitelist für unaufdringliche Werbung eingeführt. Die Filterung wird auf den Webseiten in der Whitelist abgeschaltet, so dass diese Webseiten Werbung einblenden können. Bisher ist die Whitelist ziemlich leer. Man kann dieses Feature wie in Bild 4.11 in der Übersicht der Filterlisten abschalten, indem man die Option *Nicht aufdringliche Werbung zulassen* deaktiviert. Alternativ kann man auch das Add-on **TrueBlock** statt Adblock verwenden. Es ist 100% kompatibel mit Adblock, das Whitelisting ist jedoch standardmäßig deaktiviert.

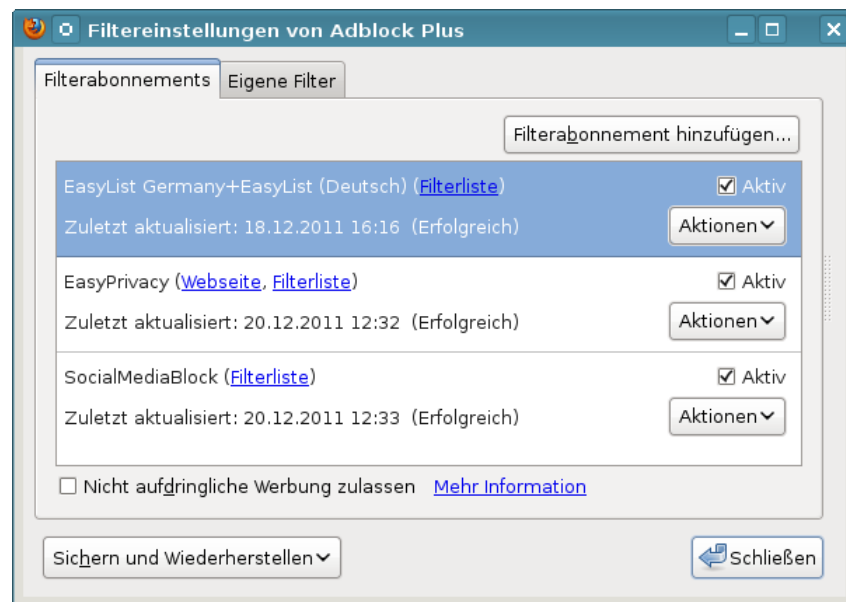


Abbildung 4.11: Whitelisting in Adblock Plus deaktivieren

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.

4.7 History Sniffing

Browser speichern Informationen über besuchte Webseiten in einer Surf-History. Eine empirische Untersuchung der University of California ²³ zeigt,

²³ <http://cseweb.ucsd.edu/users/lerner/papers/ccs10-jsc.pdf>

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 ²⁴ zeigt, dass diese History-Daten auch zur Deanonymisierung der Surfer 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 vieler Surfer nur durch den Aufruf der präparierten Webseite ermittelt werden.

Neben Javascript können auch CSS-Hacks für das Auslesen der Surf-Historie genutzt werden. In der wissenschaftlichen Arbeit *Feasibility and Real-World Implications of Web Browser History Detection* ²⁵ zeigen Security Experten, wie man die unterschiedliche farbliche Darstellung von besuchten Links auswerten kann.

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.

4.8 Risiko Plugins

Für die Darstellung von Inhalten, die nicht im HTML-Standard definiert sind, kann Firefox Plugins nutzen. Populär sind Plugins für die Anzeige von PDF-Dokumenten im Browser oder Flash Videos. Die Nutzung dieser Plugins ist jedoch ein Sicherheitsrisiko. Firefox ab Version 14.0 bietet eine einfache Möglichkeit, die Gefahr durch Plug-ins zu reduzieren. Man kann unter der Adresse *about:config* die folgende Variable setzen:

```
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.

4.8.1 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 ²⁶. 2008 gelang es dem *Ghostnet*, die Rechnersysteme westlicher

²⁴ <http://heise.de/-919076>

²⁵ <http://www.w2spconf.com/2010/papers/p26.pdf>

²⁶ <http://heise.de/-979037>

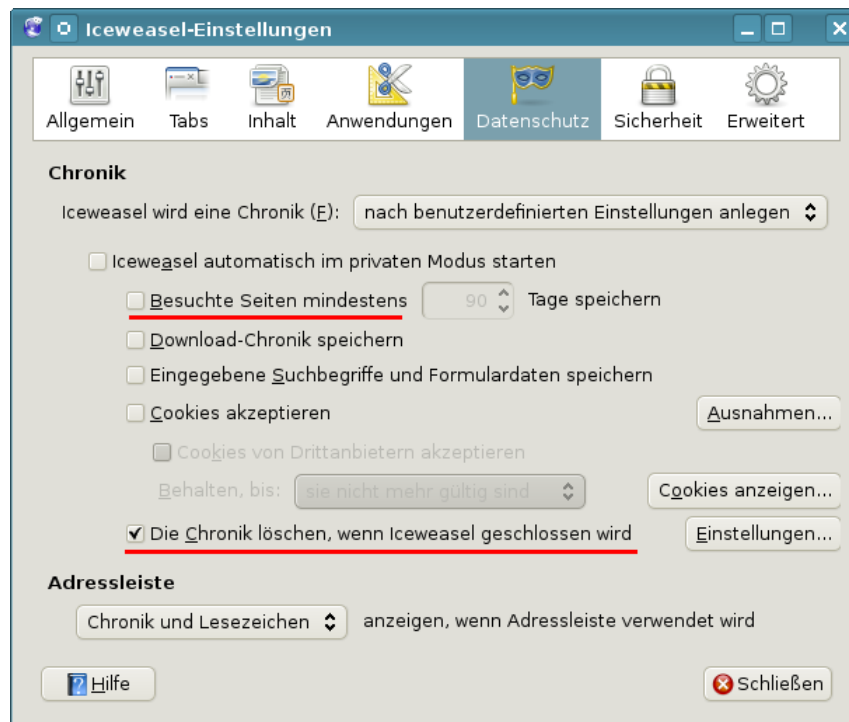


Abbildung 4.12: Speichern der Surf-Chronik deaktivieren

Regierungen, der US-Regierung und des Dalai Lama mit böartigen PDFs zu infizieren²⁷. Über eine von Adobe als *nicht kritisch* eingestufte Sicherheitslücke einer überflüssigen PDF-Funktion wurde der Wurm Win32/Auraax verteilt²⁸.

Nach Beobachtung des Sicherheitsdienstleisters Symantec²⁹ und Scan-Safe³⁰ erfolgen die meisten Angriffe aus dem Web mit böartigen 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.org³¹ Open Source Alternativen vor.

- Für Windows werden *Evince* und *Sumatra PDF* empfohlen.
- Für Linux gibt es *Okular* (KDE) und *Evince* (GNOME, XFCE).

²⁷ <http://www.linux-magazin.de/Heft-Abo/Ausgaben/2010/01/Geisterstunde>

²⁸ <http://heise.de/-990544>

²⁹ <http://heise.de/-981631>

³⁰ http://www.scansafe.com/downloads/gtr/2009_AGTR.pdf

³¹ <http://www.pdfreaders.org/index.de.html>

- Für MacOS wird *Vindaloo* empfohlen.
2. Wenn die PDF Reader Plugins nicht deinstallierbar sind, 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 ³² nutzen, um PDF-Dokumente aus dem Internet zu betrachten ohne den eigenen Rechner zu gefährden.

4.8.2 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.

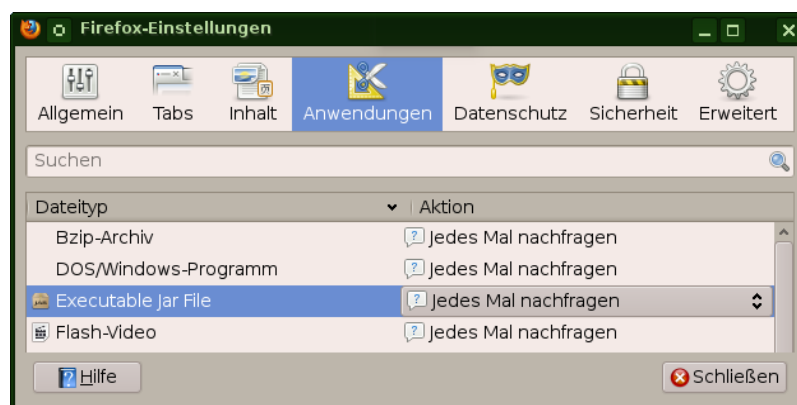


Abbildung 4.13: Externe Anwendungen nur auf Nachfrage öffnen

Auf dem Reiter *Anwendungen* im Dialog *Einstellungen* können die Helper-Applications wie im Bild 4.13 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.

4.8.3 Java-Applets

Es gibt eine Vielzahl von sinnvollen Java-Anwendungen. Im Internet spielt Java aber keine Rolle mehr (im Gegensatz zu Javascript, bitte nicht verwech-

³² <http://view.samurajdata.se>

seln). Trotzdem installieren Java Runtime Environments ohne Nachfrage ein Browser-Plugin zum Ausführen von Java-Applets. Diese Applets sind in erster Linie ein Sicherheitsrisiko und können den Rechner unbemerkt infizieren.

Der (Staats-) Trojaner der italienischen Firma *HackingTeam*³³ wird beispielsweise über eine sauber signierte JAR-Datei auf dem Zielsystem installiert und kann neben Windows auch MacOS, Linux und diverse Smartphones auf diesem Weg infizieren. Der Trojaner belauscht Skype, fängt Tastatureingaben ab, kann die Webcam zur Raumüberwachung aktivieren und den Standort des Nutzers ermitteln.

Das Add-on **NoScript** blockiert Java-Applets und andere eingebettete Elemente, in der Default Konfiguration aber nur auf nicht vertrauenswürdigen Seiten. Es gibt keine Probleme, wenn man diese Einschränkungen auch auf vertrauenswürdige Seiten anwendet. Da man Javascript häufig freigeben muss und die Website damit als vertrauenswürdige definiert wird, wird diese Anpassung der Konfiguration dringend empfohlen. (Bild 4.14)

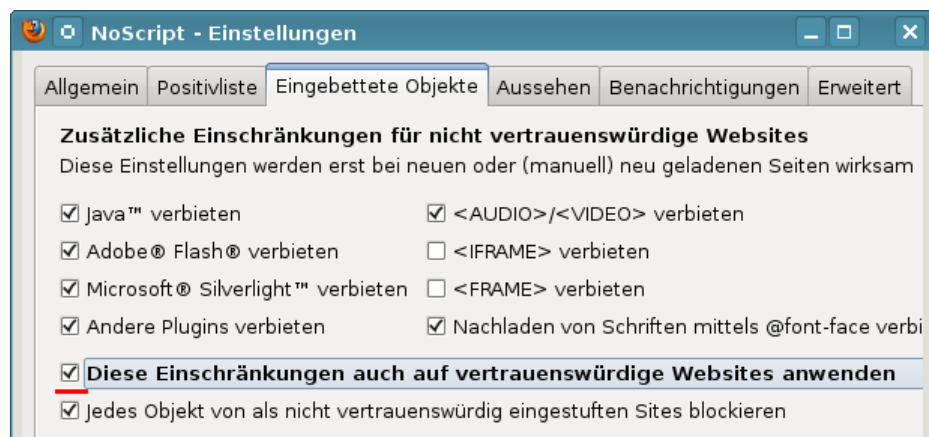


Abbildung 4.14: Java auch für vertrauenswürdige Webseiten blockieren

4.8.4 Flash und Silverlight

Auch diese Plugins sind ein Sicherheits- und Privacyrisiko. Sie werden meist für die Darstellung von Videos im Web (Youtube) und Panoramadiensten wie Street View (Google) bzw. Street Side (Microsoft) genutzt.

Schutzmaßnahmen:

1. Das Add-on **NoScript** kann diese Inhalte blockieren. Es wird ein Platzhalter angezeigt. Bei Bedarf kann man das Video mit einem Mausklick anschauen.

³³ <http://heise.de/-1671203>

2. Web Videos können mit Hilfe von Download Sites wie KeepVid ³⁴ oder ShareTube ³⁵ als Datei gespeichert und mit einem Mediaplayer angezeigt werden. Wer noch keinen passenden Mediaplayer installiert hat, kann den VideoLAN Player nutzen, der für alle Betriebssysteme zur Verfügung steht.
3. Die Firefox Add-ons **UnPlug** ³⁶ oder **DownloadHelper** ³⁷ können Videos von vielen Websites herunter laden und in ein gebräuchlicheres Format für Mediaplayer konvertiert werden.

4.9 HTTPS 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.

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.

HTTPS-Everywhere

Das Firefox Add-on HTTPS-Everywhere³⁸ der EFF.org kann auch komplexe Umschreibungen der URLs realisieren, wie es beispw. für Wikipedia notwendig ist. Das Add-on bringt aber 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 4.16).

³⁴ <http://keepvid.com>

³⁵ <http://www.share-tube.de/flvdownload.php>

³⁶ <https://addons.mozilla.org/en-US/firefox/addon/unplug>

³⁷ <https://addons.mozilla.org/de/firefox/addon/video-downloadhelper>

³⁸ <https://www.eff.org/https-everywhere>

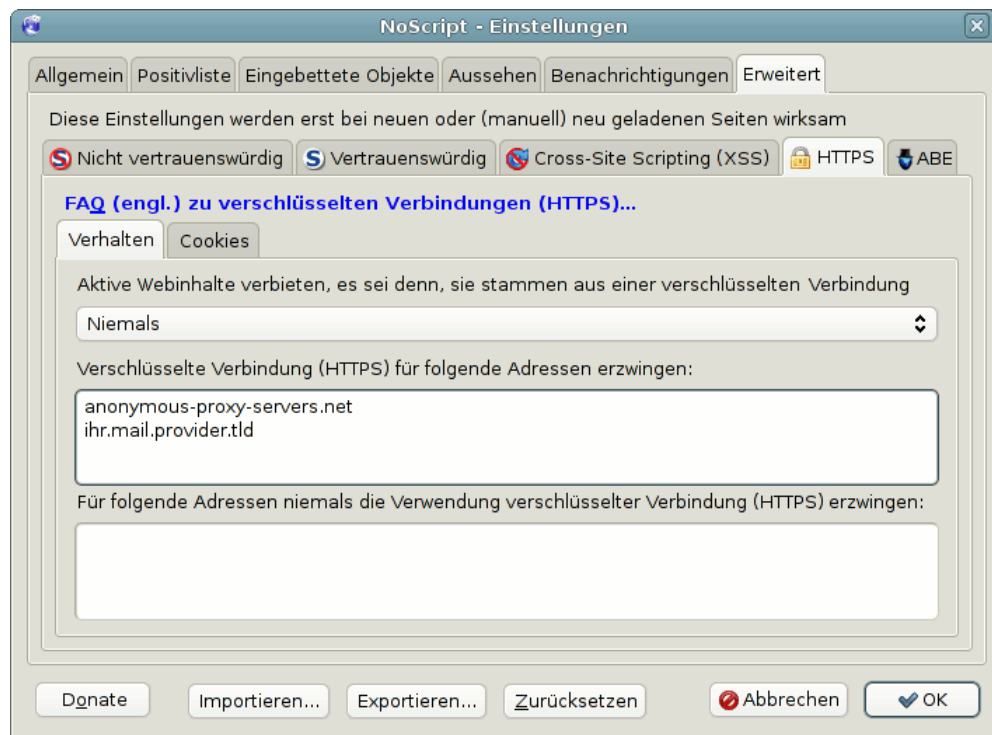


Abbildung 4.15: Einstellungen für NoScript STS

HTTPS-Finder

Das Add-on HTTPS-Finder³⁹ kann erkennen, ob eine Webseite auch via HTTPS erreichbar ist und erzwingt dann die Nutzung von HTTPS. Es können automatisch Regeln für HTTPS-Everywhere erstellt und aktiviert werden. Das Add-on ist eine gute Ergänzung für HTTPS-Everywhere und erspart das komplexe Erstellen der XML-Dateien von Hand.

4.10 Vertrauenswürdigkeit von HTTPS

IT-Sicherheitsforscher der EFF kommen in einer wissenschaftlichen Arbeit⁴⁰ 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 EFF:

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.

³⁹ <https://addons.mozilla.org/de/firefox/addon/https-finder/>

⁴⁰ <https://eff.org/deepinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl>

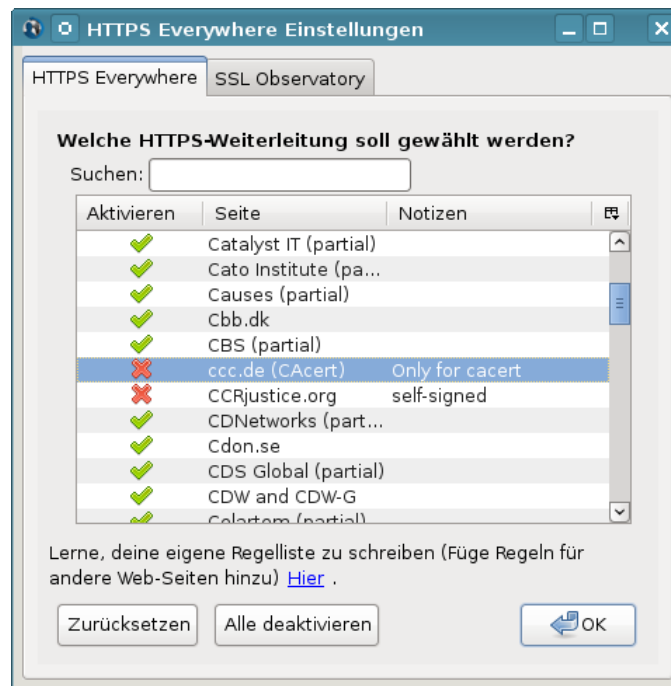


Abbildung 4.16: Einstellungen für Htps-Everywhere

Ein erster Angriff dieser Art gegen iranische Internet Nutzer wurde im August 2011 nachgewiesen. Er betraf neben Google die Webdienste mehrerer Geheimdienste (MI6, CIA, Mossad) und außerdem www.torproject.org. Bei diesem Angriff wurde keine Zertifikate einer standardmäßig vertrauenswürdigen Certification Authority genutzt, sondern die niederländische Certification Authority DigiNotar wurde gehackt, um gültige Zertifikate zu erlangen. Insgesamt wurden 531 SSL-Zertifikate kompromittiert.⁴¹

Neben DigiNotar wurden 2011 die Certification Authorities Comodo, InstantSSL und zwei weitere Sub-Registrare von Comodo erfolgreich angegriffen⁴². Die Angreifer konnten sich unbefugt gültige Zertifikate für die Webseiten von Google, Yahoo, Mozilla und Skype erstellen. Nach Beobachtung des SSL-Observatory der EFF wurden bei den Angriffen mindestens 248 Zertifikate erfolgreich kompromittiert. Auch in diesen Fällen soll der Angriff vom Iran ausgegangen sein. StartSSL wurde offenbar erfolglos mit dem gleichen Ziel angegriffen.

Die Software für einen man-in-the-middle Angriff mit den gefälschten Zertifikaten gibt es als Open Source, z.B. den mitm-proxy⁴³ der Stanford

⁴¹ https://threatpost.com/en_us/blogs/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112

⁴² <http://heise.de/-1213999>

⁴³ <http://crypto.stanford.edu/ssl-mitm/>

University oder dsniFF ⁴⁴. Auf der ISS World (Messe für Überwachungstechnik) werden fertige Appliances angeboten, gegen Aufpreis auch mit gültigem CA-Zertifikat.

Wer Kosten (für den Aufpreis) oder Mühen (für das Hacken einer CA) scheut, kann sich so einfach als Unberechtigter ein gültiges SSL-Zertifikat für einen Mail- oder Web-Server ausstellen zu lassen ⁴⁵. Man muss nur einen der zulässigen E-Mail Accounts für SSL-Admins registrieren und kann ein gültiges Fake-Zertifikat erstellen. Par ordre du mufti werden *webmasterdomain.tld*, *postmasterdomain.tld*, *ssladmindomain.tld*, *ssladministratoromain.tld* u.a.m. von den Certification Authorities akzeptiert. Nicht immer sind diese Adressen reserviert und geschützt.

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. (Firefox Add-ons: Certificate Patrol, JonDoFox)
- **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.
(Firefox Add-ons: HTTPS-Everywhere, Perspectives, Convergence.io)
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 verteilt und ausgewertet werden. Das wäre ein besserer Weg, als der Vergleich mit externen Beobachtern.
Über einen unabhängigen Weg wird festgelegt, welche Zertifikate für die HTTPS-Verschlüsselung einer Webseite genutzt werden dürfen. Nur diese Zertifikate werden vom Browser akzeptiert. Google hat die Fingerprints der Zertifikate seiner Webseiten fest im Browser Chrome codiert. Dieses Verfahren skaliert aber nicht. Möglich wäre auch die Nutzung von DNSSEC mittels Sovereign Keys. Brauchbare Ideen zum Certificate Pinning sind noch in der Entwicklung.

⁴⁴ <http://www.monkey.org/~dugsong/dsniff/>

⁴⁵ https://bugzilla.mozilla.org/show_bug.cgi?id=556468

4.10.1 Firefox Add-ons

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

HTTPS-Everywhere

HTTPS-Everywhere⁴⁶ kann das SSL-Observatory der EFF.org nutzen. Wenn man diese Funktion in den Einstellungen des Add-on aktiviert (Bild 4.17), werden die SSL-Zertifikate der besuchten Webseiten an das SSL-Observatory gesendet. Ist das Zertifikat nicht ok, wird man ab Version 3.0 gewarnt. Es wird eine Datenbasis von weltweit verteilten Nutzern aufgebaut. (Meine Empfehlung!)

Certificates Patrol

Certificates Patrol⁴⁷ speichert Informationen zu den Zertifikaten einer Website in einer internen Datenbank. Beim Erstbesuch wird mit einem Informationsbalken am oberen Seitenrand auf ein neues Zertifikat hingewiesen. Man kann es bei Bedarf überprüfen. Am einfachsten kann man ein SSL-Zertifikat prüfen, wenn die Fingerprints vom Webmaster veröffentlicht wurden.

Hat sich das Zertifikat bei späteren Besuchen der Website geändert, zeigt das Add-on Informationen oder Warnungen zum Zertifikatswechsel wie im Bild 4.18 gezeigt.

Der Gefahrenwert wird dabei anhand einer Heuristik ermittelt. Im Beispiel wurde überraschend ein neues Zertifikat für die Webseite der EFF gefunden, obwohl das alte Zertifikat noch lange gültig gewesen wäre. Außerdem wurde die CA gewechselt.

Der Nutzer muss bei Warnungen das neue Zertifikat bestätigen, da es ein Hinweis auf einen Angriff sein. Wie kann man prüfen, ob der Zertifikatswechsel ok ist?

1. Häufig veröffentlicht der Webmaster der Seite eine Information zum Zertifikatswechsel im Blog mit den Informationen zum neuen Zertifikat.
2. Bei Banken u.ä. Diensten kann man telefonisch nachfragen, ob das SSL-Zertifikat geändert wurde.
3. Man kann prüfen, welches Zertifikat andere Teilnehmer im Netz sehen, beispielsweise mit dem Add-on Perspectives (siehe unten). Das Projekt bietet auch eine Demo-Webseite⁴⁸, wo man die Informationen der Notary Server abfragen kann.

⁴⁶ <https://www.eff.org/https-everywhere>

⁴⁷ <https://addons.mozilla.org/de/firefox/addon/certificate-patrol/>

⁴⁸ http://data.networknotary.org/notary_web/notary_query

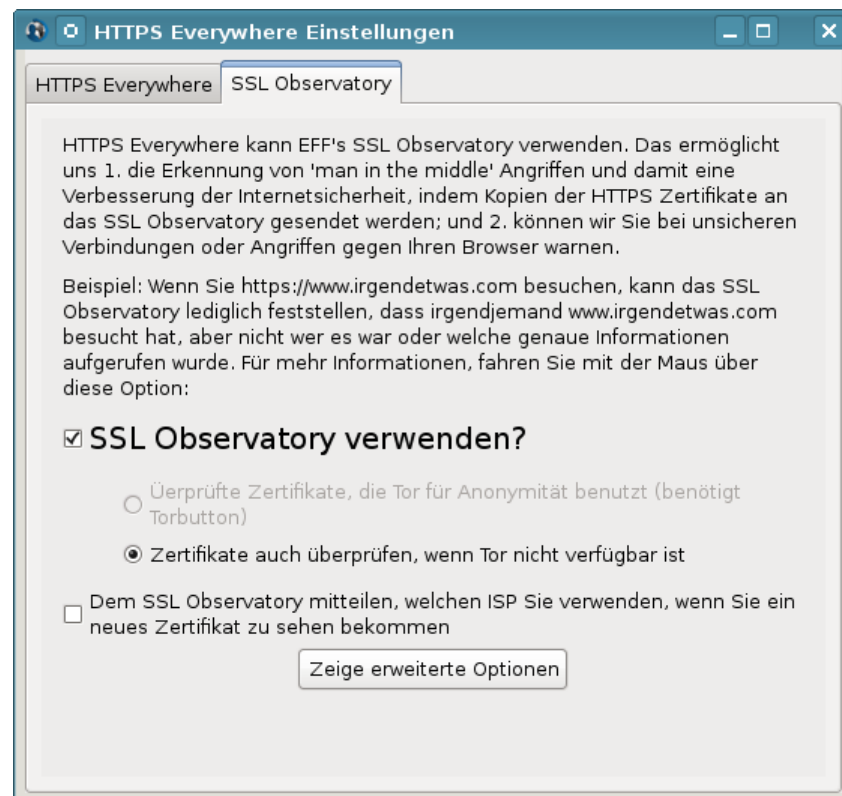


Abbildung 4.17: SSL-Observatory aktivieren in HTTPS-Everywhere



Abbildung 4.18: Warnung bei setsamen Wechsel des SSL-Zertifikat

Perspectives

Perspectives⁴⁹ 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 4.19 zu setzen.

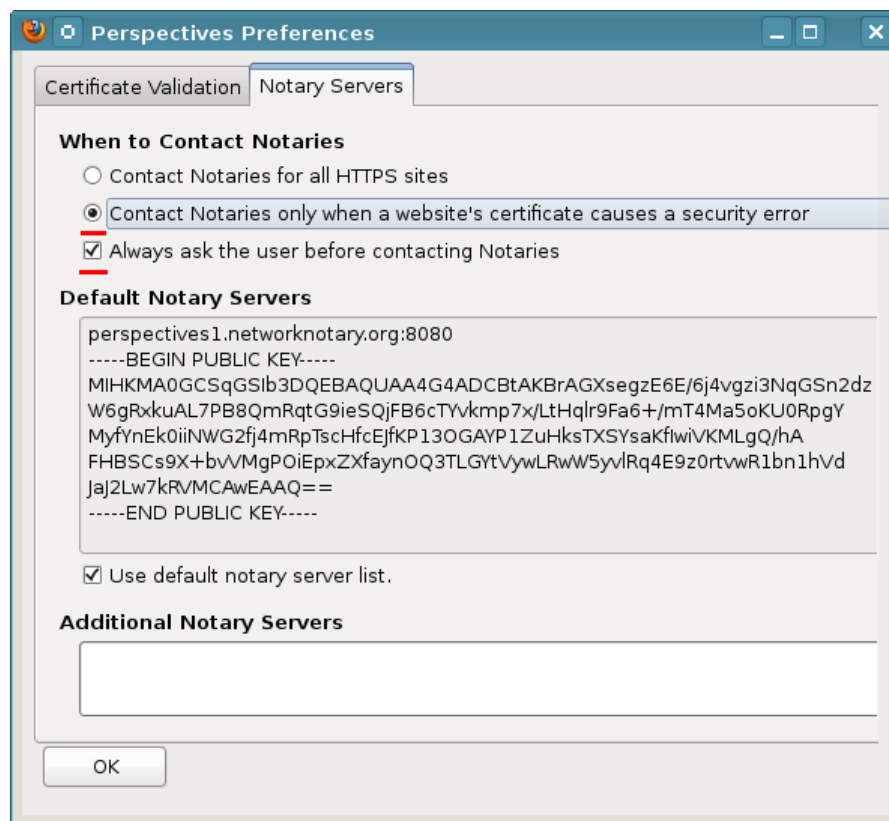


Abbildung 4.19: Perspectives Konfiguration

⁴⁹ <https://addons.mozilla.org/en-US/firefox/addon/perspectives/>

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.

Convergence.io

Convergence (Beta): Während Certificate Patrol und Perspectives auf dem alten Zertifikatssystem aufsetzen und es etwas verbessern, vollzieht Convergence.io einen radikalen Bruch. Das Add-on ersetzt die Validierung der Zertifikate im Firefox vollständig durch ein eigenes System. Dabei werden ähnlich wie bei Perspectives die Beobachtungen von Notary Server genutzt und mit dem aktuellen Zertifikat verglichen.

Ich habe (noch) keine Erfahrungen mit Convergence.io gesammelt.

4.11 HTTPS Tracking

Beim Aufbau einer verschlüsselten HTTPS-Verbindung wird eine sogenannte Session initialisiert. Die kryptografischen Details sollen an dieser Stelle nicht erläutert werden.

Es ist möglich, diese HTTPS-Session für das Tracking zu nutzen und für bis zu 48h immer wieder zu erneuern. Dieses Tracking-Verfahren ist so gut wie nicht nachweisbar, da es vollständig durch den Webserver realisiert wird und keine Spuren im Browser hinterlässt. Man kann davon ausgehen, dass dieses Tracking als Ergänzung zu (Ever-) Cookies genutzt wird. Der Tracking-Service Woopa verwendet seit 2008 HTTPS Session Tracking.

Für HTTPS Session Tracking gibt es zwei Möglichkeiten:

Tracking via Session Resumption ist im RFC 5077 beschrieben.

Gegen Tracking via Session Resumption kann man sich schützen, indem man im Mozilla Firefox unter *about:config* die folgende Variable auf FALSE setzt:

```
security.enable_tls_session_tickets    false
```

Das führt zu geringen Einbußen der Performance bei SSL-verschlüsselten Webseiten, da für jede Seite eine neue HTTPS Session ausgehandelt werden muss.

Tracking via SSL-Session-ID wird ebenfalls von allen Webservern unterstützt. Auch Webshops können die Session-ID für das Tracking verwenden, z.B. die xtcModified eCommerce Shopsoftware⁵⁰.

⁵⁰ http://www.modified-shop.org/wiki/SESSION_CHECK_SSL_SESSION_ID

Gegen das Tracking via Session-ID schützen nur das TorBrowserBundle und der JonDoBrowser (Beta). Man kann sich nicht durch Konfigurationseinstellungen oder Add-ons schützen, da der Source-Code des Browser dafür modifiziert werden muss.

4.12 Starke Passwörter nutzen

Jeder kennt das Problem mit den Passwörtern. Es sollen starke Passwörter sein, sie sollen für jede Site unterschiedlich sein und außerdem muss man sich das alles auch noch merken.

- 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 gleichen Passwörter wurden vom Führungspersonal für eine Reihe weiterer Dienste genutzt: E-Mail, Twitter und Linked-In. Die veröffentlichten 60.000 E-Mails waren sehr peinlich für HBGary ⁵¹.
- 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)

Das Add-on **PwdHash**⁵² vereinfacht den Umgang mit Passwörtern. Wenn man vor der Eingabe des Passwortes die Taste F2 drückt oder mit einem doppelten @@ beginnt, wird es umgerechnet und ein Hash aus dem Master Passwort und der Domain berechnet. Das Ergebnis der Berechnung ist eine 10-stellige zufällige Kombination von Buchstaben und Zahlen und wird als Passwort gesendet.

Damit ist es möglich, ein einfach zu merkendes Master Passwort für alle Sites zu nutzen, bei denen *PwdHash* funktioniert. Wichtig ist, dass die Domains der Webseiten für die Änderung und Eingabe der Passwörter identisch sind. PwdHash schützt damit auch vor Phishing Attacken. 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 ⁵³ steht der Algorithmus auch als Javascript Applet zur Verfügung.

⁵¹ <http://www.heise.de/ct/artikel/Ausgelacht-1195082.html>

⁵² <https://addons.mozilla.org/de/firefox/addon/pwdhash/>

⁵³ <https://www.pwdhash.com>

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.

4.13 HTTP-Header filtern

Neben der Verwendung von Cookies wird auch der Inhalt des HTTP-Header für die Gewinnung von Informationen über den Surfer genutzt. Das Projekt *Panopticlick*⁵⁴ der EFF.org zeigt, dass anhand des Fingerprint des HTTP-Headers 80% der Surfer eindeutig erkennbar sind. Eine Verknüpfung dieser Information über mehrere Websites hinweg kann eine Verfolgung von Nutzern ermöglichen. Kombiniert man diese Verfolgung mit Daten von Sozialen Netzen (Facebook, Xing), ist eine vollständige Deanonymisierung möglich.

- Beispiel **Referer**: Von welcher Seite kommt der Surfer? Die Schleimspur im Internet, sehr gut geeignet für das Tracking. Zwar sollte es belanglos sein, von welcher Seite der Surfer kommt, einige Websites werten den Referer jedoch aus.
- Beispiel **User-Agent**: 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 Kunden⁵⁵. Außerdem können anhand der Informationen gezielt Lücken in der verwendeten Software ausgenutzt werden.

- **ETags aus dem Cache**: 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 auch eine User-ID enthalten. Die Firma KISSmetrics verwendete diese Technik bis August 2011, um gelöschte Tracking-Cookies wieder herzustellen.
- Ergänzende Informationen wie zum Beispiel die bevorzugte **Sprache**, installierte **Schriftarten** und **Größe des Browserfensters** können einen individuellen Fingerprint des Browsers ergeben. Viele Werte können per Javascript ausgelesen werden. Bei der Google-Suche und beim Trackingdienst Multicounter⁵⁶ wird die innere Größe des Browserfensters ausgelesen. Die Firma bluecave⁵⁷ nutzt z.B. im Trackingscript *BCAL5.js* u.a. Informationen über installierte Schriftarten.

⁵⁴ <http://panopticlick.eff.org>

⁵⁵ <http://heise.de/-1626368>

⁵⁶ <http://www.multicounter.de/features.html>

⁵⁷ <http://www.bluecava.com>

Deshalb sollte man Javascript nur für vertrauenswürdige Webseiten erlauben und das Auslesen der Werte behindern (soweit möglich).

Installierte Schriftarten verstecken für Firefox

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 4.20 die Option zu deaktivieren.

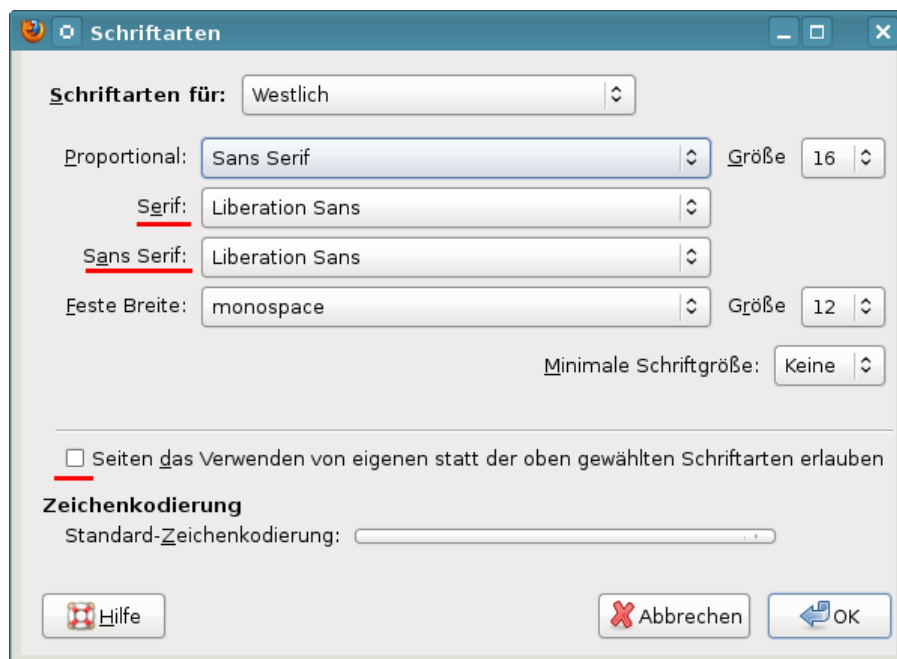


Abbildung 4.20: Schriftarten

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* (siehe Screenshot).

Browser Cache löschen

Ein vollständiges Abschalten des Cache ist nicht empfehlenswert. Man sollte den Cache des Browsers beim Schließen reinigen. Alle Browser bieten die Möglichkeit, diese Option in den Einstellungen zur Privatsphäre zu aktivieren.

Im Firefox findet man die Konfiguration im Dialog *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 (Bild 4.21) kann man detailliert festlegen, welche Daten beim Schließen des Browsers gelöscht werden sollen.

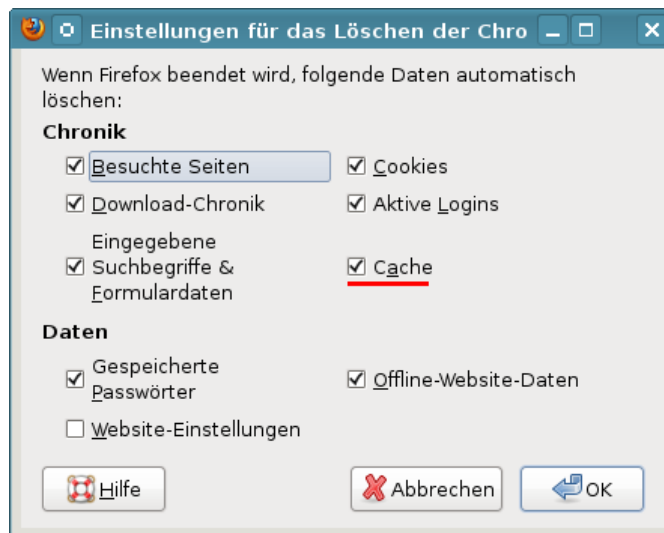


Abbildung 4.21: Cache löschen beim Beenden

Firefox verwendet einen Cache im Hauptspeicher und einen Disk-Cache auf der Festplatte. Der Cache im Hauptspeicher ist mit 64 MB groß genug. 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
```

Referer modifizieren für Firefox

Das Add-on **RefControl**⁵⁸ modifiziert den Referer. Spezifische Einstellungen für einzelne Webseiten sind möglich. Nach der Installation des Plug-Ins sollte im Dialog *Optionen* der Standard-Wert angepasst werden.

Die Einstellung *“Blockieren (nur beim Wechsel)”* liefert einen plausiblen Referer, solange man innerhalb einer Domain bleibt, entfernt ihn beim Wechsel der Domain. Die Schleimspur wird unterbrochen ohne Funktionen der Website einzuschränken.

⁵⁸ <https://addons.mozilla.org/de/firefox/addon/refcontrol/>

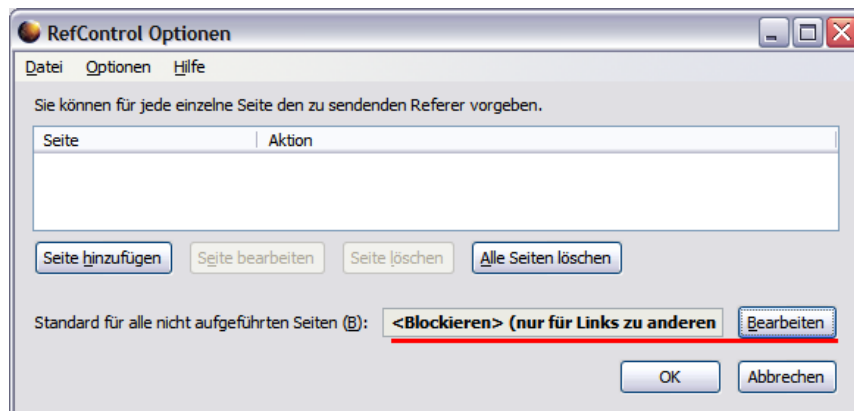


Abbildung 4.22: Einstellungen von RefControl

Technisch hochentwickelte Datensammler können den Schutz von RefControl bereits aushebeln. Google+ und einige Werbenetzwerke übertragen den Referer zusätzlich in URL-Parametern. RefControl schadet aber nicht und dümmere Webmaster tracken auch.

User-Agent modifizieren für Firefox

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 Browser durch individuelle 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. Daher sollte man einen Fake von Firefox für Windows nutzen, um in einer größeren Anonymitätsgruppe abzutauchen. Für Windows Nutzer empfehle ich keine Fakes, da man durch kleine Fehler nur eindeutiger identifizierbar wird.

Um die User-Agent Kennung zu ändern, gibt man in der Adresszeile `about:config` ein und setzt die angegebenen Variablen auf die Werte. Alle Werte sind vom Typ *String*. Die folgenden Einstellungen des JonDoFox und TorBrowser kann man für Firefox 10.0.x (esr) und auch für Firefox 11 | 12 | 13 nutzen, wenn man einen eher seltenes Betriebssystem nutzt.

Variable	Wert
general.useragent.override	Mozilla/5.0 (Windows NT 6.1; rv:10.0) Gecko/20100101 Firefox/10.0
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	0

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. Die Nutzung der Geolocation API erfolgt mit Javascript. Da man Javascript auf vielen Seiten freigeben muss, ist eine Deaktivierung der Geolocation-API sinnvoll. Dann kann ein Webserver den Standort nur relativ ungenau anhand der IP-Adresse ermitteln.

Bei Firefox wird die Geolocation API unter *about:config* deaktiviert, indem folgende Variable auf *FALSE* gesetzt wird:

```
geo.enabled = false
```

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

Kill Switch für Add-ons abschalten

Die extension blocklist⁵⁹ 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
```

⁵⁹ <https://addons.mozilla.org/en-US/firefox/blocked>

4.14 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 *CookieMonster* + *NoScript* + *AdBlock Plus* + *RefControl*. Viele Add-ons bieten Funktionen, die von dieser Kombination bereits abgedeckt werden. Andere sind einfach nur überflüssig.

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 Surfracker, die ignoriert werden.

Die Add-ons NoScript und AdBlock erledigen diese Aufgabe besser. Kategorie: *echtes Snakeoil*

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 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 oder Startingpage.com, für E-Mails einen Provider nutzen, der den Inhalt der Nachrichten nicht indexiert, openstreet-map.org statt Google-Maps verwenden. . . Kategorie: *gefährliches Snakeoil*

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 Tracker blockiert, die AdBlock mit den *Privacy Listen* sehr gut blockiert.
- *No FB Tracking* blockiert die Facebook Like Buttons, das kann AdBlock aber besser. Die *SocialMediaBlock* Listen von AdBlock 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 auch den Datensammler Rapleaf.com aufgebaut hat, als einer der Hauptinvestoren die Entwicklung von Facebook maßgeblich mitbestimmt und zum Steering Committee der Bilderberg Konferenzen gehört.

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. Internationales Aufsehen erregte die Sperrung der Konten von Wikileaks. Daneben gibt es viele weitere, weniger bekannte Fälle. Mehr als 30 deutschen Online-Händlern wurden die Konten gesperrt, weil sie kubanische Produkte (Zigarren, Rum, Aschenbecher) in Deutschland anboten. Begründet wurde diese Sperrung mit einem amerikanischen Handelsembargo gegen Kuba, das für Europäer eigentlich 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.

Bezahl systeme 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 Bezahlungssystem 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 Reisepreise 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 Bezahlungsmethoden 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.

5.1 Paysafecard, UKash, Liberty Reserve, 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.

Hinweis 1: Eine PaySafeCard ist 12 Monate uneingeschränkt gültig. Danach werden für jeden weiteren Monat 2 Euro vom Guthaben abgezogen. Es ist also sinnvoll, kleinere Guthaben bei Bedarf zu kaufen. Das verhindert auch eine technisch mögliche Verkettung mehrerer Einkäufe über den gleichen Gutscheincode.

Hinweis 2: nach praktischen Erfahrungen von sind die Verkäufer im Supermarkt, Tankstellen u.ä. nicht immer über die angebotene Möglich-

keit des Verkaufes von Paysafecard Gutscheinen informiert. Hartnäckig bleiben und die Verkäuferin auf das Paysafecard Symbol im GUI der Kasse hinweisen hilft.

Hinweis 3: 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 per E-Mail an den Support von PaySafeCard wenden und kann gegen Vorlage einer Kopie des GutscheinCodes einen Ersatzgutschein erhalten. Auszahlung der Codes und Erstattung der Geldbeträge ist bei Vorlage von Ausweisdokumenten möglich.

Hinweis 4: Aufgrund des Gesetzes gegen Geldwäsche ist PaySafeCard gezwungen, die Anonymität des Zahlungsmittels einzuschränken. Deutsche Nutzer sollen (aber müssen nicht) auf der Website unter "My PaySafecard" 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.

Hinweis 5: 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 etwas 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 anonym, als mit PaySafeCard.

Mit UKash Codes kann man Konten bei Liberty Reserve (via eCardOne) oder cashU aufladen. Dabei muss man sich jedoch mit einer Kopie des Ausweises oder Pass authentifizieren. Das ist praktisch und auch der einzige Weg, ein Konto bei cashU von Deutschland aus aufzuladen, aber man ist nicht mehr anonym gegenüber dem Zahlungsdienstleister.

- **Liberty Reserve:** ist ein weiterer vertrauenswürdiger Bezahlendienstleister im Web. Man muss einen Account erstellen, die Angaben werden aber nicht überprüft. Lediglich die E-Mail Adresse muss gültig sein. Bei Liberty Reserve werden getrennte Konten für Dollar und Euro geführt. Man muss darauf achten, welche Währung der Webshop akzeptiert.

Aufladen des Accounts mit Guthaben ist über verschiedene Exchanger möglich. Bei eCardOne kann man den Liberty Reserve Account mit UKash Codes aufladen, muss sich dafür aber neuerdings mit einer Ausweiskopie identifizieren. Da Liberty Reserve ein sehr großer Bezahl-dienstleister ist, gibt es viele unseriöse Anbieter, die ein Aufladen des Account versprechen aber nur die Zahlung einsacken und nichts dem Liberty Reserve Account gutschreiben (z.B. UCash Exchanger) oder Gebühren von mehr als 50% der Zahlung nehmen (z.B. cashvouchers).

Nutzen Sie nur die auf der Website von Liberty Reserve gelisteten und verifizierten Exchanger!

- **Pecunix:** wickelt Bezahlungen in Gold ab. Die Geldbeträge werden bei Bezahlung automatisch in Gold umgerechnet. Um mit Pecunix zu bezahlen, ist ein Account zu erstellen, bei dem ebenfalls lediglich die E-Mail Adresse gültig sein muss. Als einziger Bezahl-dienstleister 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:** ein Bezahl-service der hauptsächlich in der arabischen Welt angesehenes Zahlungsmittel ist. 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 (einen anderen Weg habe ich von Deutschland aus noch nicht gefunden), wenn man sich mit einer Kopie des Ausweises identifiziert.

5.1.1 Anonyme Online-Zahlungen vor dem Aus?

Die Bundesregierung bereitet unter dem Deckmantel des Kampfes gegen Geldwäsche ein Gesetz vor, das für anonyme Bezahlungen im Internet das Aus bedeuten könnte. Künftig sollen Verkaufsstellen von Paysafecards und UKash Vouchers die Käufer identifizieren und die Daten für eine mögliche Prüfung vorhalten. Im Gegensatz zu Bareinzahlungen, die statt bisher ab 15.000 Euro zukünftig ab 1.000 Euro berichtspflichtig werden, sollen für E-Geld keine Mindestgrenzen gelten. (<http://heise.de/-1269409>)

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 Prepaid-

karten eine Rolle. Das sind 0,7% aller Verdachtsfälle. Der Bundesdatenschutzbeauftragte Schaar hat sich gegen den Entwurf ausgesprochen:

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

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

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

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

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

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

5.2 Bitcoin

Bitcoin ist eine digitale Peer-2-Peer Währung ohne zentrale Verwaltung. Die Software löst mit kryptografischen Methoden vor allem ein Problem: Kopieren und mehrfache Verwendung der Bits und Bytes, die das *Bitcoin* repräsentieren, ist innerhalb des Netzwerkes nicht möglich.

Darauf aufbauend kann Bitcoin als Bezahlmethode verwendet werden.

- Bitcoins lassen sich in reale Währungen hin- und zurücktauschen. Der Kurswert der Bitcoins beim Tausch gegen reale Währungen (z.B. Euro) ergibt sich dabei ausschließlich aus dem Markt. Er wird nicht zentral festgelegt oder manipuliert.
- Die Bezahlungen können relativ schnell am PC abgewickelt werden. Es dauert in der Regel nur 1-2h, bis das Bitcoin Netzwerk eine Transaktion hinreichend bestätigt hat.
- Außerdem hat Bitcoin einen Inflationsschutz. Neue Bitcoins werden nach einem festen Schema generiert und die Gesamtzahl ist limitiert.

Viele Dienste im Netz akzeptieren Bitcoins als Bezahlung. Eine Übersicht findet man im Bitcoin Wiki. 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 der Anbieter vom mittleren Tauschkurs abweicht.

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. Die 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. Dann bestätigt der Verkäufer den Eingang des realen Geldes, die Bitcoins werden freigegeben und zum Käufer übertragen. Die Procedure kann je nach Zahlungsmethode 1-2 Tage dauern, dass sollte man einplanen.

In der Regel verwalten die Marktplätze / Exchanger im Web für Nutzer die gekauften Bitcoins. Das vereinfacht die Nutzung von Bitcoin als Zahlungsmittel, da keine Installation von Software nötig ist. Die erworbenen Bitcoins können aber auch auf den eigenen PC transferiert und lokal verwaltet werden. Hierfür muss ein Bitcoin Client installiert werden.

5.2.1 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 für Nutzer bereitstellen.

In der Regel verifizieren alle Exchange die Identität der Nutzer. Eine anonyme Nutzung ist meist nicht möglich. Hinweise zum anonymen Kauf von Bitcoins finden Sie unten im Abschnitt *Anonymität von Bitcoin*.

Für den Einstieg gefällt mir www.bitcoin.de sehr gut. Die Webseite wird professionell betreut, bietet in einer übersichtlichen Struktur alle nötigen Informationen für Kaufen, Verkaufen und die Verwaltung der eigene Bitcoins und ist für die ersten Schritte gut geeignet. Allerdings ist der Dienst nicht ganz kostenfrei. Es wird eine Gebühr von 1% für alle den Handel mit Bitcoins erhoben. Das ist jedoch wesentlich weniger, als bei anonymen Banküberweisungen anfällt.

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. Temporäre E-Mail Adressen sollten nicht genutzt werden, da bei jeder Transaktion Informationen per Mail ausgetauscht werden. Man kann zusätzliche Zahlungsmöglichkeiten wie Liberty Reserve oder Money Bookers.

Bitcoins kaufen: Im Marktbereich stehen in einer Liste mehrer 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 24h. 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.

Wichtig: Sie senden 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 4,00 Euro.
- Der Käufer überweist 3,98 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.

5.2.2 Anonymität von Bitcoin

Über die Anonymität von Bitcoin gibt es viele Missverständnisse. So wie jeder Geldschein eine eindeutige Nummer hat und verfolgt werden kann, ist es einem potenten Beobachter auch möglich, Bitcoin Zahlungen zu verfolgen.

Alle Bitcoin Transaktionen werden im *ewigen Logfile* protokolliert, das öffentlich zugänglich ist. Das ist kein Designfehler sondern notwendig, um double spending zu verhindern. Forscher der TU Darmstadt haben auf dem 28C3 eine Analyse der Anonymität von Bitcoin¹ vorgestellt. Eine weitere Analyse² wurde von D. Ron und A. Shamir publiziert. In beiden Analysen konnten mehrere scheinbar unabhängige Bitcoin Adressen auf einen Account zurück führen und die IP-Adressen von Spendern an öffentlich publizierte Bitcoin Adressen ermitteln. Dazu zählen beispielsweise Spenden an Wikileaks via Bitcoin. Außerdem wurden als Beispiel Zahlen zur Bitcoin Nutzung von Wikileaks veröffentlicht. Bis März 2012 nutzte Wikileaks 83 Bitcoin Adressen und erhielt 2605.25 BTC von Unterstützern.

Die Forscher kommen zu dem Schluss, dass die Anonymität von Bitcoin geringer ist, als eine einfache Banküberweisung. Informationen zu Banküberweisungen kann man nicht *einfach so* bekommen. Das Bankgeheimnis verwehrt einfachen Mitmenschen den Zugriff auf die Kontoinformationen ihrer Mitbürger. Die Bitcoin Transaktionen kann jeder analysieren.

Die CIA hat nach eigenen Aussagen Bitcoin als Zahlungsmittel bereits auf dem Radar. Im Juni 2011 wurde Gavin Andresen (ein führender Bitcoin Entwickler) ins CIA-Hauptquartier zu einer Präsentation eingeladen. (Daraus ergibt sich KEIN Grund für eine Verschwörungstheorie gegenüber den Bitcoin Entwicklern!)

¹ <http://events.ccc.de/congress/2011/Fahrplan/events/4746.en.html>

² <http://eprint.iacr.org/2012/584>

Bitcoin anonymisieren

Da der 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 ein Bitcoin-Brieftasche (eWallet) bei einem Webservice verwenden, das man mit JonDo oder Tor und einem Browser anonym verwalten kann.

- Blockchain.info³ bietet die Verwaltung eines anonymen eWallet auf dem Webserver und erfordert keine Angaben bei der Registrierung.
- StrongCoin.com⁴ erfordert die Angabe einer E-Mail Adresse bei der Registrierung. Wegwerfadressen werden akzeptiert.
- InstaWallet.org⁵ oder EasyWallet.org⁶ sind für die Verwaltung kleinerer Beträge geeignet. Eine Registrierung ist nicht nötig. Beim Aufruf der Webseite wird automatisch ein einmaliger Link generiert, der als Lesezeichen zu speichern ist. Zugriff auf das eWallet ist nur mit diesem Link möglich, es gibt keinen Passwortschutz.

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

- Bitcoins in Berlin⁷ bietet die Möglichkeit, Geld per Brief zu senden oder ein direktes Treffen zur Geldübergabe per E-Mail zu vereinbaren. Dem Geld ist der QR-Code der Bitcoin Adresse beizulegen, an welche die gekauften Bitcoins gesendet werden sollen. Den QR-Code kann man auf der Webseite btc.to generieren lassen.
- Auf der Webseite LocalBitcoins.com⁸ findet man weitere Anbieter in der Umgebung, die Bitcoins gegen Cash mit persönlicher Geldübergabe verkaufen.
- Im IRC Channel #bitcoin-otc kann man beliebige Formen der Geldübergabe mit dem Verkäufer vereinbaren.

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.

³ <https://www.blockchain.info/wallet>

⁴ <https://www.strongcoin.com>

⁵ <https://instawallet.org>

⁶ <https://easywallet.org>

⁷ <http://bitcoinsinberlin.com/>

⁸ <https://localbitcoins.com/>

Im Bitcoin-Wiki werden Mixing-Services wie Blockchain Mixing Service⁹ oder Cleanbit.org¹⁰ 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 können und einen potenten Angreifer nicht von einer Verfolgung der Transaktionen abhalten können.

⁹ <https://blockchain.info/wallet/send-anonymously>

¹⁰ <http://www.cleanbit.org/>

Kapitel 6

Allgemeine Hinweise zur E-Mail Nutzung

Die folgenden Hinweise beziehen sich in erster Linie auf den E-Mail Client Mozilla Thunderbird.

6.1 Mozilla Thunderbird

Informationen und Downloadmöglichkeiten für Mozilla Thunderbird stehen auf der deutschsprachigen Website des Projektes ¹ 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* (allerdings meist in einer veralteten Version). Das Mozilla Debian Team stellt eine aktuellere Version in einem separaten Repository und eine Anleitung² zur Installation bereit.

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 meist automatisch. Es können auch die Einstellungen eines bisher verwendeten Programms übernommen werden.

Standardmäßig schlägt Thunderbird beim Einrichten eines neuen Kontos ein IMAP-Konto vor. Bei diesem Kontotyp liegen alle E-Mails dauerhaft auf dem Server. Bei Nutzung eines POP3-Kontos (von mir empfohlen) werden die Mails lokal auf dem eigenen Rechner gespeichert und bleiben nicht in Ewigkeit auf dem Server liegen. Die Möglichkeit des weltweiten Zugriffs auf seine Mails bei IMAP-Konten erkauft der Nutzer sich mit einer Einschränkung

¹ <http://www.mozilla.org/de/thunderbird/>

² <http://mozilla.debian.net/>

des Datenschutzes³.

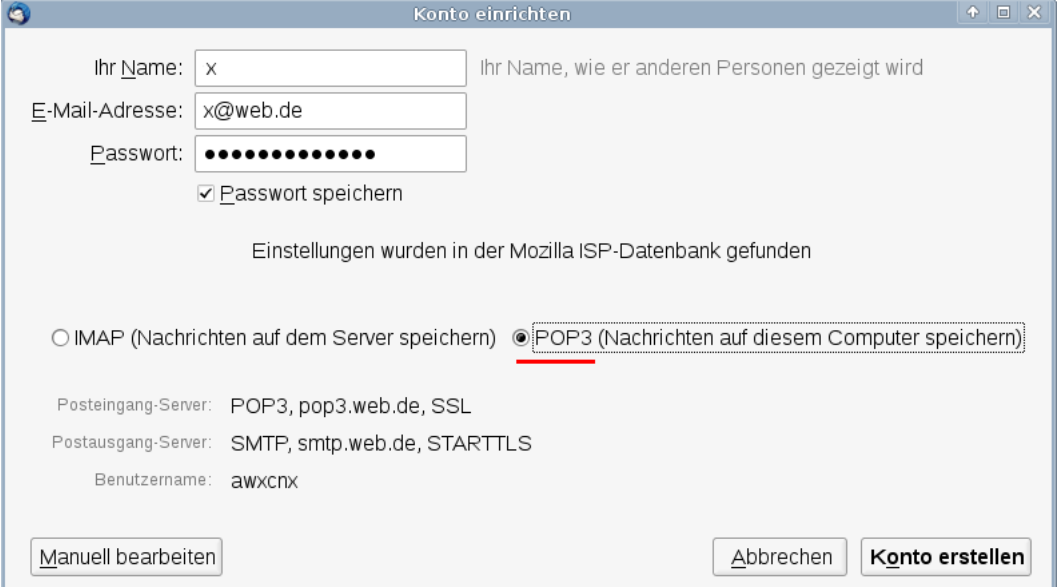


Abbildung 6.1: Assistent zur Einrichtung eines Account

6.1.1 Mehrere E-Mail Adressen nutzen

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 unten).

³ <http://blog.kairaven.de/archives/1060-Unsichere-und-geschuetzte-E-Mail-Sphaeren.html>

Eine kleine Liste von E-Mail Providern abseits des Mainstream:

- **Posteo.de** ⁴ und **aikQ.de** ⁵ (deutsche Mailprovider, Accounts ab 1,- Euro pro Monat, anonyme Accounts möglich)
- **Hushmail** ⁶ (kanadischer Mailprovider, kostenfreie Accounts nur via Webinterface nutzbar)
- **VFEmail** ⁷ (anonymer Mailprovider, benötigt eine Wegwerf-Adresse für Registrierung, kostenfreie Accounts mit POP3/SMTP und beliebig vielen temporären E-Mail Adressen)
- **SecureNym** ⁸ und **CryptoHeaven** ⁹ (kostenpflichtige, anonyme Mailprovider ab \$60 pro Jahr, bieten anonyme Accounts, einfache Verschlüsselung der Kommunikation mit Accounts beim gleichen Provider, Offshore registrierte Firmen)
- **XMAIL.net** ¹⁰ (die Betreiberfirma Aaex Corp. ist auf den British Virgin Islands registriert, die Server stehen in Kanada, kostenfrei Accounts mit POP3, aber ohne SMTP)
- **Lavabit** ¹¹ (US-amerikanische Mailprovider, anonyme Accounts möglich, sperrt Tor Nodes wegen häufigem Missbrauch, kostenfreie Accounts nur via Webinterface nutzbar)
- Cotse bietet keine kostenfreien Accounts, Preise ab \$50 pro Jahr

Für politische Aktivisten gibt es die Provider nadir.org, aktivix.org und ri-seup.net, die sich bemühen, die damit verbundenen Anforderungen zu erfüllen. Sie werden durch Spenden finanziert. Für einen Account muss man seine politischen Aktivitäten nachweisen, aber nicht unbedingt seine Identität offen legen.

Hinweis: es kostet Geld, einen zuverlässigen Mailservice bereitzustellen. Es ist durchaus sinnvoll, die *alles kostenlos Mentalität* für einen vertrauenswürdigen Mailprovider fallen zu lassen.

6.1.2 Wörterbücher installieren

Nach der Installation von Thunderbird sind keine Wörterbücher für die Rechtschreibkontrolle vorhanden. Die Wörterbücher müssen zusätzlich installiert werden, wenn man auf das Feature nicht verzichten möchte. Nach dem Download der Wörterbücher ¹² 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 6.2, kann man die Dateien mit den Wörterbüchern als Add-on installieren.

⁴ <https://posteo.de>

⁵ <https://www.aikq.de>

⁶ <https://www.hushmail.com/>

⁷ <https://www.vfemail.net>

⁸ <https://securenym.net>

⁹ <https://www.cryptoheaven.com/>

¹⁰ <https://www.xmail.net>

¹¹ <https://lavabit.com>

¹² <https://addons.mozilla.org/de/thunderbird/language-tools/>

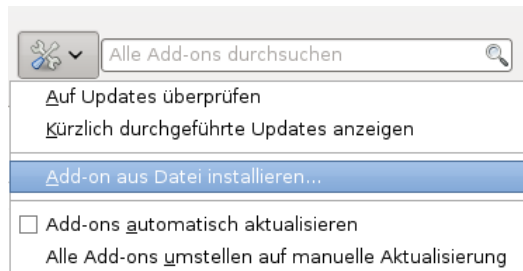


Abbildung 6.2: Wörterbücher in der Add-on Verwaltung installieren

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.

6.1.3 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.

6.1.4 Gesicherte Verbindungen zum Mail-Server

Die Grafik im Bild 6.3 zeigt den Weg einer E-Mail vom Sender zum Empfänger.

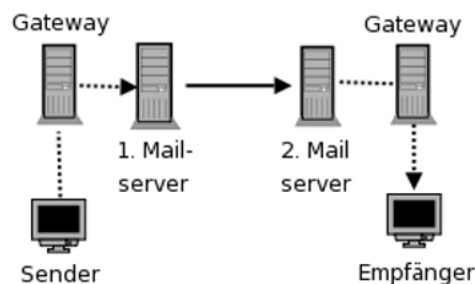


Abbildung 6.3: Der Weg einer E-Mail durch das Web

In der Regel sind die Rechner der Nutzer nicht direkt mit dem Internet verbunden. Der Zugang erfolgt über ein Gateway des Providers oder der

Firma.

Der 1. Mailserver nimmt die Mail via SMTP entgegen und sendet sie an den 2. Mailserver. Hier liegt die Mail, bis der Empfänger sie mittels POP3 abrufen. Mit dem Abrufen kann die Mail auf dem Server gelöscht werden. Es ist auch möglich, die Mail auf dem Server zu lesen, z.B. über ein Webinterface oder mittels IMAP-Protokoll.

Die im Bild 6.3 gestrichelt dargestellten Verbindungen zu den Mailservern können mittels 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.

Wie einfach es ist, ungesicherte Verbindungen zu belauschen, die Passwörter zu extrahieren und das Mail-Konto zu kompromittieren, wurde von T. Pritlove auf der re:publica 2007 demonstriert ¹³.

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 ¹⁴. 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.

Unsichere Verschlüsselungen deaktiviere

Aus Gründen der Kompatibilität mit einigen Mail-Providern unterstützt Thunderbird noch immer veraltete und unsichere Verschlüsselungsoptionen für die Verbindung zu dem Mailservern. In den *Erweiterten Einstellungen* kann man diese Optionen deaktivieren:

<code>security.enable_ssl3</code>	<code>= false</code>
<code>security.ssl.require_safe_negotiation</code>	<code>= true</code>
<code>security.ssl.treat_unsafe_negotiation_as_broken</code>	<code>= true</code>
<code>security.warn_submit_insecure</code>	<code>= true</code>

Wenn man die im Bild 6.4 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. Meistens bietet der Server keine Secure Renegotiation beim Aufbau der

¹³ <http://tim.geekheim.de/2007/04/24/netzwerksicherheit-auf-der-republica/>

¹⁴ <http://heise.de/-206233>

verschlüsselten Verbindung. Das Problem wird seit 2009 als schwingend eingestuft ¹⁵.

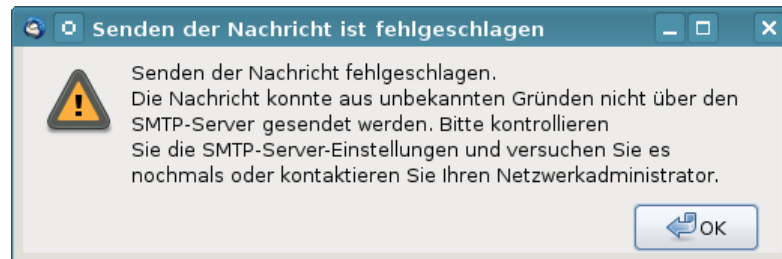


Abbildung 6.4: Fehlermeldung bei unsicherer Verbindung

In diesem Zusammenhang verweise ich auf die Antwort der Bundesregierung auf eine Kleine Anfrage zu Fernmeldeaufklärung des BND vom Mai 2012:

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

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

Tools zum Ausnutzen der Insecure Renegotiation gibt es auch als OpenSource (z.B. dsniff).

6.1.5 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 6.5).
- 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.

¹⁵ <https://www.verbraucher-sicher-online.de/news/fehlerhaftes-design-im-wichtigsten-verschluesselungsprotokoll-fuer-angriffe-nutzbar>

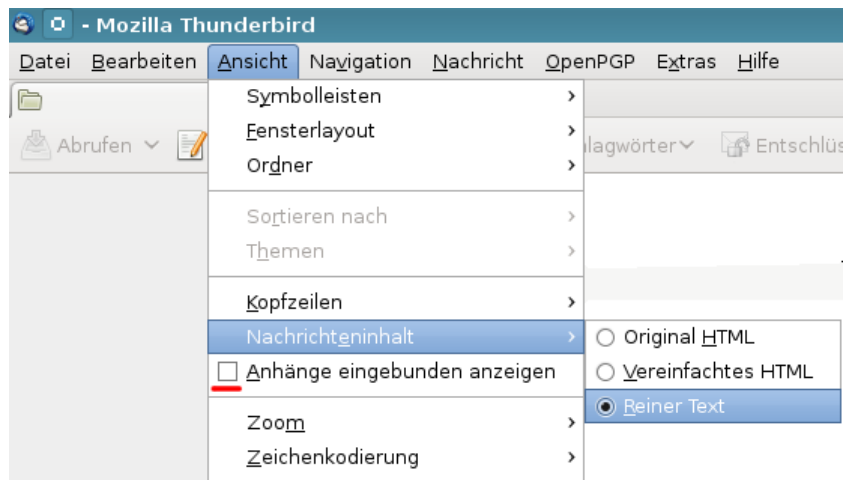


Abbildung 6.5: E-Mails als reinen Text darstellen

- 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
security.enable_tls_session_tickets	= false
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 Trackingservice geladen wird:

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

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

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

Um Tracking mit Bildern und HTML-Wanzen zu verhindern, kann man in den *Erweiterten Einstellungen* das Laden externer Bilder blockieren:

```
permissions.default.image = 2
```

Auch andere Medienformate können von einem externen Server geladen und als Wanzen genutzt werden. Einen 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
```

- Gespeicherte Passwörter für den Zugriff auf SMTP-, POP- oder IMAP-Server können mit einem Masterpasswort geschützt werden.

6.1.6 Datenverluste vermeiden

Die folgenden Hinweise wurden von den Mozilla-Entwicklern erarbeitet, um den Nutzer bestmöglich vor Datenverlusten zu schützen:

- Das Antiviren-Programm ist so einzustellen, dass es den Profilordner von Thunderbird NICHT(!) scannt. Die automatische Beseitigung von Viren kann zu Datenverlusten führen.
- Der Ordner *Posteingang* sollte so leer wie möglich gehalten werden. Gelesene E-Mails sollten auf themenspezifische Unterordner verteilt werden.
- Die Ordner sollten regelmäßig komprimiert werden. 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 6.6). 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.

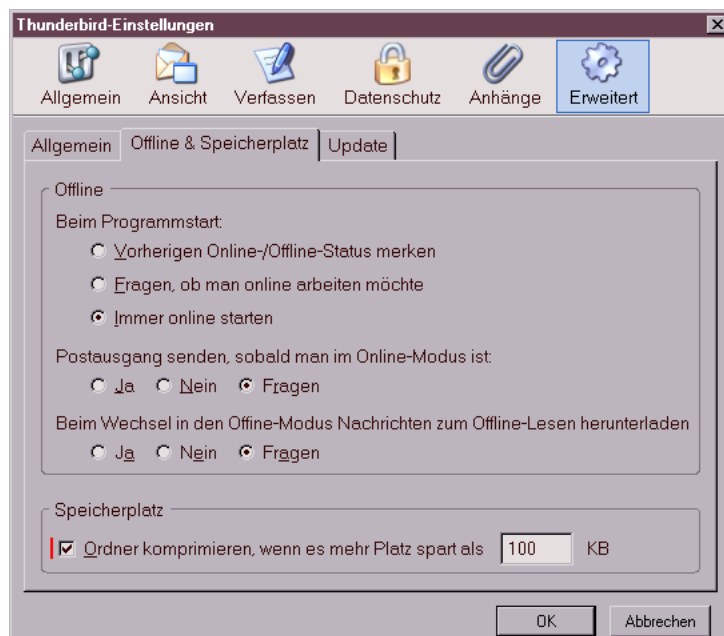


Abbildung 6.6: Ordner automatisch komprimieren

6.1.7 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.

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.

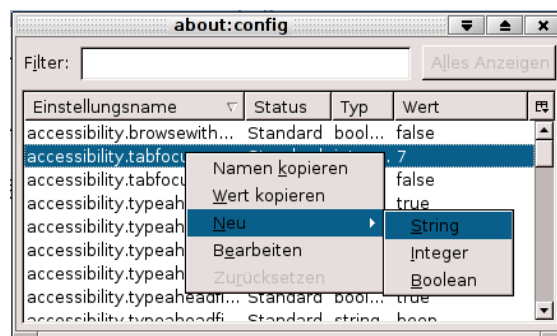


Abbildung 6.7: Neue Config-Variable anlegen

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
```

6.1.8 Spam-Schutz

Man muss nicht bei jeder Gelegenheit im Web seine richtige E-Mail Adresse angeben. Damit fängt man sich eine Menge Spam (Junk) ein.

Außerdem ist die E-Mail Adresse ein wichtiges Identitätsmerkmal. Datensammler 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.

Um die eigene E-Mail Adresse nicht zu kompromittieren und trotzdem Angebote zu nutzen, welche die Angabe einer Mailadresse erfordern, kann man temporäre *Wegwerf-Adressen* nutzen.

Bei der Nutzung temporärer Mailadressen geht es nicht(!) um die Umgehung der Vorratsdatenspeicherung. Hinweise dafür findet man im Abschnitt *“E-Mail anonym nutzen”*.

AnonBox des CCC

Bei der AnonBox des CCC ¹⁶ kann ein E-Mail Account für den Empfang von Nachrichten 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! Versenden von Nachrichten ist nicht möglich.

Beim Erzeugen einer E-Mail Adresse erhält man einen Link, unter dem man ankommende Mails lesen kann. Der Link ist als Lesezeichen zu speichern, wenn man später nochmal nachschauen möchte, ob neue Mail eingetroffen sind.

10min - 120min Mail-Adressen

Man kann auf den Webseiten der Anbieter mit einem Klick eine E-Mail Adresse anlegen, die für 10min...12h gültig ist (ja nach Anbieter). Bei Bedarf kann die Verfügbarkeit der E-Mail Adresse verlängert werden. Das reicht, um sich in einem Forum anzumelden oder einen Blog-Kommentar zu posten.

¹⁶ <https://anonbox.net>

- www.10minutemail.com (10min gültig, verlängerbar)
- mail2null.nl (10min gültig, Session-Cookies freigegeben)
- www.spamsalad.in (sehr schön gemacht, 10min gültig, Session-Cookies und Javascript freigegeben)
- tempemail.co.za (30min gültig, Session-Cookies freigegeben)
- Squizzly.de (60min gültig, Session-Cookies freigegeben)
- sector2.org (120min gültig, Session-Cookies freigegeben)
- topranklist.de (12h gültig, Session-Cookies freigegeben)

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.

6-12h Mail-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@sofort-mail.de* kann man überall und ohne Vorbereitung unbekümmert angeben. Das Postfach ist unbegrenzt gültig.

In einem Webformular auf der Seite des Betreibers findet man später alle eingegangenen Spam- und sonstigen Nachrichten für das gewählte Pseudonym. Für das Webinterface des Postfachs gibt es in der Regel keinen Zugriffsschutz. Jeder, der das Pseudonym kennt, kann die Nachrichten lesen und löschen. Nachrichten werden nach 6-12h automatisch gelöscht.

Liste einiger Anbieter (unvollständig):

- <http://www.spambog.com> (weitere E-Mail Domains auf der Webseite, Account kann mit Passwort gesichert werden, Löschen der Mails ist möglich, Session-Cookies erforderlich, VDS-artige Speicherung der IP-Adressen)
- <http://onewaymail.com> (weitere E-Mail Domains auf der Webseite, keine Cookies oder Javascript nötig, E-Mails können gelöscht werden)
- <http://dudmail.com> (weitere Domains auf der Webseite, Weiterleitungen können eingerichtet werden, Mails werden 14 Tage gespeichert)
- <http://www.sofort-mail.de>

- <http://www.trash-mail.com>
- <http://dodgit.com>
- <http://www.mailinator.com/>
- <https://www.privvy-mail.de> (Javascript erforderlich, SSL-verschlüsselt)

In einem Webformular auf der Seite des Betreibers findet man alle eingegangenen Spam- und sonstigen Nachrichten für das gewählte Pseudonym. Für das Webinterface des Postfachs gibt es keinen Zugriffsschutz. Jeder, der das Pseudonym kennt, kann die Nachrichten lesen. Alle eingegangenen Nachrichten werden nach 6-12h meist automatisch gelöscht.

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.

Firefox Add-on Bloody Vikings

Das Firefox Addon *Bloody Vikings* ¹⁷ vereinfacht die Nutzung von Wegwerf-adressen. Nach der Installation von der Webseite kann ein bevorzugter Dienst für die Wegwerfadressen gewählt werden.

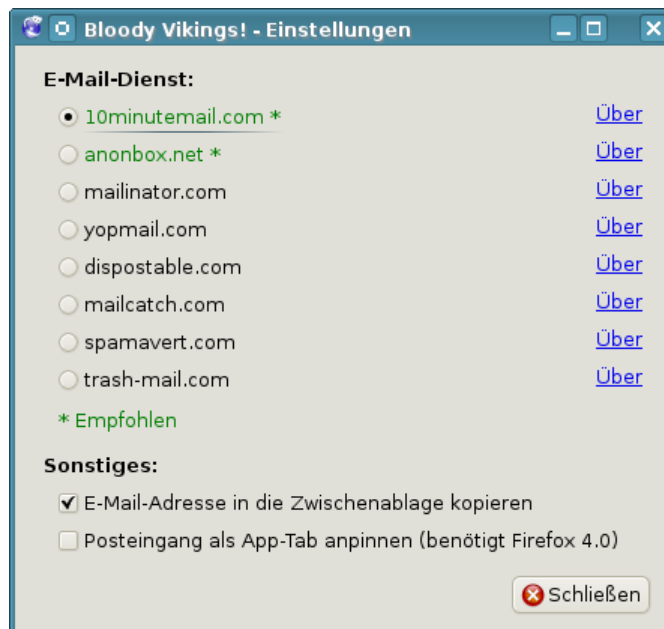


Abbildung 6.8: Bloody Vikings konfigurieren

¹⁷ <https://addons.mozilla.org/de/firefox/addon/bloody-vikings>

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.

6.1.9 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, dass eine vertrauliche Nachricht von Dritten gelesen wird. Verschlüsselung wäre eine naheliegende Lösung. Das ist aber nur möglich, wenn Absender und Empfänger über die nötige Kompetenz verfügen.

Als Alternative kann man folgende Dienste nutzen:

- *Certified Privnote*¹⁸ ist vom ULD mit dem EuroPrise Siegel zertifiziert. Die Zertifizierung garantiert die Respektierung der Privatsphäre der Nutzer durch den Anbieter.
- *Privnote*¹⁹ wird ebenfalls von der Firma insophia betrieben. In dieser nicht-zertifizierten Version sind Änderungen an der Software und Weiterentwicklungen möglich.
- *Burn Note*²⁰ ist ein weiterer Dienst dieser Kategorie, den man nutzen kann.

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.

PrivNote und *BurnNote* sind 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

¹⁸ <https://certified.privnote.com>

¹⁹ <https://privnote.com>

²⁰ <https://burnnote.com>

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.

6.1.10 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 YouSendIt²¹ und Box.net²² 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.

²¹ <https://www.yousendit.com>

²² <https://www.box.com/>

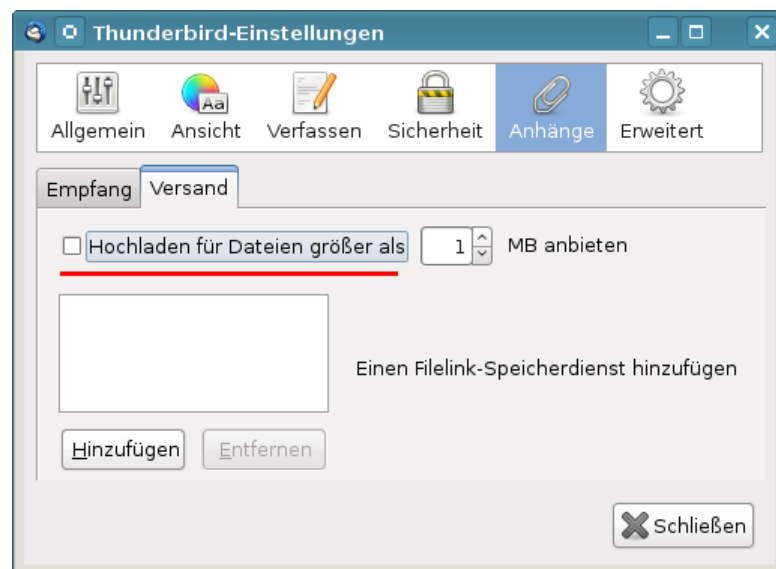


Abbildung 6.9: Filelink deaktivieren

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 beim Schnorcheln anfallenden Datenmengen. Für Syrien, Iran, Saudi Arabien 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. 37 Mio. E-Mails meldeten die Scanner im Jahr 2010 als verdächtig, die näher analysiert 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 selbst 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.

Linux: alle Distributionen installieren GnuPG standardmäßig.

MacOS: nutzen Sie die GPGTools ¹.

Windows 1: Das Projekt gpg4win ² stellt ein Paket für Windows bereit mit GnuPG v. 2.0 und dem GNU Privacy Assisten für die Schlüsselverwaltung.

Windows 2: Ich kann auch das Paket GpgSX ³ empfehlen, welches neben GnuPG einige zusätzliche Tools enthält (grafische Schlüsselverwaltung, Erweiterung für den Explorer).

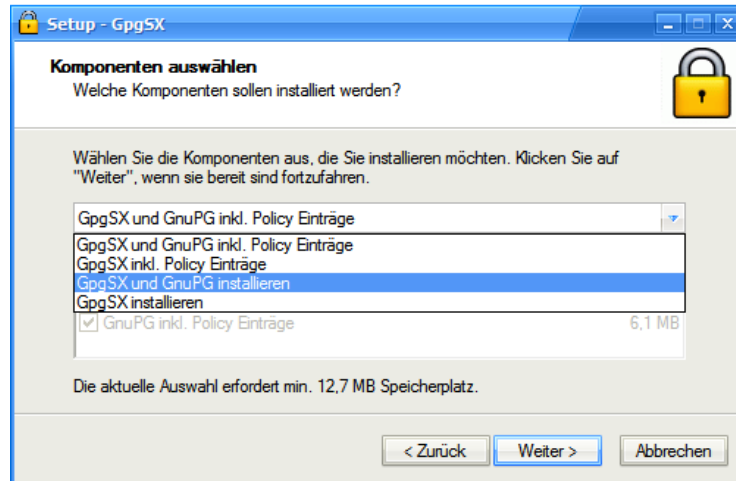


Abbildung 7.1: GpgSX Installation

Nach dem Download ist das Setup-Programm zu starten und den Anweisungen zu folgen. Die Komponenten GnuPG und GpgSX sind zu installieren.

¹ <http://www.gpgtools.org>

² <http://www.gpg4win.org>

³ <http://gpgsx.berlios.de>

7.1.2 Installation der Enigmail-Erweiterung

Enigmail⁴ 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.

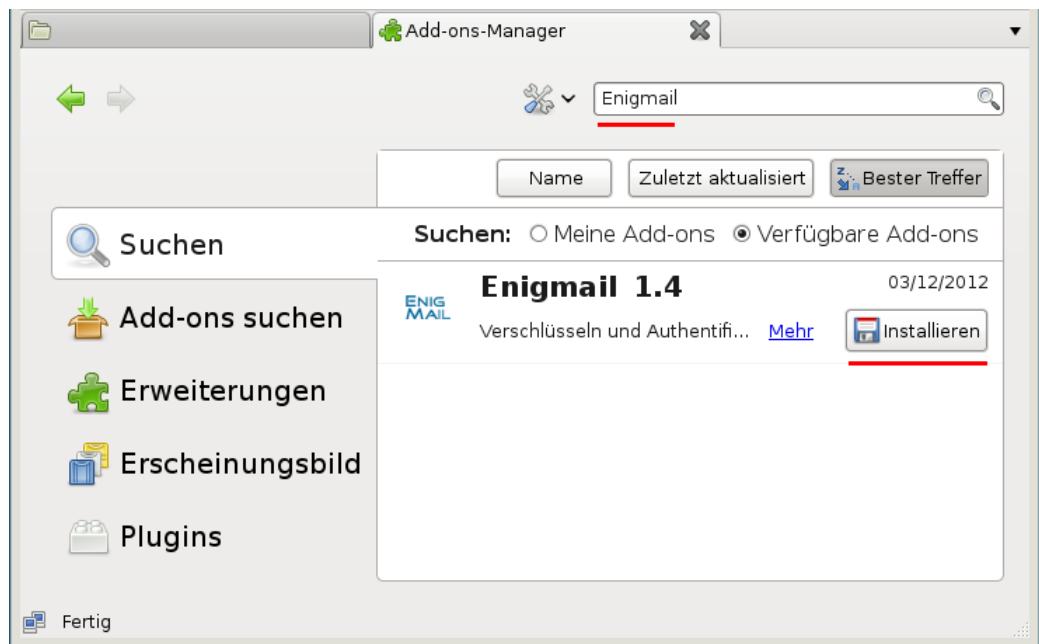


Abbildung 7.2: Installation von EnigMail

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.
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 <http://enigmail.mozdev.org>

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 Kryptoanalys 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.

7.1.3 Schlüsselverwaltung

Die Schlüsselverwaltung findet man in Thunderbird unter dem Menüpunkt *OpenPGP - 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.

Exportieren des eigenen öffentlichen Schlüssels

Um verschlüsselt zu kommunizieren, muss den Kommunikationspartnern der eigene öffentliche Schlüssel zur Verfügung gestellt werden. Der einfachste Weg nutzt die Schlüsselserver im Internet. In der Schlüsselverwaltung findet man den Menüpunkt *Schlüssel-Server / Schlüssel hochladen*. Der öffentliche Schlüssel wird auf den Schlüsselserver exportiert und steht dort allen Partnern zur Verfügung. Die verschiedenen Server synchronisieren ihren Datenbestand.

Alternativ könnte man den öffentlichen Schlüssel als E-Mail Attachment versenden oder als Datei auf einem Webserver ablegen. Den Menüpunkt für

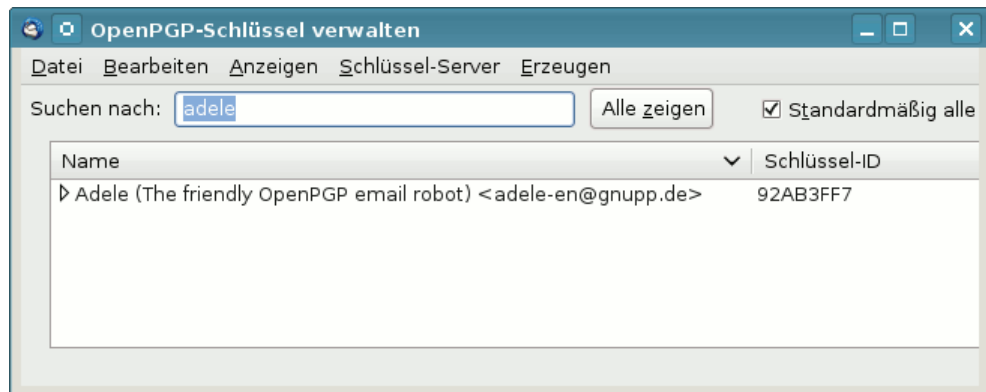


Abbildung 7.3: Schlüsselverwaltung von EnigMail

den Export in eine Datei findet man unter *Datei - Schlüssel exportieren* in der Schlüsselverwaltung. Um den Schlüssel als Attachment an eine Mail anzuhängen, aktivieren Sie die Option *OpenPGP - Meinen öffentlichen Schlüssel anhängen* beim Schreiben einer Mail wie im Bild 7.4 zu sehen.

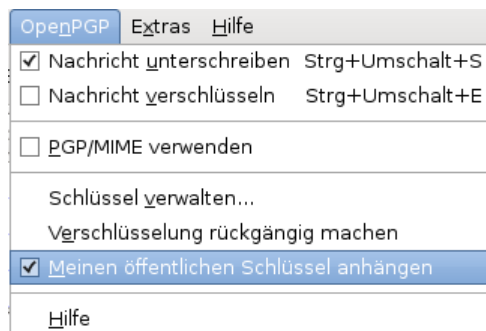


Abbildung 7.4: OpenPGP-Schlüssel versenden

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*

- Wenn der Schlüssel als Text angeboten wird, sieht es etwa so aus:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.1

mQENBEt5GIIBCAC0n0eTtfBIUbdC0mw5D1LuxkQB4uQ/8HbSUaH96s1z
HqFA/31GB70podyEKqc41T2DdWWITfdy1dpXeGwopBK/wljPAuNagJQ
....
fU7xEW/RQT76n0RfTXnbj2m/DRPmoivcXW5G/zJM6QUj1++v070B+3xb
SnDCMQtawHM57eLcmnsMAK3qH0Y1VrNUTSvEgatjUqLU
=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 7.5 dargestellt mit *Bearbeiten - Aus Zwischenablage importieren*.



Abbildung 7.5: OpenPGP-Schlüssel aus Zwischenablage importieren

- Auch ohne eine signierte E-Mail erhalten zu haben, kann man die Schlüsselservers nach dem zu einer E-Mail Adresse gehörenden Schlüssel durchsuchen. Die Funktion findet man unter dem Menüpunkt *Schlüssel-Server / Schlüssel suchen*. Man gibt in der sich öffnenden Dialogbox die E-Mail-Adresse des Empfängers ein und bestätigt mit Ok.

Wurden zur Suchanfrage passende Schlüssel gefunden, werden diese in einer Liste angezeigt. Wählen Sie aus dieser Liste den zu importierenden Schlüssel und bestätigen Sie mit OK. Wenn mehrere passende Schlüssel für eine E-Mail Adresse gefunden wurden, ist in der Regel der neueste Schlüssel die richtige Wahl.

7.1.4 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 ist für jede E-Mail explizit festzulegen, dass sie verschlüsselt werden soll.

Das Fenster für das Erstellen einer neuen E-Mail (Bild 7.7) zeigt nach der Installation des Enigmail-PlugIns einen neuen Button *OpenPGP*. Klickt man auf diesen Button, öffnet sich der im Bild 7.7 gezeigte Dialog, der es

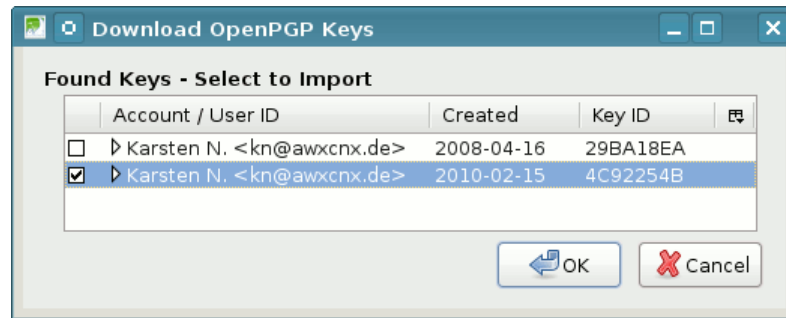


Abbildung 7.6: Mehrere OpenPGP-Schlüssel gefunden

ermöglicht, die Krypto-Eigenschaften für diese E-Mail festzulegen.

Sollte die E-Mail Anhänge enthalten, ist die Option *PGP / MIME* zu aktivieren, um die Attachements standardkonform zu verschlüsselt.

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.

Alternativ ist es auch möglich, lediglich für bestimmte Empfänger festzulegen, dass alle E-Mails signiert oder verschlüsselt werden sollen. Für die Festlegung dieser Regeln ist der entsprechende Dialog über *OpenPGP / Empfängerregeln* in Thunderbird zu öffnen.

7.1.5 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 7.4)

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:

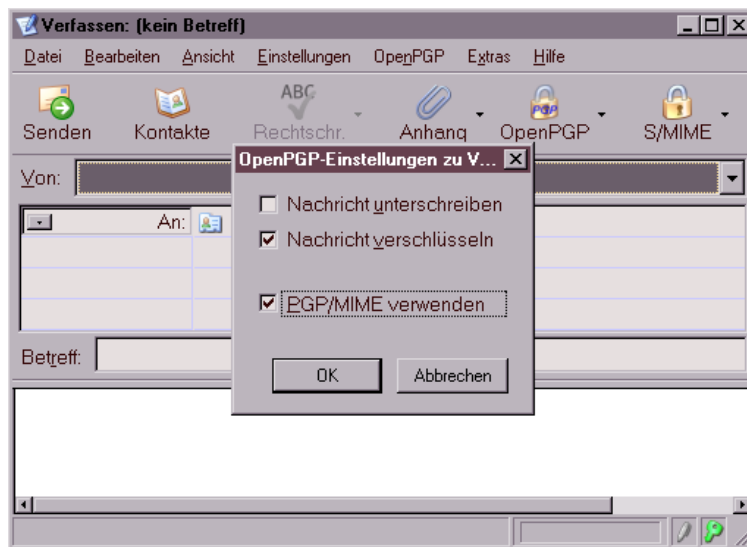


Abbildung 7.7: Signieren und Verschlüsseln einer E-Mail

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
RouuaDQukNINWk2V2Er0WzFnJqdzpapeuPJi0Wp0uIEvU3FRPhYlytw9dFfwAHv4
MJ7639tAx9PfXBmZ0d1PAoE451+VLhIG1LQiFGFppJ57SZ1EQ71/+/nkSwCg8Mge
....
EQIABgUCPIWU1QASCRD1czRpkqs/9wd1R1BHAAEBv20AoJJGeeZjMCSbXtmNSwfW
QsL0d0+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.

7.1.6 Verschlüsselung in Webformularen

Auch bei der Nutzung eines Webmail Accounts oder Webforms für die Versendung anonymer E-Mails muss man auf Verschlüsselung nicht verzichten.

Einige grafische Tools für die Schlüsselverwaltung wie z.B. GPA (*GNU Privacy Assistant*)⁵ oder KGPG 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.

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**⁶ bietet einen Editor mit den Buttons für das Ver- und Entschlüsseln des Textes, Dateiverschlüsselung sowie eine kleine Schlüsselverwaltung (Signieren und Prüfen der Signatur steht noch auf der ToDo Liste). Das ZIP-Archiv enthält Versionen für Windows und Linux. Es kann einfach auf dem USB-Stick genutzt werden.
2. Die Applikation **Portable PGP**⁷ ist eine Java-Anwendung (plattformunabhängig), die 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.

⁵ http://www.gnupg.org/related_software/gpa/index.de.html

⁶ <http://gpg4usb.cpunk.de>

⁷ <http://ppgp.sourceforge.net>

7.1.7 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* ⁸ 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 ⁹.

CryptoStick: Da das Handling mit CardReader und SmartCard unter Umständen etwas umständlich sein kann, wurde ein USB-Stick entwickelt, der CardReader plus eine SmartCard in einem kleinen Gehäuse enthält und voll kompatibel mit der Version 2.0 der OpenPGP SmartCard ist. Weitere Informationen gibt es auf der Webseite des Projektes ¹⁰.



Abbildung 7.8: CryptoStick

Hardware-Treiber installieren

Vor der Nutzung der SmartCard ist der Hardware-Treiber für den CardReader zu installieren.

⁸ <http://www.elcomsoft.de/programme/edpr.html>

⁹ <http://www.kernelconcepts.de/shop/products/security.shtml?hardwaree>

¹⁰ <http://www.crypto-stick.com>

- WINDOWS: Die Lieferung des CardReaders von kernelconcepts.de enthält eine CD mit den nötigen Treiber für WINDOWS. Das zum Gerät passende ZIP-Archiv ist zu entpacken und *setup.exe* als Administrator zu starten.

Für den CryptoStick gibt es den PC Twin USB PC/SC Treiber ¹¹.

- Linux: Da Linux out-of-the-box viel mehr Hardware unterstützt als Windows, sind die nötigen Treiber in den Repositories enthalten. Unter Debian/Ubuntu installiert man alles Nötige für die Nutzung der SmartCard mit folgendem Kommando:

```
# aptitude install pcscd libpcsc-lite1 libccid
```

Die Pakete *openct* und *opensc* sollten entfernt werden, da diese zu Beeinträchtigungen führen können.

```
# aptitude purge openct opensc
```

Außerdem benötigen die aktuelle OpenPGP-SmartCard und der CryptoStick GnuPG mindestens in der Version 1.4.9+ oder die 2.0.12+. Unter WINDOWS funktioniert erst die Version 1.4.10. Aktualisieren sie ihre GnuPG Version, wenn nötig.

Wer "gpg2" nutzen möchte, sollte beachten, dass der "gpg-agent" unbedingt nötig ist. In der Datei *\$HOME/.gnupg/gpg.conf* ist am Ende einfach ein *use-agent* einzufügen. Dann meldet man sich vom Desktop ab und wieder an.

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 .... D27600xxxxxxxxxxxxxxxx
Version ..... 2.0
Manufacturer ..... unknown
....
```

SmartCards und CryptoStick mit Enigmail nutzen

Enigmail ist seit der Version 1.0.1 voll kompatibel mit der SmartCard und dem CryptoSick. Das Add-on bietet eine grafische Oberfläche, um die SmartCard zu verwalten. Diese Funktionen öffnet man über den Menüpunkt *OpenPGP - Smartcard verwalten*.

1. Als Erstes kann man die Card personalisieren und den Namen usw. editieren, eine 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

¹¹ <http://support.gemalto.com/?id=46>

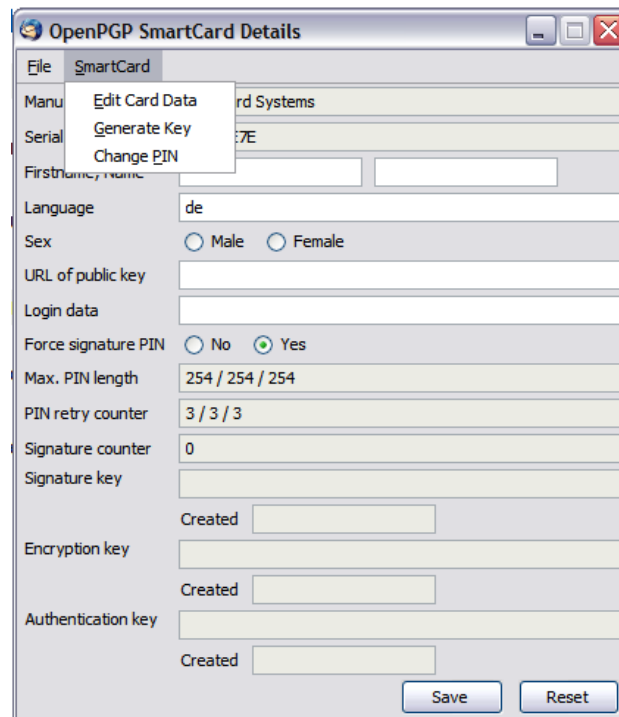


Abbildung 7.9: SmartCard verwalten

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.

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



Abbildung 7.10: SmartCard-PINs ändern

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.

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 einen 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 zerstört!

7.1.8 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 [7.11](#) zeigt eine mögliche Variante für den Key von Anton (A).

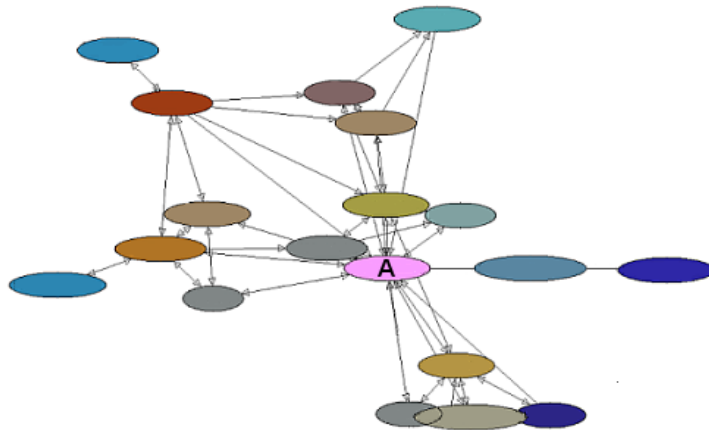


Abbildung 7.11: Beispiel für ein Web of Trust

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 7.12 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*.

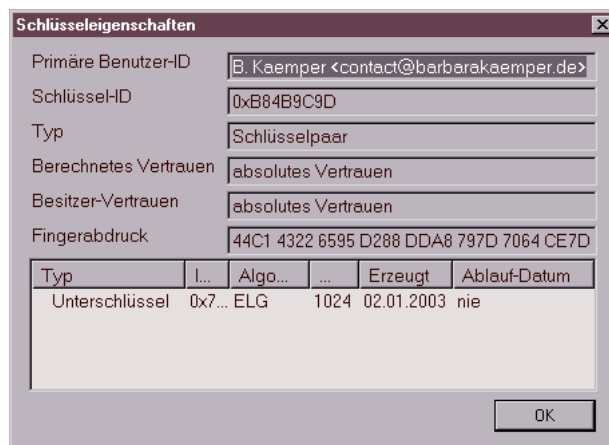


Abbildung 7.12: Schlüssel-Eigenschaften

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
- Krypto-Kampagne der Zeitschrift Ct
- 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
```

7.1.9 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 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 Assurern 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 eigenen 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 7.13).

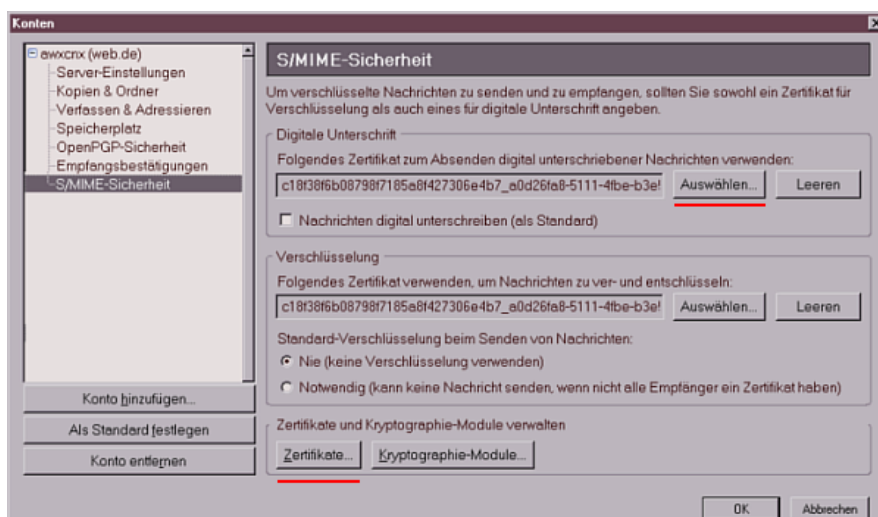


Abbildung 7.13: Kontoeinstellungen zur S/MIME-Sicherheit

Zuerst ist das persönliche Zertifikat zu importieren. Ein Klick auf den Button *Zertifikate* öffnet den Manager für eigene Zertifikate (Bild 7.14). Hier ist der Button *Importieren* zu wählen und das gespeicherte persönliche Zertifikat mit öffentlichem und geheimem Schlüssel zu importieren.

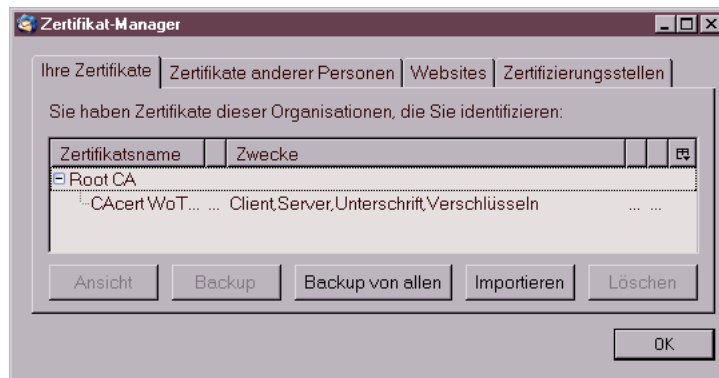


Abbildung 7.14: Zertifikatsmanager für eigene Zertifikate

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 7.15), um die Verwaltung zu öffnen.

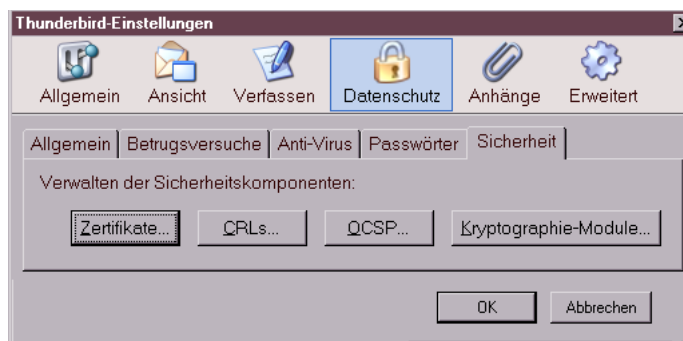


Abbildung 7.15: Dialog Sicherheits-Einstellungen

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 7.16 dargestellte Menü zum Festlegen der Kryptographie-Optionen für die aktuelle

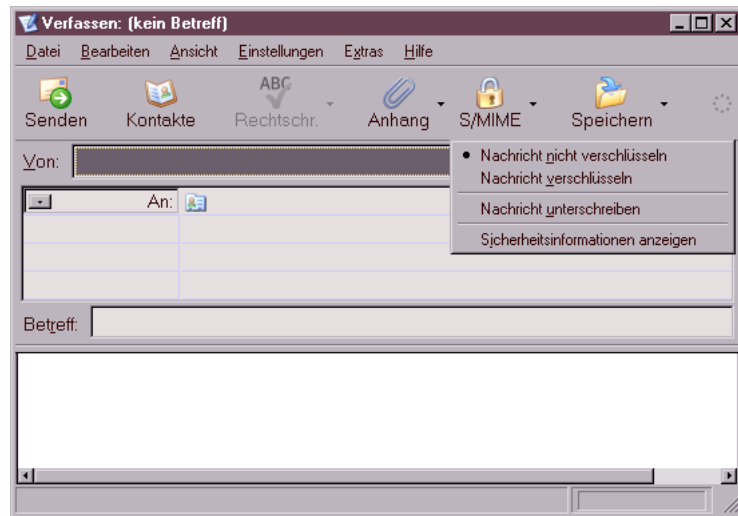


Abbildung 7.16: Verschlüsseln oder Signieren einer E-Mail

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 7.17)

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.

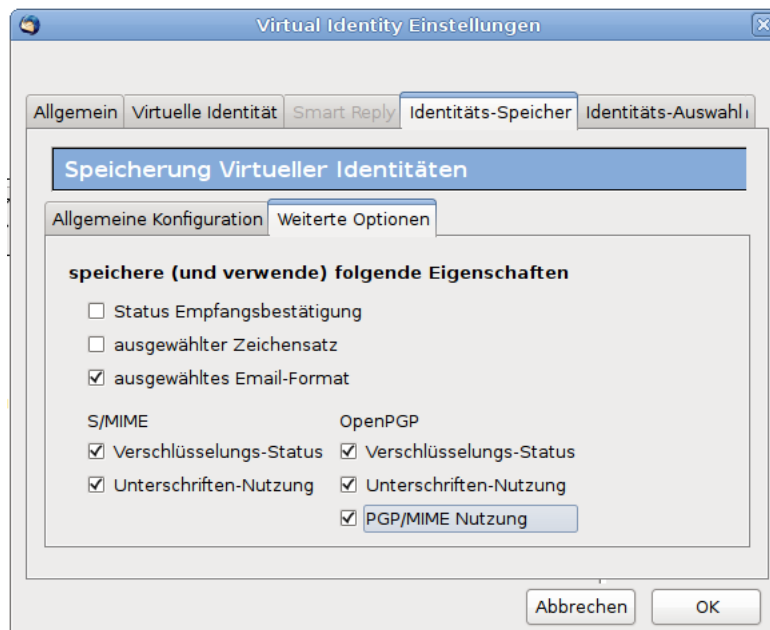


Abbildung 7.17: Einstellungen des Plug-In Virtual Identity

7.3.1 Webbrowser Firefox

Nutzer des Browsers Firefox klicken auf auf das *Root Certificate* und aktivieren in dem sich öffnenden Dialog (Bild 7.18) 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 7.19 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).

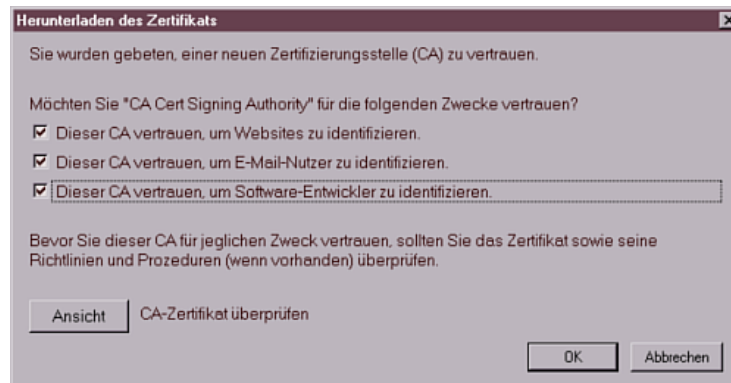


Abbildung 7.18: Herunterladen eines Zertifikates

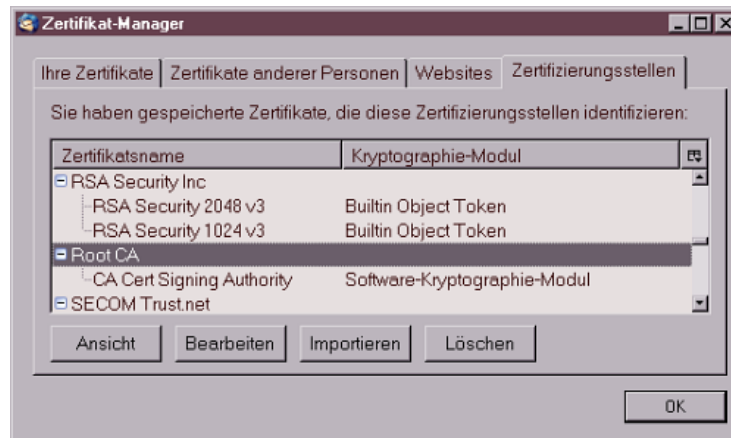


Abbildung 7.19: Zertifikats-Manager von Thunderbird

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-zertifikaterstellung.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.

The screenshot shows a window titled "Erstelle CA" with a sub-header "Neue CA erstellen". It contains a form with the following fields and values:

- Name (für die lokale Speicherung): Test
- Daten für das CA Zertifikat
- Common Name (für die CA): Test_CA
- Land (2 Buchstaben-Code): DE
- Passwort (zum Signieren):
- Passwort (Bestätigung):
- Bundesstaat oder Provinz: Berlin
- Standort (z.B. Stadt): Berlin
- Organisation (z.B. Firma): privat
- Organisationseinheit (z.B. Abteilung):
- eMail Adresse: admin@test_ca.de
- Gültigkeit (in Tagen): 3650
- Schlüssellänge: ☐ 1024 ☐ 2048 ☒ 4096
- Digest: ☒ SHA-1 ☐ MD2 ☐ MDC2 ☐ MD4 ☐ MD5 ☐ RIPEMD-160

At the bottom, there are two buttons: "OK" and "Abbrechen".

Abbildung 7.20: 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 7.21). 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)

eMail Adresse:

Passwort (sichert den privaten Schlüssel):

Passwort (Bestätigung):

Land (2 Buchstaben-Code)

Bundesstaat oder Provinz:

Standort (z.B. Stadt):

Organisation (z.B. Firma):

Organisationseinheit (z.B. Abteilung):

Schlüssellänge: ☒ 4096 ☐ 1024 ☐ 2048

Digest: ☒ SHA-1 ☐ MD2 ☐ MDC2 ☐ MD4 ☐ MD5 ☐ RIPEMD-160

Algorithmus: ☒ RSA ☐ DSA

Abbildung 7.21: 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

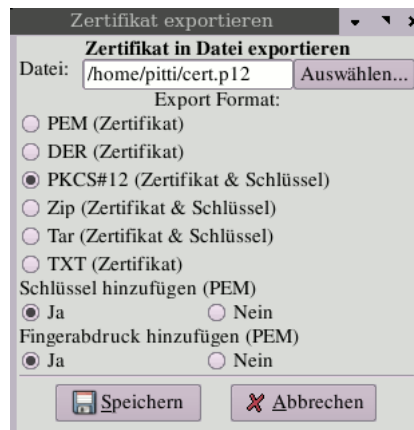


Abbildung 7.22: Zertifikat exportieren

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 Entschlüsseln 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 unbedachte 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 verschlüssel?”

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 Mailedienst.
- TorMail gibt es als Hidden Service unter <http://jhiwjllqpyawmpjx.onion> mit POP3 und SMTP Service und ist auch aus dem Web unter xxx@tormail.net erreichbar.
- Tor Privat Messaging unter <http://4eiruntyxxbgfv7o.onion/pm/> ist ein Tor Hidden Service im Onionland, um Textnachrichten unbeobachtet auszutauschen. Der Dienst kann nur im Webinterface genutzt werden.

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 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.

8.3 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.

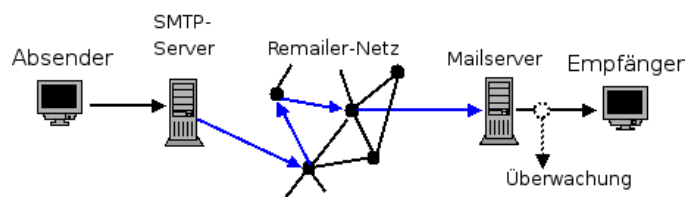


Abbildung 8.1: Konzept einer anonymen E-Mail

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. unbekannten Inhaltes (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: da die E-Mail keine Angaben über den Absender enthält, funktioniert der *Antworten-Button* der Clients auf der Empfängerseite nicht! Der Text der E-Mail sollte einen entsprechenden Hinweis enthalten!

8.3.1 Remailer-Webinterface nutzen

Die einfachste Möglichkeit, eine anonyme E-Mail zu schreiben, besteht darin, ein Webinterface zu nutzen. Es gibt verschiedene Angebote im Internet:

- <https://www.awxcnx.de/anon-email.htm>
- <https://www.cotse.net/cgi-bin/mixmail.cgi>

Verglichen mit der lokalen Installation eines Remailer Clients ist dies die zweitbeste Möglichkeit, eine anonyme E-Mail zu versenden. Den Betreibern der Server liegen alle Daten im Klartext vor und sie könnten beliebig loggen. Die Installation von Quicksilver (für Windows) oder Mixmaster (für Linux) finden sie in der Online-Version des Privacy-Handbuch.

8.4 Fake Mailer

Im Webinterface eines Fake-Mailers können sie eine beliebige Absenderadresse angeben. Um anonym zu bleiben, sollte man Fake Mailer nur mit Anonymisierungsdiensten nutzen. Es besteht kein Schutz gegen Aufdeckung des Absenders durch den Betreiber des Dienstes.

- <https://emkei.cz>

Im Gegensatz zu Remalern dauert es nicht mehrere Stunden, bis die Mail zugestellt wird. Es ist aber möglich, dass diese Mails in Spam-Filtern hängen bleiben, da viele Spam-Filter diese Absenderadresse und die IP-Adresse des sendenden Servers in ihre Bewertung einfließen lassen. Man sollte zusätzliche Spam-Merkmale im Text der Nachricht vermeiden.

8.5 PrivacyBox der GPF

Die PrivacyBox ¹ ermöglicht es, anonyme Nachrichten zu empfangen. Es können nur Nachrichten empfangen werden. Die Nachrichten müssen auf der Kontaktseite des Empfängers geschrieben werden. Die PrivacyBox nimmt keine E-Mails an und bietet auch keine Möglichkeit, E-Mails zu versenden. Es ist so etwas, wie ein Toter Briefkasten. Hinweise zur Nutzung:

- Die PrivacyBox gehört zur Klasse der *host-based crypto systems* (wie Hushmail oder CryptoCat Webinterface). Ich teile die Ansicht von Patrick Ball ² und Bruce Schneier³, dass diese Systeme **für politische Aktivisten ungeeignet** sind. Insbesondere sollte man beachten, dass die PrivacyBox von einem deutschen Verein betrieben wird und bspw. linken Gruppen keinen Schutz gegen Ermittlungen nach §129a durch das BKA bieten kann.
- Als Alternative zur E-Mail kann die PrivacyBox vor dem allgegenwärtigen Tracking kommerzieller Akteure schützen. Sind eure E-Mail Adressen schon bei Facebook, LinkedIn, Twitter, Path, Foursquare, Viper usw. gelandet, obwohl ihr diese Dienste nicht nutzt? Habt ihr schon einmal eine E-Mail an eine GMail Adresse versendet? Die Daten werden mit dem Surfverhalten verknüpft und in die Personalisierung einbezogen, auch wenn man selbst keinen Account bei den Datensammlern hat. Das kann man vermeiden, indem man *harmlose* Dinge via PrivacyBox kommuniziert.

Ich habe die PrivacyBox lange Zeit uneingeschränkt empfohlen. Als Administrator und Hauptentwickler konnte ich sicher sein, dass keine Daten gespeichert wurden und es keine Kooperation mit Geheimdiensten gab. Im Sommer 2011 hat der Vorstand der GPF gegen meinen Wunsch einen zweiten Administrator für die PrivacyBox bestätigt, der meiner Meinung nach im Verdacht steht, als informeller Mitarbeiter unter dem Decknamen *Sysiphos* für die "Dienstesü arbeiten (neusprech: als *Vertrauensperson*).

Die folgenden Vorschläge zur Lösung wurden vom Vorstand der GPF abgelehnt:

- ein unverdächtiges Mitglied der GPF als zweiten Admin einsetzen
- der komplette Vorstand und der neue Admin der PrivacyBox unterzeichnen eine eidesstattliche Erklärung zur Nicht-Kooperation mit Geheimdiensten

Ich habe daraufhin die Administration und Weiterentwicklung der PrivacyBox sowie meine Mitgliedschaft in der GPF niedergelegt. Aus heutiger Sicht ist das Projekt PrivacyBox ähnlich wie VPN-Dienste oder Hushmail einzustufen. Mehr war mit den bescheidenen Mitteln eines Vereins nicht realisierbar.

¹ <https://privacybox.de>

² http://www.wired.com/threatlevel/2012/08/wired_opinion_patrick_ball

³ <https://www.schneier.com/blog/archives/2012/08/cryptocat.html>

Kapitel 9

Im Usenet spurenarm posten

Das Usenet ist noch immer eine umfangreiche Quelle für Informationen zu aktuellen Themen.

Dabei geht es nicht immer um die im Artikel veröffentlichten Informationen. Auch über den Absender läßt sich viel herausfinden. Die folgenden Hinweise sollen eine Recherche zur Erstellung eines Persönlichkeitsprofils erschweren:

- Um eine langfristige Speicherung der Postings zu verhindern sollte ein zusätzlicher Header ins Posting eingefügt werden: *X-No-Archive: yes*
- Es sollte ein News-Server genutzt werden, der SSL-Verschlüsselung bietet und möglichst wenig über den Absender preisgibt.
- Man könnte seine Identität regelmäßig wechseln, sofern keine besondere Reputation mit einer bestimmten Identität verbunden ist.
- Mail2News-Gateways können zum Versenden des Postings genutzt werden. Das Posting wird per E-Mail an das Gateway gesendet, welches es dann an den Newsserver übermittelt. In der Regel übernehmen Mail2News-Gateways die Absender- und IP-Adresse. Eine Liste gut erreichbarer Gateways:
 - mail2news (at) m2n.mixmin.net
 - mail2news (at) dizum.com
 - mail2news (at) bananasplit.info
 - mail2news (at) reece.net.au
- Remailer bieten die Möglichkeit, anonyme Beiträge zu veröffentlichen. Das Posting wird dabei als anonyme E-Mail an ein Mail2News-Gateway gesendet.

Da anonymes Posten insbesondere in deutschen News-Gruppen nicht gern gesehen wird, sollte man gut überlegen, ob es wirklich nötig ist. Ein Pseudonym reicht meistens auch.

Wer die nötige Installation der Software scheut, kann ein Webinterface nutzen unter:

- <https://www.awxcnx.de/anon-news.htm>
- <https://www.cotse.net/cgi-bin/mixnews.cgi>
- <https://www.bananasplit.info/cgi-bin/anon.cgi>

9.1 News-Server

Der Server news.mixmin.net bietet SSL-Verschlüsselung für den lesenden Zugriff und einen ebenfalls TLS-verschlüsselten SMTP-Zugang für das Senden von News-Beiträgen.

Server-Einstellungen:

News-Server: news.mixmin.net
Port: 563 (SSL-verschlüsselt)

SMTP-Server: news.mixmin.net
Port: 25 (TLS-verschlüsselt)

news.mixmin.net verwendet ein SSL-Zertifikat, welches von CAcert.org signiert wurde. Standardmäßig wird diese CA nur von wenigen Newsreadern akzeptiert. Das Root-Zertifikat von CAcert.org ist von <http://www.cacert.org> zu holen und zu importieren.

Die Nutzung von TOR als anonymisierender Proxy ist nach unseren Erfahrungen problemlos möglich.

9.2 Thunderbird konfigurieren

1. Anlegen eines neuen SMTP-Servers. Diese Server findet man im Dialog *Konten...* ganz unten. Der bereits konfigurierte Standard-Server tut es aber auch (und protokolliert jedes Posting).
2. Erstellen und Einrichten eines News-Kontos. Dabei ist auch der SMTP-Server auszuwählen.
3. Hinzufügen des Headers *X-No-Archive: yes* für das News-Konto.

Im Einstellungs-Dialog von Thunderbird findet man in der Sektion *Erweitert* den Reiter *Allgemein*. Ein Klick auf den Button *Konfiguration bearbeiten* öffnet eine Liste aller Optionen.

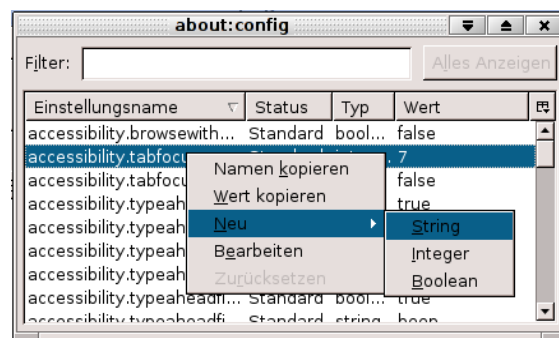


Abbildung 9.1: Neue Config-Variable anlegen

Hier fügt man zwei neue String-Variablen mit folgenden Werten ein (N entspricht dabei der id-Nummer des News-Kontos):

```
mail.identity.idN.headers      archive
mail.identity.idN.header.archive X-No-Archive: yes
```

4. Abonnieren der News-Gruppen.

Kapitel 10

Anonymisierungsdienste

Anonymisierungsdienste verwischen die Spuren der Nutzer im Internet. Die verschlüsselte Kommunikation verhindert auch die Auswertung des Internetverkehrs durch mitlesende Dritte. Diese Dienste sind nicht nur für den anonymen Zugriff auf Websites geeignet. Sie ermöglichen auch eine 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.

10.1 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 spezifische Merkmale modifiziert, die den Nutzer identifizieren könnten (Browser-Typ, Betriebssystem, TCP-Timestamps, Referer....).

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:** Da den Anbietern von Webdiensten keine sinnvolle IP-Adresse zur Verfügung steht, können sie den Standort des Nut-

zers nicht via Geolocation bestimmen. Außerdem 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 Verschlüsselung 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 verbreitete 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 Honeypot genutzt. Ein Beispiel sind die Leimrute des BKA. In mehr als 150 Fällen wurden

die Fahndungseiten von LKAs oder des BKA als Honeygot genutzt und die Besucher der Webseiten in Ermittlungen einbezogen¹. 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.

10.2 Tor, I2P, Freenet und JonDonym

Ein kurzer, oberflächlicher Vergleich soll die technischen Unterschiede zwischen verschiedenen Diensten zeigen und Hilfe bei der Entscheidung bieten.

- **Tor Onion Router** ist ein weltweit verteiltes Anonymisierungsdienst-Netzwerk. Die Projektwebsite bietet umfangreiche Informationen unter der Adresse <https://www.torproject.org>.
- **JonDonym** steht in einer eingeschränkten kostenfreien Variante zur Verfügung sowie in einer kommerziellen Variante. Die kostenfreien Mix-Kaskaden sind in der Geschwindigkeit stark gedrosselt und nur für anonymes Surfen nutzbar. Bezahl-Kaskaden bieten eine höhere Anonymität, hohe Geschwindigkeit und sind für alle Internetprotokolle nutzbar. Weitere Informationen unter <https://www.anonym-surfen.de>.
- Das **Invisible Internet Project** hat das primäre Ziel, Anonymität sowohl für Konsumenten als auch für Anbieter von Angeboten zu bieten. Dieses Ziel lässt sich nur in einem geschlossenen Netz verwirklichen. Es bietet aber auch die Möglichkeit, anonym auf herkömmliche Websites zuzugreifen. Projektwebsite: <http://www.i2p2.de>.

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

¹ <http://heise.de/-1704448>

nicht möglich.

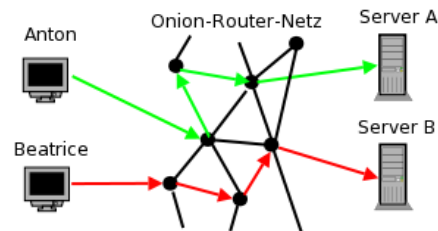


Abbildung 10.1: Prinzip von Tor

Da die Route ständig wechselt, müsste ein großer Teil des Netztes kompromittiert worden sein, um einen Zusammenhang von Surfer und angefragter 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. Mozilla Firefox wird mit TorButton oder JonDoFox optimal eingestellt.

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 einem 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.

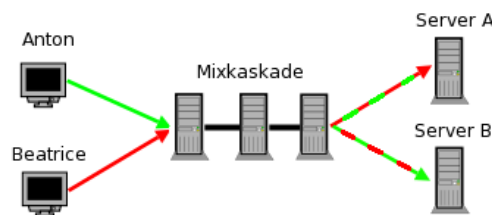


Abbildung 10.2: Prinzip von JonDonym

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, dass 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 von JonDos 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.

Invisible Internet Project

I2P hat das Ziel, Anonymität sowohl für Konsumenten als auch für Anbieter von Diensten zu bieten. Dieses Ziel läßt sich nur in einem geschlossenen Netz verwirklichen.

Es wird die Infrastruktur des WWW genutzt, 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 I2P-Router ist auch ständig an der Weiterleitung von Daten für andere Nutzer beteiligt. Das macht die Beobachtung einzelner Teilnehmer durch Dritte nahezu unmöglich.

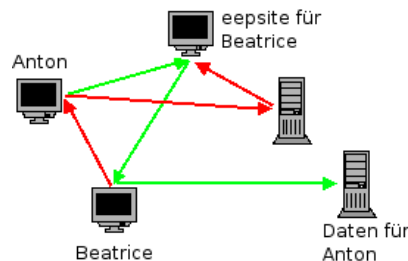


Abbildung 10.3: Prinzip von I2P

Das Projekt bietet einen Java-basierten Client. Dieser Client verschlüsselt den gesamten Datenverkehr. Außerdem stellt er sicher, dass ständig neue Verbindungen zu anderen Rechnern des Netzwerkes aufgebaut werden.

Die im Invisible Internet bereitgestellten Angebote sind nicht lokalisierbar. Neben Websites (sogenannten *eepsites*) gibt es spezielle Möglichkeiten für E-Mails, Foren oder Filesharing. Da die Nutzung der Angebote mit technischen Hürden verbunden ist, sind diese Angebote weit weniger frequentiert, als klassische Webservices.

Einzelne Gateways ins normale Internet oder ins Onionland sind zwar vorhanden, aber nicht das primäre Ziel des Projektes.

Freenet Project

Das 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. Wie beim *Invisible Internet Project* wird ein Java-Client genutzt, der Proxydienste für verschiedene Protokolle bietet (HTTP, SMTP, POP3....).

Im Unterschied zu I2P werden die Inhalte im Freenet redundant über alle Peers verteilt und verschlüsselt abgelegt. Ein Freenet Knoten sollte also möglichst dauerhaft online sein und mehrere GByte Speicherplatz bereitstellen.

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 auch vom Autor nicht mehr modifiziert werden. Es ist jedoch möglich, aktualisierte Versionen zu veröffentlichen und die Freenet Software stellt sicher, dass immer die aktuellste Version angezeigt wird.

Unabhängig vom *Open Freenet* kann man mit vertrauenswürdigen Freunden ein eigenes Netz konfigurieren, welches sich vollständig der Beobachtung durch Dritte entziehen kann.

RetroShare

RetroShare ist ein Friend-2-Friend Netzwerk. Wie bei I2P und Freenet wird die Infrastruktur des Internet als Basis genutzt und ein voll verschlüsselter Layer darüber gelegt. Im Gegensatz zu I2P gibt es kein zentrales Netzwerk, mit dem man sich als Teilnehmer verbindet, sondern viele kleine Netze. Diese Mininetze müssen die Teilnehmer der Gruppe selbst aufbauen, indem sie kryptografische Schlüssel austauschen (z.B. per E-Mail) und diese Schlüssel im RetroShare Client importieren.

RetroShare ermöglicht die unbeobachtete Kommunikation in Gruppen ohne zentrale Server im Internet zu nutzen. Die Kommunikation ist durch Dritte sehr schwer kompromittierbar.

10.2.1 Testergebnisse von Computer-Zeitschriften

Populär unter den Surfern ist vor allem Tor Onion Router. Die Testergebnisse von verschiedenen Zeitschriften empfehlen jedoch meist JonDonym, da die Software JonDo+JonDoFox besser gegen Deanonymisierung durch Browser Spuren schützt. I2P, Freenet und RetroShare werden meist nicht in die Auswahl der getesteten Dienste einbezogen.

- Test der Anonymisierungsdienste in Chip Nov. 2009

Wer so anonym wie möglich surfen möchte, sollte zum Premium-Paket von JonDo greifen und das optionale JonDoFox installieren.

Kein anderer Client bietet dem User einen so transparenten Service und vielfältige Einstellungen.

- Test der Anonymisierungsdienste c't 18/2011

Es gibt mehrere Pakete wie Xerobank oder das TOR Browser Bundle [...] Doch alle uns bekannten setzen auf einen veralteten Browser, kosten viel zu viel oder lassen Lücken. Bei JonDonym bekommt man dagegen zusammen mit dem Firefox-Profil JonDoFox ein besonders einfach einzurichtendes und zu nutzendes System in deutscher Sprache [...] Es ist auch das einzige Paket, das sich wirksam um die Persönlichkeitsspuren im Browser kümmert.

Lediglich die ComputerBild kommt bei ihren jährlichen Tests zu anderen Ergebnissen und setzt regelmäßig den VPN-Anbieter CyberGhost auf den ersten Platz. Möglicherweise ist CyberGhost ein guter Anzeigenkunde?

Die c't schreibt in ihrem Test im Heft 18/2011 über VPNs:

Bei VPNs und Proxies liegt die Information [...] beim Betreiber komplett vor, sodass eine gerichtliche Anfrage oder ein Hacker-Einbruch genügt, um die Anonymität komplett aufzuheben. Dagegen weiß bei einer Proxy-Kaskade kein Beteiligter alles über Herkunft und Ziel der Daten Proxy-Kaskaden verbergen also die IP-Adresse am wirksamsten...

Also lasst die Finger davon.

10.2.2 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 10.4 zeigt die Zusammensetzung der Spender für 2009 (Quelle Tor Financial Report 2009).

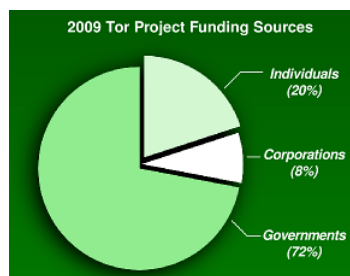


Abbildung 10.4: Anteil der Finanzierung von TorProject.org

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

In den Jahren 2000-2004 erhielt das Projekt AN.ON als Vorläufer von JonDonym ca. 1 Mio. Euro aus dem deutschen Forschungsetat für den Aufbau des Dienstes. Seit dem Ende der Förderung bemüht sich die JonDos GmbH, die Finanzierung durch kostenpflichtige Premium-Angebote zu sichern. Für diese 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.

Invisible Internet Project

Das Invisible Internet und das Freenet Project haben einen anderen Weg ohne externe Finanzierung gewählt. Die Entwicklung der Software erfolgt vollständig auf freiwilliger Basis ohne finanzielle Vergütung. Die 100-Dollar-Kampagne von zzz war ein ironischer Vergleich mit der 1-Mio-Dollar-Kampagne von Tor.

Die Infrastruktur wird durch die beteiligten Nutzer aufgebaut. Jeder Teilnehmer anonymisiert auch Daten für andere Nutzer. Eine ausgeprägte Client-Server-Architektur wie bei JonDonym (und praktisch auch bei Tor) gibt es nicht. Für einzelne Projekte im Invisible Internet gibt es leistungsfähige Knoten, die von einzelnen Anhängern des Dienstes finanziert und betreut werden.

10.2.3 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 meist mit Flash- oder Java-Applets möglich.
- Nahezu alle 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.

10.3 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 implementiert und damit unter verschiedenen Betriebssystemen nutzbar. Es gibt auch eine Version ohne grafisches Interface: JonDo-Console.

1. Für **WINDOWS** bietet die Downloadseite des Projektes ein Setup Programm (34MB), welches nach dem Download als Administrator zu starten ist. Im Verlauf der Installation werden alle benötigten, nicht auf dem Rechner vorhandenen Komponenten installiert (inclusive Java Runtime). <https://www.anonym-surfen.de/jondo.html>

Es besteht die Möglichkeit, JonDo auf dem Rechner als Programm zu installieren, oder als portable Version auf dem USB-Stick. Für die portable Installation brauchen sie keine Administratorrechte und es wird die benötigte Portable Java JRE installiert.

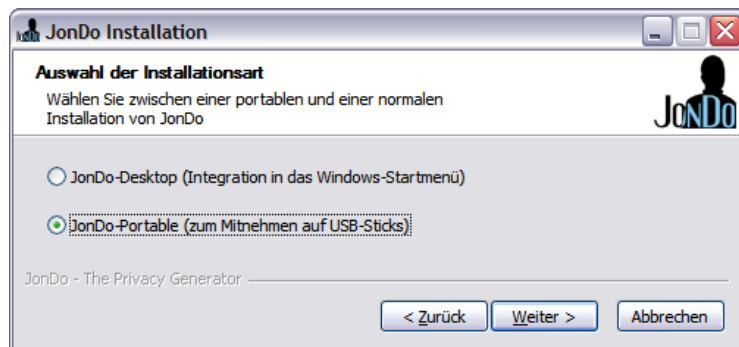


Abbildung 10.5: Installation von JonDo

Im Anschluss an die portable Installation wird angeboten, auch gleich den JonDoFox (portable Version) für anonymes Surfen zu installieren.

2. Für **Ubuntu** sowie **Debian** bietet JonDos fertige Pakete. Um das Software Repository der JonDos GmbH zu nutzen, ist in der Datei `/etc/apt/sources.list` folgende Zeile einzufügen und DISTRI durch die verwendete Distribution zu ersetzen (*squeeze*, *wheezy*, *sid*, *maverick*, *natty*, *oneiric* oder *precise*):

```
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

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/UNIX** Versionen ist als erstes ein Java Runtime Environment zu installieren. Aktuelle Distributionen bieten die Pakete *openjdk6-jre* oder *sun-java6-jre*, die mit dem Paketmanager installiert werden können.

Anschließend startet man den JonDo wie unter 1. beschrieben via **Java Web Start** oder nutzt das Archiv *jondo_linux.tar.bz2* von der JonDo-Website für die Installation. <https://www.anonym-surfen.de/jondo.html>. Nach dem Download ist das Archiv zu entpacken und die Software mit dem Install-Script zu installieren:

```
> 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
```

4. Wenn eine aktuelle Java Version bereits installiert ist, geht es ganz einfach mit dem **Java Web Start**. Man gibt die URL <http://infoservice.inf.tu-dresden.de/japRelease.jnlp> in der Adressleiste des Browsers ein und ruft die Web Start Datei auf. Diese prüft, ob bereits eine aktuelle Version des JonDo Client vorhanden ist, lädt bei Bedarf die aktuelle stabile Version und startet sie. Für zukünftige Starts kann man ein Lesezeichen für diesen Link speichern.

(Sollte der Browser nicht selbst erkennen, mit welcher Anwendung er die JNLP-Datei zu öffnen hat, muss man ihm erklären, dass das Programm *javaws* aus dem Verzeichnis *java/bin* dafür zuständig ist.)



Abbildung 10.6: Hauptfenster von JonDo

Startet man JonDo, öffnet sich das im Bild 10.6 gezeigte Hauptfenster des Programms. Hier kann man eine Kaskade auswählen und mit Klick auf die Option *Anonymität Ein* die Verbindung herstellen.

10.3.1 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 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.
- Zugriff auf den anonymen Dateispeicher von JonDonym unter <https://storage.anonymous-proxy-servers.net>

JonDonym bietet mehrere Volumen-Tarife, die im Voraus zu bezahlen sind. Als Bezahlmethoden stehen Paysafecard, Paypal, Überweisung und Briefsendung zur Auswahl. Im Webshop der JonDos GmbH kann man außerdem mit Bitcoin, Liberty Reserve, Pecunix oder via Western Union bezahlen. Die Einrichtung eines Premium-Account erfolgt im JonDo Client.

Wählen Sie im Hauptfenster von JonDo den Button *Bezahlen*. Es startet ein Assistent, der Sie durch die Einrichtung eines Kontos führt. Als erstes ist ein Tarif auszuwählen. Es stehen Tarife mit einem monatlichen Volumen-Kontingent für die Dauer von 4 Monaten zur Verfügung oder einfache Volumentarife mit einer längeren Laufzeit.

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

Im folgenden Schritt können Sie die Bezahlmethode wählen. Hohe Anonymität und bei der Bezahlung und sofortige Verfügbarkeit des Kontos bietet die Methode **Paysafecard**. Eine Paysafecard für einen Betrag von 10 Euro kann man an verschiedenen Tankstellen oder Zeitungsgeschäften kaufen. Der Code wird beim Bezahlvorgang auf der Paysafecard Webseite eingegeben - fertig.

The screenshot shows a window titled 'Konto erstellen' with a close button in the top right corner. The main content area is titled 'Bezahlungen' and contains four radio button options: 'PayPal', 'paysafecard' (which is selected), 'Ueberweisung', and 'Bargeld per Briefpost'. Below these options, it states 'Bezahlt wird für folgenden Tarif: M-Volume (10,00 Euro)'. At the bottom of the window are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'.

Bei der **Briefzahlung** ist es wichtig, dass Sie die Transaktionsnummer der Geldsendung beilegen, damit die Zahlung auch Ihrem Account zugeordnet werden kann. Sie können den vorbereiteten Text über die Zwischenablage in eine Textverarbeitung übernehmen, ausdrucken und mit dem Betrag verschicken.

The screenshot shows the same 'Konto erstellen' window, but with the 'Informationen zur Bezahlung' tab selected. It contains the following text: 'Bitte schicken Sie den Betrag in bar an folgende Adresse. **Wichtig:** Legen Sie unbedingt eine Notiz mit der unten angezeigten Transaktionsnummer bei.' followed by the address 'JonDos GmbH, Bruderwöhrdstrasse 15b, 93055 Regensburg, Deutschland' and the payment details 'Betrag: 10,00 Euro' and 'Transaktionsnummer: 783035982550'. Below this is a button 'Kopieren in Zwischenablage'. At the bottom, there is a checkbox labeled 'Ich werde die Zahlung wie beschrieben durchführen.' which is currently unchecked. The same three navigation buttons ('< Zurück', 'Weiter >', 'Abbrechen') are at the bottom.

Aktivieren Sie die Option *Ich werde die Zahlung durchführen* und Sie können bei Briefzahlung die Freischaltung Ihres Accounts in 2-3 Tagen erwarten.

10.3.2 Anonym Surfen mit dem JonDoFox

Um mit Firefox und JonDonym anonym zu surfen, reicht es nicht, einfach nur den Proxy umzuschalten. Weitere Daten sollten blockiert oder modifiziert

werden, um in einer möglichst großen Anonymitätsgruppe abzutauchen.

Die JonDos GmbH bietet einfertiges Profil für Firefox zum Download an. Neben der Anpassung der Proxy-Einstellungen bietet es weitere Features für spurenarmes, sicheres und anonymes Surfen. JonDoFox ist 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 besser überprüft und Werbung wird blockiert.

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

- Für WINDOWS startet man das Install-Script *JonDoFox.paf.exe* nach dem Download und folgt den Anweisungen. Man kann zwischen der Installation auf dem eigenen Rechner oder als portable Version auf dem USB-Stick wählen. Die Installation auf dem Rechner setzt voraus, dass Firefox bereits vorhanden ist. Bei der USB-Version wird ein portabler Firefox mit installiert.
- Für Debian und Ubuntu steht das Paket *jondofox-de* im Software-Repository der JonDos GmbH bereit. Nach der Installation des Paketes findet man in der Programmgruppe *Internet* den Menüpunkt *JonDoFox*.
<https://www.anonym-surfen.de/help/firststeps2.html>

Der JonDoFox ist nicht mehr mit dem in Debian *squeeze* enthaltenen *Iceweasel* kompatibel. Es ist nötig, eine aktuellere Version des Browsers zu installieren, die vom Mozilla Debian Team bereitgestellt wird. Eine Anleitung zur Nutzung des Repositories findet man unter <http://mozilla.debian.net>.

- Für andere Linux Distributionen lädt man das Archiv *jondofox_linux_de.tar.bz2* herunter, entpackt es und startet das Install-Script. Das Script legt einen Menüpunkt in der Programmgruppe *Internet* an und integriert das JonDoFox-Profil in eine bestehende Firefox Konfiguration. Firefox oder Iceweasel sind zuvor zu installieren.

```
> tar -xjf jondofox_linux.tar.bz2
> cd jondofox_linux_de
> ./install_linux.sh
```

Nach der Installation fragt Firefox bei jedem Start, welche Konfiguration genutzt werden soll (Bild 10.7). Damit wird der Nutzer auch gezwungen, den Browser zu schließen, bevor er zum anonymen Surfen wechselt.

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.

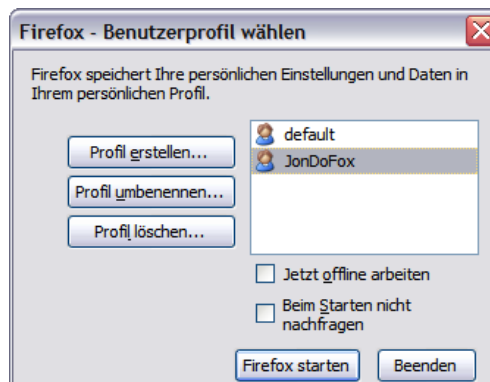


Abbildung 10.7: Profil beim Start von Firefox wählen

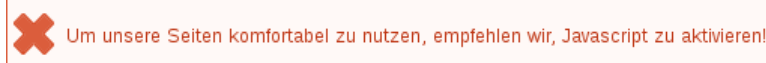
<http://ip-check.info>

Die Lesezeichen kann man vom Profil *default* übernehmen (exportieren und importieren) oder via Firefox Sync holen.

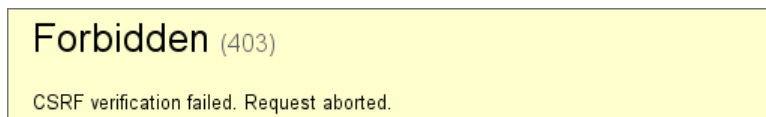
Cookies und Javascript

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.

Die Add-ons CookieMonster und NoScript ermöglichen es, diese Techniken für einzelne, vertrauenswürdige Webseiten gezielt freizugeben. Als erstes sollte man versuchen, Cookies temporär freizugeben. Diese Kekse wird man einfach wieder los. CookieMonster ermöglicht es, die Restriktion für einzelne,

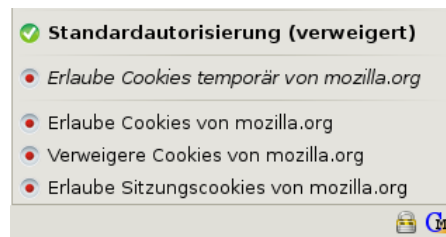


Abbildung 10.8: Cookies für eine Websites freigeben

vertrauenswürdige Webseiten temporär oder dauerhaft aufzuheben.

Erlaube Cookies temporär erlaubt es dem aktuellen Server, nur für diese Sitzung Cookies zu setzen. Mit dem Schließen des Browsers werden die Cookies und die Ausnahmeregelung gelöscht.

Erlaube Cookies erlaubt es dem aktuellen Server, unbegrenzt gültige Cookies zu setzen. Diese Variante wird nur benötigt, wenn man bei einem späteren Besuch der Website automatisch wieder angemeldet werden möchte.

Verweigere Cookies erlaubt es dem aktuellen Server nicht, Cookies zu setzen.

Erlaube Sessioncookies erlaubt es dem aktuellen Server, Cookies zu setzen. Mit dem Schließen des Browsers werden diese Cookies wieder gelöscht. Bei folgenden Besuchen dürfen wieder neue Cookies gesetzt werden.

Wenn die Freigabe von Cookies das Problem nicht löst, kann man **JavaScript** für einzelne Domains mit einem Klick auf das NoScript-Symbol in der Toolbar temporär freigeben. 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.

Flash Videos (Youtube o.ä.)

Aus Sicherheitsgründen ist Flash im JonDoFox deaktiviert. Es ist möglich, mit Flash-Applets die Proxy-Einstellungen zu umgehen und die reale IP-Adresse des Surfers zu ermitteln.

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 Unplug. Sie können die Videos in verschiedenen Formaten und Qualitätsstufen speichern. Das Format MP4 kann von allen Mediaplayern abgespielt werden.

10.4 Tor Onion Router nutzen

Das Onion Routing wurde von der US-Navy entwickelt. Die Weiterentwicklung liegt beim TorProject.org, wird durch Forschungsprojekte u.a. von deutschen Universitäten oder im Rahmen des *Google Summer of Code* unterstützt.

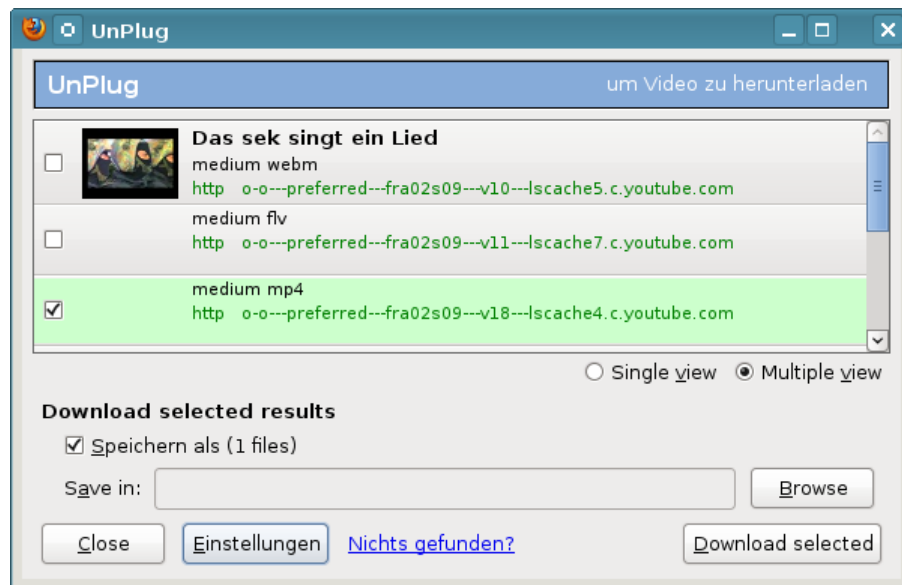


Abbildung 10.9: Video-Download mit Unplug

Das Tor Onion Router Netzwerk besteht gegenwärtig aus ca. 2500 Servern (Nodes), die weltweit verteilt sind.

10.4.1 TorBrowserBundle

Das **TorBrowserBundle** enthält eine portable Firefox-Version, Tor und das Control Panel Vidalia. Eine Installation ist nicht nötig. Das Archiv ist nach dem Download von <https://www.torproject.org> zu entpacken - fertig.

- Unter Windows öffnet man nach dem Download das selbstentpackende Archiv mit einem Doppelklick im Dateimanager, wählt ein Zielverzeichnis und klickt auf den Button *Extract*. Nach dem Entpacken des Archives wechselt man in das neu erstellte Verzeichnis und startet Tor, Vidalia und den fertig konfigurierten Firefox mit der Applikation **Start Tor Browser**.

Man kann eine Verknüpfung zu dem Startprogramm Start Tor Browser erstellen und diese Verknüpfung auf den Desktop ziehen. Das vereinfacht später den Start der Programme.

- Unter Linux nutzt man den bevorzugten Archiv-Manager oder erledigt es auf der Kommandozeile mit:

```
> tar -xaf tor-browser-gnu-linux-*
```

Das TorBrowserBundle kann auch auf dem USB-Stick mitgenommen werden. Wird der TorBrowser vom USB-Stick gestartet hinterläßt er keine Spuren auf dem Rechner.

10.4.2 Anonym Surfen mit Tor

Das TorBrowserBundle ist für anonymes Surfen vorbereitet. Man startet alle nötigen Komponenten (Tor, Vidalia, Browser) mit dem Tool **Start Tor Browser.exe** (Windows) oder **start-tor-browser** (Linux) (Bild 10.10). Mit dem Schließen des Browsers werden auch Tor und Vidalia beendet.

Der TorBrowser ist für anonymes Surfen konfiguriert. Tracking-Spuren und Werbung sehen die Entwickler nicht als Problem, da der Datenverkehr anonymisiert ist. Es ist empfehlenswert, zusätzlich einige Anpassungen vorzunehmen, um überflüssige Spuren im Netz zu minimieren.

Javascript deaktivieren

TorProject.org empfiehlt in den offiziellen FAQ Javascript nicht zu deaktivieren.

However, we recommend that even users who know how to use NoScript leave JavaScript enabled if possible, because a website or exit node can easily distinguish users who disable JavaScript from users who use Tor Browser bundle with its default settings (thus users who disable JavaScript are less anonymous).

Ein Test mit Panoptlick lässt aber das Gegenteil als sinnvoll vermuten.

- **Mit aktiviertem Javascript:**

Within our dataset of several million visitors, only one in 33,726 browsers have the same fingerprint as yours.

Die Tabelle der ausgewerteten Features zeigt, dass (bei mir) die per Javascript ausgelesene Bildschirmgröße den höchsten Informationswert hat. Genau dieses Merkmal wird von Googles Suche seit einiger Zeit ausgewertet oder von Trackingdiensten wie Multicounter ² als individuelles Merkmal registriert.

Browser Characteristic	bits of identifying information	one in x browsers have this value
User Agent	6.39	84.13
HTTP_ACCEPT Headers	6.94	123.1
Browser Plugin Details	5.12	34.73
Time Zone	4.54	23.24
Screen Size and Color Depth	12.28	4978.58
System Fonts	3.34	10.1
Are Cookies Enabled?	0.39	1.31
Limited supercookie test	3.1	8.6

- **Javascript deaktiviert**

Within our dataset of several million visitors, only one in 2,448 browsers have the same fingerprint as yours.

² <http://www.multicounter.de/features.html>

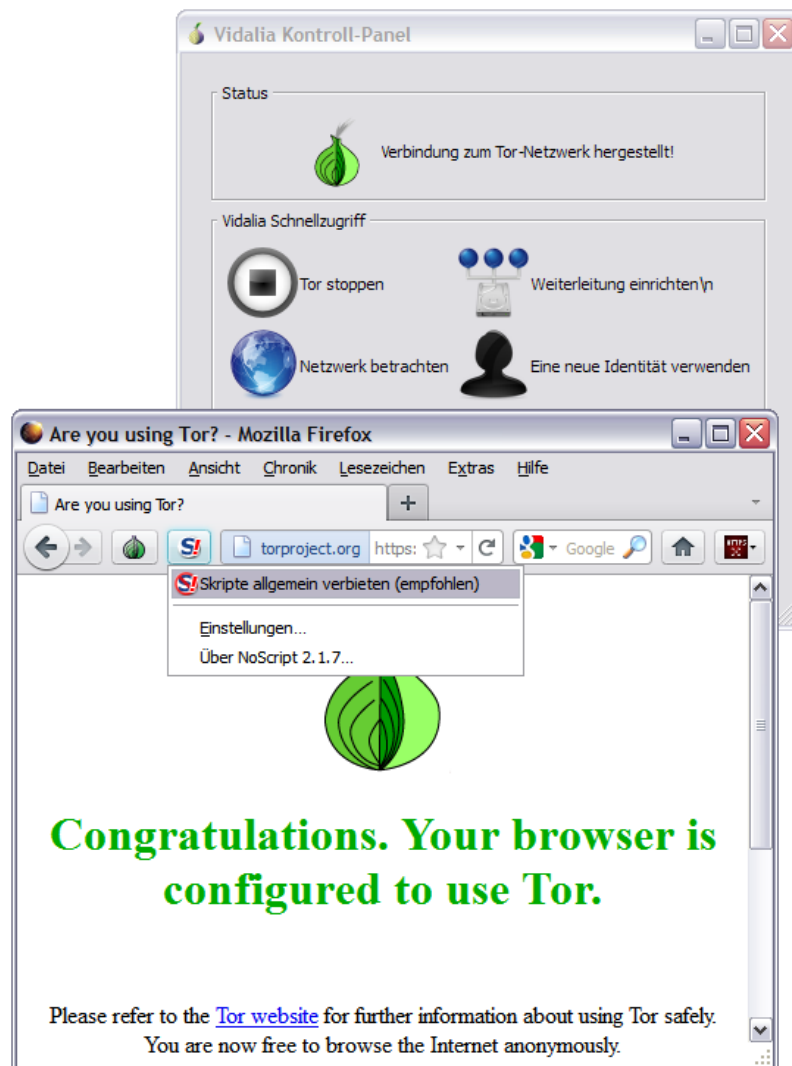


Abbildung 10.10: Start des TorBrowser

Browser Characteristic	bits of identifying information	one in x browsers have this value
User Agent	6.39	84.13
HTTP_ACCEPT Headers	7	127.63
Browser Plugin Details	1.89	3.71
Time Zone	1.88	3.69
Screen Size and Color Depth	1.88	3.69
System Fonts	1.89	3.7
Are Cookies Enabled?	0.39	1.31
Limited supercookie test	1.88	3.69

Auch wenn Panoptlick einer wissenschaftlichen Untersuchung nicht standhält und auch manipulierbar ist, sind die Ergebnisse mit Unterschieden von mehr als einer Zehnerpotenz ein deutlicher Hinweis.

Javascript ermöglicht das Auslesen vieler Informationen, die zu einem individuellen Fingerprint verrechnet werden können. Auch ein böartiger Exit-Node könnte diese Informationen erlangen, wie TorProject.org in den FAQ erwähnt. Javascript sollte allgemein verboten werden und nur für vertrauenswürdige Webseiten freigegeben werden (siehe Screenshot oben). Das verbessert auch die Geschwindigkeit beim Laden von Webseiten.

Werbung und Trackingscripte blockieren

Das TorBrowserBundle enthält keinen Werbeblocker. TorProject.org argumentiert, dass mit einem Werbeblocker das Internet gefiltert wird und jede Filterung lehnen die Entwickler grundsätzlich ab. Außerdem möchte TorProject.org nicht in den Ruf kommen, Geschäftsmodelle im Internet zu stören. Als drittes könnten möglicherweise unterschiedliche Filterlisten als Merkmal für den Browserfingerprint genutzt werden. Es gibt allerdings bisher keine wiss. Untersuchungen, die diese Vermutung belegen oder entkräften.

Das Blockieren von Werbung reduziert nicht nur die Belästigung. Da das Tor-Netz langsam ist, wird auch der Seitenaufbau beschleunigt, wenn überflüssige Daten nicht geladen werden.

Empfehlenswert ist die Installation von Adblock Plus. Nach der Installation kann man die Sperrliste *EasyList Germany* + *EasyList* abonnieren sowie die *EasyPrivacy* und *SocialMediaBlock* hinzufügen, wie es im Kapitel *Spurenarm Surfen* beschrieben wurde.

Cookies und EverCookies

Im Gegensatz zum JonDoFox akzeptiert der TorBrowser standardmäßig Cookies von der aufgerufenen Webseite und lässt EverCookie Markierungen zu. Ein Ändern der Einstellungen zur Annahme von Cookies empfehle ich nicht. Viele Webdienste nutzen EverCookie Techniken zum Tracking, wenn Cookies gesperrt wurden.



Abbildung 10.11: Neue Identität im TorBrowser wählen

Man sollte dem Anonymitätskonzept des TorBrowser folgen und bei Bedarf gelegentlich alle Identifikationsmerkmale löschen. Alle Cookies und alle bekannten EverCookie Markierungen werden beim Beenden des Browsers gelöscht oder wenn man den Menüpunkt *Neue Identität* der Zwiebel in der Toolbar wählt (Bild 10.11). Insbesondere vor und nach dem Login bei einem Webdienst sollte man alle Markierungen entfernen, um eine Verknüpfung des Surfverhaltens mit Accountdaten zu verhindern.

Weitere Maßnahmen

- Da sich im Tornetzwerk nicht nur die *good guys* tummeln, sollte man den Abschnitt HTTPS-Security beachten. Das Add-on *HTTPSEverywhere* ist bereits vorhanden, zusätzlich kann man *Certificates Patrol* installieren.
- Je nach Nutzung können einige weitere Add-ons sinnvoll sein: PwdHash für starke Login-Passwörter oder für Videos Downloads den Download-Helper bzw. UnPlug.

Tor mit weiteren Anwendungen nutzen

Wenn man Tor nicht nur mit dem TorBrowser sondern auch mit einem E-Mail Client oder Instant Messaging Client nutzen möchte, muss man den Listen Port von Tor von *Auto* auf einen festen Wert setzen, damit die anderen Programme konfiguriert werden können.

Es ist die Konfigurationsdatei *torrc* mit einem Texteditor zu öffnen. In der Regel findet man diese Datei in Unterverzeichnis *Data/Tor* des entpackten Tor-BrowserBundles. Dort ändert man den Parameter für den SocksPort von *auto* auf einen festen Wert (üblicherweise Port 9050).

SocksPort 9050

10.4.3 Tor Bad Exit Nodes

Ein sogenannter *Bad-Exit-Node* im Tor-Netz versucht den Traffic zu beschneffeln 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.

Cookies, Javascript und Java sind für anonymes Surfen zu deaktivieren. Dann kann der Nutzer nicht durch eingeschmuggelte Cookies oder Scripte deanonymisiert werden.

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	\$3163a22dc3849042f2416a785eaeebf00a10cc48
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

Die genannten 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) *ling* war ein chinesischer Tor Node, der im Frühjahr 2008 versuchte, mit gefälschten SSL-Zertifikaten die Daten von Nutzern zu ermitteln³. Die zeitliche Korrelation mit den Unruhen in Tibet ist sicher kein Zufall.
- (b) *LateNightZ* war ein deutscher Tor Node, der ebenfalls dabei erwischt wurde, SSL-Verbindungen zu modifizieren⁴.

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 russische Exit-Nodes die HTTPS-Links in Webseiten durch HTTP-Links ersetzt. Wie erfolgreich damit die SSL-Verschlüsselung ausgehebelt werden kann, wurde auf der Black Hack 2009 beschrieben.

Bradiex	bcc93397b50c1ac75c94452954a5bcda01f47215 IP: 89.208.192.83
TorRelay3A2FL	ee25656d71db9a82c8efd8c4a99ddbec89f24a67 IP: 92.48.93.237
lolling	1f9803d6ade967718912622ac876feef1088cfaa IP: 178.76.250.194

- 4. Da die NSA die gesamte elektronische Kommunikation aller US-Bürger abhört, ist es nicht unwahrscheinlich, dass sie sich auch um Daten aus dem Tor-Netz bemühen.

Ein passiv schnüffelnder Node ist nicht erkennbar. Es wäre eine mühselige Sisyphus Arbeit für einzelne Nutzer, jedem Verdacht und jeder Verschwörungstheorie nachzugehen und einzelne Nodes zu sperren. Effektiver ist es, nur vertrauenswürdige Exits zu nutzen.

10.4.4 Tor Good Exit Nodes

Im Abschnitt *Tor Bad Exits* sind einige Nodes genannt, denen man nicht trauen sollte. Diese Aufzählung kann nicht vollständig sein. Es ist so gut wie unmöglich, einen passiv schnüffelnden Tor Node zu erkennen.

Verschiedene Sicherheitsforscher haben nachgewiesen, dass es recht einfach möglich ist, mit schnüffelnden Exits Informationen über die Nutzer zu sammeln (D. Egerstad 2007, C. Castelluccia 2010...). Man kann davon ausgehen, dass es verschiedene Organisationen gibt, die mit unterschiedlichen Interessen im Tor Netz nach Informationen phishen. Auch SSL-verschlüsselte Verbindungen sind nicht 100% geschützt. C. Soghoian und S. Stamm haben in einer wiss. Arbeit gezeigt, dass Geheimdienste wahrscheinlich in der Lage sind, gültige SSL-Zertifikate zu faken.

³ <http://archives.seul.org/or/talk/Mar-2008/msg00213.html>

⁴ <http://www.teamfurry.com/wordpress/2007/11/20/tor-exit-node-doing-mitm-attacks/>

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. Eine Liste der Server findet man unter:
<https://www.torservers.net/services.html>.
- Die von der GPF/SPF betriebenen Server sammeln keine Informationen. Eine Liste der Server findet man unter:
<https://www.privacyfoundation.de/service/serveruebersicht>.
- Der CCC betreibt nach eigenen Aussagen die Tor Nodes: *chaoscomputerclub42*, *chaoscomputerclub23* ... (wird ergänzt, sobald verifiziert)
- Der Tor Node *FoeBud3* wird wirklich vom FoeBud betrieben.

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 *torrc* 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.

Konfiguration in Vidalia

Das GUI Vidalia bietet viele Möglichkeiten für die Konfiguration von Tor, aber nicht alle. Um Optionen zu konfigurieren, die nicht in Vidalia zugänglich sind, kann eine Konfigurationsdatei angegeben werden, die zusätzliche Optionen enthält, die beim Start von Tor zu berücksichtigen sind. Unter Linux findet man diese Datei standardmäßig unter *\$HOME/.vidalia/torrc*. Es kann jedoch eine beliebige andere Datei verwendet werden. In die Tor-Konfigurationsdatei trägt man die oben genannten Optionen ein.

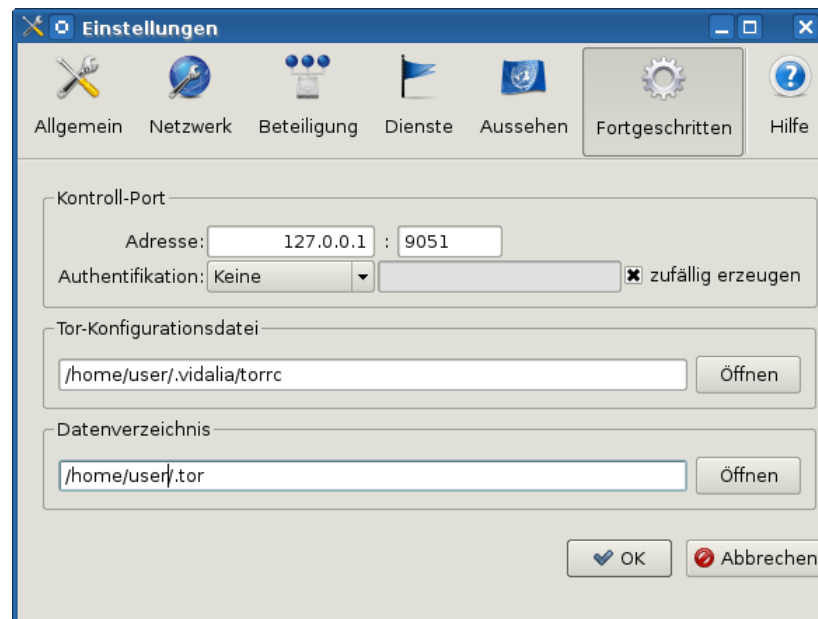


Abbildung 10.12: torrc in Vidalia auswählen

10.4.5 Tor Hidden Services

Das Tor Netzwerk ermöglicht nicht nur den anonymen Zugriff auf herkömmliche Angebote im Web sondern auch die Bereitstellung anonymer, zensurresistenter und schwer lokalisierbarer Angebote auf den Tor-Nodes. Der Zugriff auf die Tor Hidden Services 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.

Es gibt mehrere Angebote im normalen Web, die zusätzlich als Tor Hidden Service anonym und unbeobachtet erreichbar sind. Die Suchmaschine DuckDuckGo ist unter der Adresse <http://3g2upl4pq6kufc4m.onion> zu finden, awxcnx.de unter <http://a5ec6f6zcxtudtch.onion> u.a.m.

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).
- 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.

Es gibt also kaum etwas, dass ich weiterempfehlen möchte.

Vielleicht kann man für unbeobachtete und vorratsdatenfreie Kommunikation die folgenden Dienste nennen:

- **TorMail** unter der Adresse <http://jhiwjllqpyawmpjx.onion> bietet SMTP und POP3. Es können auch E-Mails aus dem normalen Web unter *xxx@tormail.net* empfangen werden.
- **TorPM** unter <http://4eiruntyxxbgfv7o.onion/pm/> bietet die Möglichkeit, Textnachrichten ohne Attachments unbeobachtet auszutauschen. Der Dienst erfordert das Anlegen eines Accounts. Das Schreiben und Lesen der Nachrichten erfolgt im Webinterface.
- **SimplePM:** <http://v6veu7nsxklglu.onion/SimplePM.php> arbeitet komplett ohne Anmeldung. Beim Aufruf erhält man zwei Links: einen Link kann man als Kontakt-Adresse versenden, den zweiten Link für die Inbox sollte man als Lesezeichen speichern. Es können einfache Textnachrichten via Webinterface geschrieben und gelesen werden.
- **OpenPGP Keyserver:** <http://qtt2yl5jocgrk7nu.onion> ist ein Webinterface für die Suche nach OpenPGP-Schlüsseln. Es ist ein Hidden Service für <https://keys.indymedia.org>.
- **Jabber-Server** für Instant-Messaging via XMPP:
 - *ch4an3siqc436soc.onion:5222*
 - *ww7pd547vjnlhdmg.onion:5222*
 - *3khgsei3bkgqvmqw.onion:5222*
- **Jabber-Server**
 - *p4fsi4ockecnea7l.onion:6667* (Tor Hidden Service des Freenode Netzwerk, kann nur mit registrierten Nicks genutzt werden.)

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.

10.5 Anonymous Live-CDs für JonDo und Tor

Es gibt einige Projekte, die eine Live-CD bereitstellen. Bei der Nutzung einer Live-CD 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-CD ist eine auf Debian GNU/Linux basierende Live-CD von JonDonym. Neben JonDo, Tor, I2P und Mixmaster als Anonymisierungsdienste bietet sie eine sichere Browser Konfiguration mit dem JonDoFox. Der E-Mail Client Thunderbird ist für anonyme Nutzung vorbereitet, man muss nur seine E-Mail Adresse und das Passwort für den Zugang eingeben, den Rest erledigt in der Regel der Wizard. Außerdem ist Pidgin für Instant Messaging und der VLC-Player für Video-Streams enthalten und vorkonfiguriert. Beim Booten der Live-CD werden die MAC-Adressen der Netzwerkschnittstellen gefaket und der Rechnername zufällig gesetzt, um Anonymität in Internetcafes zu ermöglichen.

Download: <https://www.anonym-surfen.de/help/jondo-live-cd.html>

TAILS *The Amnesic Incognito Live System* ist die offizielle Live-CD von Torproject.org. Der gesamte Datenverkehr ins Internet wird in der Standardkonfiguration durch Tor geschickt. Die Live-CD wird aktiv weiterentwickelt und bietet eine sehr hohe Qualität hinsichtlich Sicherheit.

TAILS bietet die Anonymisierungsdienste Tor und I2P.

Download: <https://tails.boum.org/>

Polippix ist eine Tor-Live-CD von der IT-Political Association of Denmark basierend auf Linux. Die letzte Version ist vom Juli 2010, also etwas veraltet. Es gibt eine deutsche Anleitung vom AK Vorrat.

Download: <http://polippix.org>

Privatix von Markus Mandalka bietet ebenfalls Tor als Anonymisierungsdienst. Als Internet Anwendung ist lediglich Icewaesel (die Debian-Version von Firefox) mit TorButton + Polipo vorkonfiguriert. Im Gegensatz zu TAILS und Polippix wird nicht der gesamte Datenverkehr durch Tor gejagt.

Ein besonderes Feature von Privatix ist der Installations-Wizard für USB-Sticks. Der Wizard verschlüsselt das System bei der Installation vollständig und erstellt ein schreibbares System (im Gegensatz zu UNetbootin). Privatix wird relativ selten aktualisiert, in der Regel nur mit einem neuen Debian Release. Deshalb empfehlen wir die Installation auf einem USB-Stick und regelmäßiges Einspielen der Security-Updates.

Download: <http://www.mandalka.name/privatix/>

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.

Alle Live-CDs können als ISO-Image auf einen CD-Rohling gebrannt oder auch mit einem USB-Stick genutzt werden. Die Nutzung des USB-Sticks als Boot-Medium bringt einen deutlichen Geschwindigkeitsvorteil. Mit dem Tool **UNetbootin** kann man ein ISO-Image problemlos auf einen USB-Stick "brennen". Für Windows und MacOS ist die Software von der Projektseite <http://unetbootin.sourceforge.net> herunter zu laden und zu installieren, Linuxer finden ein passendes Paket in den Repositories der Distribution und können es mit dem Paketmanager installieren.

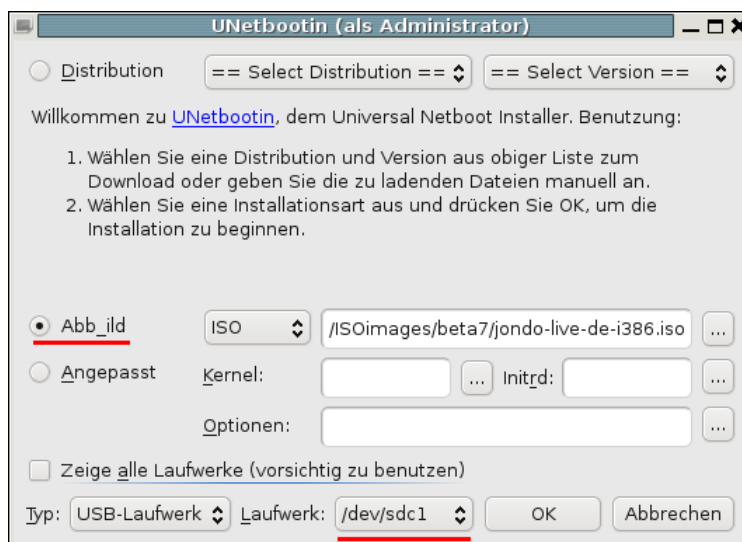


Abbildung 10.13: UNetbootin GUI

Nach dem Start von UNetbootin als Administrator oder root wählt man das ISO-Image und den USB-Stick als Ziel. Nach einem Klick auf Ok wird ein bootfähiger USB-Stick erstellt - fertig.

Mit UNetbootin "gebrannte" USB-Sticks werden beim Booten als read-only eingebunden! Wie bei einer Live-CD gehen alle Änderungen bei einem Reboot verloren. Der Vorteil liegt vor allem in einer höheren Geschwindigkeit.

Außerdem können zusätzliche Daten auf dem Stick gespeichert werden (Lesezeichen, OpenPGP-Schlüssel, JonDonym Premium Accounts...). Diese zusätzlichen Daten findet man nach dem Booten des Live-Systems im Verzeichnis `/live/image`.

10.6 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 bei einem Provider im Ausland sein. In der Regel erfolgt die Anmeldung im Webinterface des Providers. Für die Anmeldung ist ein Anonymisierungsdienst (JonDonym, Tor) zu nutzen. Einige Vorschläge für E-Mail Provider:

-
- **SecureNym** ⁵ und **CryptoHeaven** ⁶ (kostenpflichtige, anonyme Mailprovider ab \$60 pro Jahr, bieten anonyme Accounts, einfache Verschlüsselung der Kommunikation mit Accounts beim gleichen Provider, Offshore registrierte Firmen)
- **VFEmail** ⁷ (anonymer Mailprovider, benötigt eine Wegwerf-Adresse für Registrierung, kostenfreie Accounts mit POP3/SMTP und beliebig vielen temporären E-Mail Adressen)
- **TechEmail** ⁸ und **Hushmail** ⁹ (kanadische Mailprovider, kostenfreie Accounts nur via Webinterface nutzbar)
- **Posteo.de** ¹⁰ und **aikQ.de** ¹¹ (deutsche Mailprovider, Accounts ab 1,- Euro pro Monat, anonyme Accounts möglich)
- **Lavabit** ¹² und **Cotse** ¹³ (US-amerikanische Mailprovider, anonyme Accounts möglich)
 - Lavabit sperrt Tor Nodes wegen häufigem Missbrauch, kostenfreie Accounts nur via Webinterface nutzbar
 - Cotse bietet keine kostenfreien Accounts, Preise ab \$50 pro Jahr

⁵ <https://secrenym.net>

⁶ <https://www.cryptoheaven.com/>

⁷ <https://www.vfemail.net>

⁸ <http://techemail.com>

⁹ <https://www.hushmail.com/>

¹⁰ <https://posteo.de>

¹¹ <https://www.aikq.de>

¹² <https://lavabit.com>

¹³ <https://www.cotse.net>

- **Secure-Mail.biz**¹⁴ (deutsche Betreiber, Firma ist in Rumänien registriert, kostenfreie Accounts nur via Webinterface nutzbar oder HTTPMail, wird vom AK Vorrat unterstützt, unklar ist die weitere Entwicklung und Finanzierung, Einblendung von Werbung im Webinterface ist geplant)

Für politische Aktivisten gibt es die Provider nadir.org, aktivix.org und riseup.net, die sich bemühen, die damit verbundenen Anforderungen zu erfüllen. Sie werden durch Spenden finanziert. Für einen Account muss man seine politischen Aktivitäten nachweisen, aber nicht unbedingt seine Identität offen legen.

Man kann den E-Mail Account in der Regel komplett im Webinterface des Providers nutzen. Dafür brauchen Sie nur einen anonymisierten Browser wie den JonDoFox oder den TorBrowser. Besser ist jedoch die Nutzung eines E-Mail Clients. Man muss sich nicht durch ein überladenes Webinterface kämpfen, es gibt keine Probleme mit Cookies und Javascript und die OpenPGP Verschlüsselung ist wesentlich einfacher möglich.

Thunderbird-Profil erstellen

Ich empfehle, für anonyme E-Mails Thunderbird mit einem anonymen Profil zu nutzen. Damit vermeidet man den Cookie- und Javascript Trouble der verschiedenen Webseiten und reduziert das Traffic Volumen. Außerdem ist Verschlüsselung mit OpenPGP oder S/MIME möglich.

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 10.14 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. Auf meiner Webseite¹⁵ stelle ich ein TorBirdy-XPI zum Download bereits, das ein paar kleine Verbesserungen enthält, die noch nicht in den Upstream eingeflossen sind.

¹⁴ <https://www.secure-mail.biz/>

¹⁵ https://www.awxcnx.de/handbuch_24e.htm

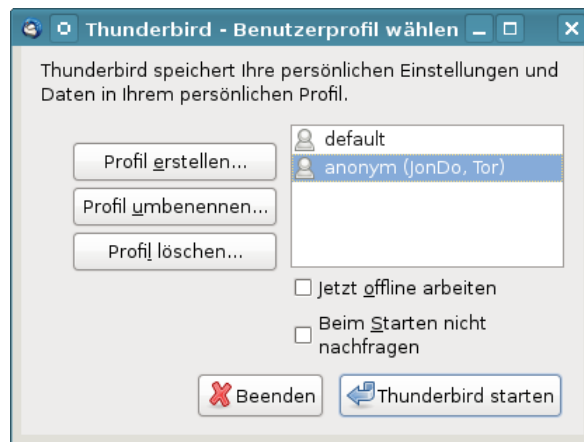


Abbildung 10.14: Profilmanager für Thunderbird

Nach dem Download öffnet man in Thunderbird die Add-on Verwaltung (Extras -> Add-ons) und installiert *TorBirdy* über den Menüpunkt *Add-on aus Datei installieren...*

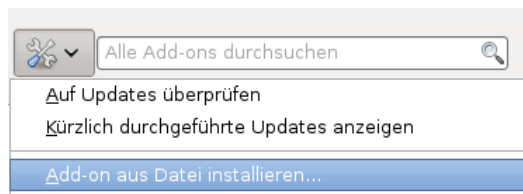


Abbildung 10.15: Add-on aus Datei installieren

Das Add-on *TorBirdy* erledigt folgende Aufgaben:

- Es werden die Einstellungen von Thunderbird (und Enigmail) angepasst, so dass eine sichere und anonyme Nutzung gewährleistet wird.
- 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.
- Die Proxy-Einstellung werden angepasst. Dabei kann man in der Statusleiste unten rechts wählen, ob man Tor oder JonDonym (Premium) nutzen möchte.



Hinweis: Tor muss am Port 9050 lauschen. Dafür ist eine Anpassung der Konfiguration nötig, siehe: *Tor mit weiteren Anwendungen nutzen*.

Danach kann man das Add-on Enigmail für die OpenPGP-Verschlüsselung installieren und die Wörterbücher der bevorzugten Sprachen hinzufügen.

Da das TorBrowserBundle keinen HTTP-Proxy mehr enthält, sollte man mit Tor keine Keyserver in der Schlüsselverwaltung von Thunderbird 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.

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.

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.

Möchte man die E-Mails von einem Tor Hidden Service abrufen, erhält man meist zuerst einen Timeout-Fehler. Es hilft, die Website des Hidden Service im Browser via Tor aufzurufen und erst, wenn diese Website geladen ist, die Mails abzurufen. Mit dem Aufruf im Browser wird ein Circuit zum Hidden Service aufgebaut. Browser sind hinsichtlich der Timeouts etwas robuster.

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 ¹⁶ zukünftig alle E-Mails der GMail Accounts in das NSA-Datcenter in Bluffdale kopiert.

10.7 Anonym Bloggen

Es gibt viele Gründe, um anonym zu Bloggen. Auf die möglichen Gründe möchte ich nicht weiter eingehen und mich auf einige technische Hinweise für die Umsetzung beschränken.

Die einfachste Variante:

- Man braucht einen anonymen Browser (TorBrowserBundle oder Jon-do+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, als Kontaktadresse...). Dabei ist es nicht unbedingt nötig, Thunderbird als E-Mail Client zu konfigurieren. Man kann die wenigen Mails auch im Webinterface des Providers im Browser lesen bzw schreiben. Dabei ist stets 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. Ich kann Wordpress.com oder Twoday.net empfehlen.

¹⁶ http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

- 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.

10.8 Anonymes Instant-Messaging mit Pidgin

Der Instant-Messenger *Pidgin* ist optimal für anonyme Jabbern vorbereitet. Er unterstützt SOCKS- und HTTP-Proxys, für jeden Account können unterschiedliche Proxys definiert werden, das OpenPGP- und OTR-Plugin für das Jabber-Protokoll ermöglicht eine starke Verschlüsselung der Chats.

Um einen Jabber-Account anonym zu nutzen, ist lediglich vor(!) der Registrierung des Accounts Tor oder JonDo als Proxy einzutragen. (Bei JonDo sind die Premiumdienste erforderlich.)

Das Bild 10.16 zeigt die Konfiguration für einen anonymen Account in Pidgin. Als Proxy-Einstellungen sind folgende Werte zu setzen:

	Tor Onion Router	JonDonym Premium
Type	Tor/Privacy	HTTP
Host	localhost	localhost
Port	9050	4001

Wichtig: Für Tor ist der Proxytyp *Tor/Privacy* (SOCKS5) zu nutzen. Die anderen Proxys sind nicht sicher und umgehen bei der Auflösung der DNS-Namen die Proxy Einstellungen. Außerdem muss Tor am Port 9050 lauschen. Dafür ist eine Anpassung der Konfiguration des TorBrowserBundles nötig, siehe: *Tor mit weiteren Anwendungen nutzen*.



Abbildung 10.16: Proxy-Einstellungen in Pidgin

Um die Möglichkeit des direkten Dateitransfers zwischen Kommunikationspartnern zu nutzen, muss ein Datei Transfer Proxy angegeben werden, da der Instant Messaging Client hinter den Proxy Kaskaden nicht direkt erreichbar ist. Man kann den Datei Transfer Proxy auf dem Reiter *Erweitert* der Kontoeinstellungen konfigurieren.

Nicht alle Jabber-Server bieten Datei Transfer Proxys an. Informationen findet man auf der Website des Anbieters. Für einige Anbieter eine kurze Liste der Datei Transfer Proxys:

- Swissjabber: *proxy.swissjabber.com*
- Draugr.de: *proxy.draugr.de*

10.9 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 ¹⁷.

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>
 - <http://storage.anonymous-proxy-servers.net> (nur für Premium-Kunden von JonDonym)
- Für Langzeit-Hosting kann man folgende Dienste verwenden:
 - <http://rapidshare.de> (benötigt Javascript)
 - <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 ein 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/>.

¹⁷ <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 Anomos-Tracker bekannt sein müssen. Download und Informationen auf der Projektwebsite <http://anomos.info>.

10.10 Invisible Internet Project

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.

Es wird die Infrastruktur des WWW genutzt, 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 I2P-Router ist auch ständig an der Weiterleitung von Daten für Andere beteiligt. Das macht die Beobachtung einzelner Teilnehmer durch Dritte nahezu unmöglich.

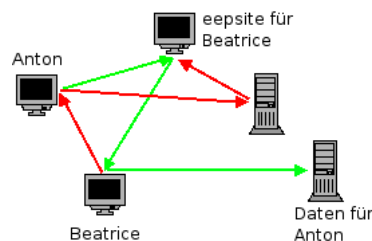


Abbildung 10.17: Prinzip von I2P

Das Projekt bietet einen Java-basierten Client. Dieser Client verschlüsselt den gesamten Datenverkehr. Außerdem stellt er sicher, dass ständig neue Verbindungen zu anderen Rechnern des Netzwerkes aufgebaut werden.

Neben der Möglichkeit, anonym zu surfen und Websites (sogenannte *eepsites*) anzubieten, sind weitere Anwendungen bereits fester Bestandteil von I2P. Es bietet anonyme E-Mail (Susimail, I2P-Bote), BitTorrent Downloads (I2Psnark), ein anonymes Usenet (Syndie) u.a.m.

Da die Nutzung der Angebote mit technischen Hürden verbunden ist, sind diese Angebote weit weniger frequentiert, als klassische Webservices.

10.10.1 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 www.i2p2.de zum Download bereit.

Als erstes ist ein Java-Runtime-Environment (JRE) zu installieren:

- **WINDOWS:** eine Version für WINDOWS bietet Oracle zum freien Download unter www.java.com an. Es ist ein kleiner Installer (.EXE) herunter

zu laden, der nach dem Start alle weiteren benötigten Komponenten lädt und installiert.

- **Linux:** bietet verschiedene Implementierungen der Java-Runtime, die mit der Paketverwaltung der jeweiligen Distribution installiert werden können. Installieren Sie das Paket *default-jre*.

II: Anschließend kann der I2P-Router installiert werden:

- **WINDOWS:** Die Datei *i2pinstall-0.x.y.exe* von der Downloadseite <http://www.i2p2.de/download.html> 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*.



Abbildung 10.18: 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>.

Hinweis: Auf dem deutschen Vista I2P NICHT in den vorgesehenen Pfad in C:/Programme installieren! Stattdessen I2P am besten in C:/I2P installieren, da es einige Probleme mit den Rechten der Programme gibt.

- **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
```

Außerdem gibt es das I2P PPA Repository von KYTV. Dieses Repository enthält neben dem I2P-Router weitere nützliche Software wie I2P-Bote, I2P Messenger, I2Py-Tahoe... Das Repository wird mit folgendem Kommando aktiviert:

```
> sudo apt-add-repository ppa:i2p.packages/i2p
```

Danach kann man wie üblich alles nötige auf die Platte spülen:

```
> sudo apt-get update
> sudo aptitude install i2p i2p-bote
```

- **Debian** Auch für Debian kann man das PPA Repository der I2P Maintainer nutzen. In die Datei */etc/apt/sources.lst* muss man für *squeeze* folgende Zeile aufnehmen:

```
deb http://ppa.launchpad.net/i2p-maintainers/i2p/ubuntu natty main
```

Für Debian *wheezy* und *sid* ist folgende Zeile zu nutzen:

```
deb http://ppa.launchpad.net/i2p-maintainers/i2p/ubuntu precise main
```

Den Signaturschlüssel des Repository fügt man mit folgendem Kommando in den apt-Keyring ein:

```
# apt-key adv --keyserver keyserver.ubuntu.com --recv-keys EB2CC88B
```

Danach kann man wie üblich den I2P-Router und nötige Hilfsprogramme auf die Platte spülen:

```
> sudo apt-get update
> sudo aptitude install i2p
```

- **Linux:** Die Installation erfolgt wie unter Windows mit der EXE-Datei *i2pinstall-0.x.y.exe* von der Downloadseite. Es ist empfehlenswert (aber nicht nötig) einen eigenen User-Account für den I2P-Router anzulegen.

```
> sudo adduser --system --disable-password --shell /bin/bash
--home /home/i2p-daemon --group i2p-daemon
```

Die Datei *i2pinstall-0.x.y.exe* ist im HOME-Verzeichnis des eingeschränkten Users zu speichern und anschließend zu starten. Der Wechsel der User-ID (erste Zeile) ist nur nötig, wenn ein eigener User für den I2P-Router angelegt wurde:

```
> sudo -u i2p-daemon
> cd ~
> java -jar i2pinstall-0.x.y.exe -console
```

Zukünftig kann der Router mit folgenden Kommandos gestartet werden:

```
> ~/i2p/i2prouter start
```

Wenn ein eigener Account für den Router eingerichtet wurde:

```
> sudo -u i2p-daemon sh /home/i2p-daemon/i2p/i2prouter start
```

Abschalten 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 AppAmor 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 30min 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.

10.10.2 Konfiguration des I2P-Router

Standardmäßig ist der I2P-Router funktionsfähig vorkonfiguriert. Ein paar kleine Anpassungen können die Arbeit etwas verbessern.

Einbindung ins I2P-Netz

Wenn der eigene I2P-Router auch vom Internet für andere Teilnehmer erreichbar ist, verbessert sich die Performance. (für fortgeschrittene Internetnutzer)

- Evtl. ist auf einem Gateway/Router ein Port Forwarding für den UDP Port zu konfigurieren.
- Außerdem braucht man einen DNS-Namen oder eine feste IP-Adresse, unter welcher der Rechner erreichbar ist. Für Einwahlverbindungen bietet z.B. dyndns.org einen entsprechenden Service.

Die Angaben können in der Router Konsole unter *configuration* (Link oben links) eingetragen werden. Auch die Begrenzung der Bandbreite für den I2P-Router kann hier dem eigenen Internetanschluss angepasst werden.

SusiDNS anpassen

Für die Zuordnung von Domain Namen 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, ist es sinnvoll, weitere subscriptions zu abonnieren. Die Einstellungen für SusiDNS findet man in der Router Konsole. Subscriptions kann man unter der Adresse

<http://localhost:7657/susidns/subscriptions.jsp> einfügen. (Bild 10.19)



Abbildung 10.19: subscriptions für SusiDNS

Folgende subscriptions bieten aktuelle Neuerscheinungen:

```
http://stats.i2p/cgi-bin/newhosts.txt
http://i2host.i2p/cgi-bin/i2hostetag
http://tino.i2p/hosts.txt
```

10.10.3 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
```

Der Proxy kann genutzt werden, um Websites im Invisible Internet aufzurufen (eepsites, erkennbar an der Toplevel Domain **.i2p**), oder um anonym im normalen Web zu surfen.

Firefox 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 10.20) 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 10.20: Firefox Profil-Manager

Anschließend kann das Profil *I2P-Fox* gestartet werden und die Proxy-Einstellungen sind wie im Bild 10.21 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.

10.10.4 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. In Abhängigkeit der auf HQ Postmaster gewählten Einstellungen kann dieser Übergang ins normale Internet bis zu 24h dauern. 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.

Router-Konsole nutzen

Ein einfaches Webinterface für Susimail ist in der I2P Router Konsole erreichbar unter der Adresse <http://localhost:7657/susimail/susimail>.

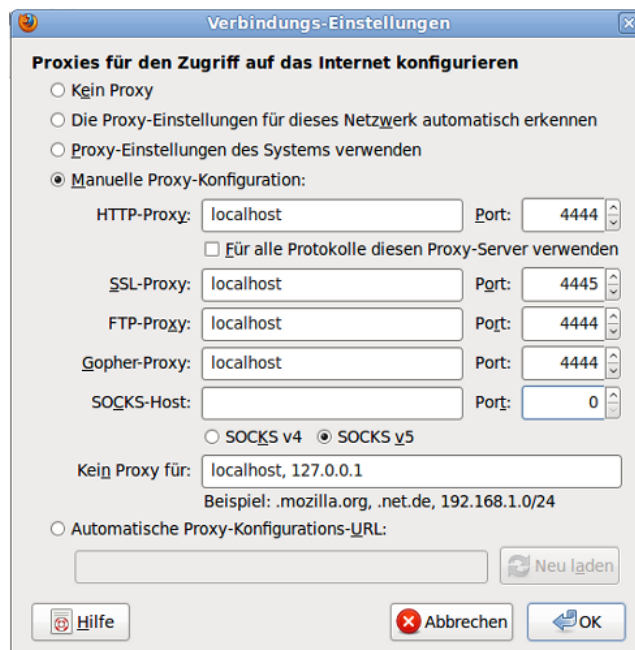


Abbildung 10.21: Firefox Proxy-Einstellungen für I2P

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 dem 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.

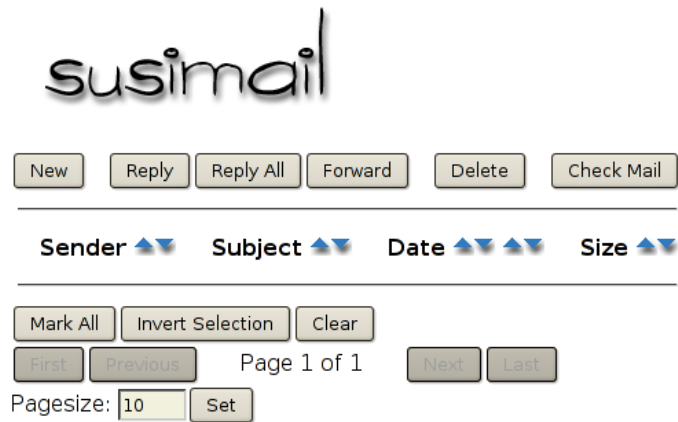


Abbildung 10.22: Webinterface von Susimail

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>

10.10.5 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.

Das Projekt ist in einem frühen Entwicklungsstadium. Es bietet folgende Features:

- Bedienung im Webinterface der I2P-Router Konsole.
- 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.

Für spätere Versionen sind folgende Feature geplant:

- POP3- und SMTP-Interface, um Mail-Clients nutzen zu können.
- Integration eines öffentlichen Adressbuches.
- Ablage von Nachrichten in selbstdefinierten Ordnern

I2P Bote ist keine Weiterentwicklung von Susimail und es soll es auch nicht ersetzen. Langfristig werden beide Projekte parallel existieren und kooperieren.

Installation von I2P Bote

Um I2P Bote zu nutzen, ist die Installation eines Plug-In für den I2P Router nötig. Auf der Seite I2P Dienste der Router Konsole (unter <http://localhost:7657/configclients.jsp>) findet man ganz unten den Abschnitt für die Installation zusätzlicher Plug-Ins (Bild 10.23).

Sollte der Download von <http://i2pbote.i2p/i2pbote.xpi2p> nicht möglich sein, kennt der eigene I2P Router möglicherweise den Server noch nicht. Man kann auch diese Adresse nutzen:

Zusatzprogramm Installation

Für die Installation eines Zusatzprogrammes bitte die Download URL eingeben:

Abbildung 10.23: Installation des Plug-in I2P Bote

<http://tjgidoycrw6s3guetge3kvrwynppqjmvqsosmtbmgqasa6vmsf6a.b32.i2p/i2pbote.xpi2p>

Nach erfolgreicher Installation findet man oben rechts einen neuen I2P Dienst "*Sichere.Mail*". Ein Klick auf den Link öffnet die Web-Oberfläche in einem neuen Browser Fenster.

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*".

Öffentlicher Name:
(Pflichtfeld, für Empfängersichtbar)

Beschreibung:
(Optional, nicht für andere sichtbar)

Mailadresse:
(Optional)

Verschlüsselung:
(Im Zweifelsfall die Voreinstellung belassen)

Elliptische-Kurven-Verschlüsselung, 256 Bit ▼

Abbildung 10.24: Neue Identität für I2P-Bote anlegen

Als Pflichtfeld ist nur ein Name anzugeben. Die Verschlüsselung belässt man am besten bei 256Bit-ECC. Diese Verschlüsselung liefert relativ kurze und starke Schlüssel. Die Mailadresse wird zur Zeit noch nicht genutzt.

Die kryptische Bote-Adresse ist an alle Partner zu verteilen oder zu veröffentlichen. In der Übersicht ist die Adresse nicht voll sichtbar. Wenn man auf die Identität klickt, erhält man eine vollständige Ansicht. Die gesammelten Adressen der Partner können in einem rudimentären Adressbuch verwaltet werden.

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.

Beim Verlassen des I2P-Bote Netzes ist keine Ende-zu-Ende-Verschlüsselung der Nachrichten gewährleistet! Bei Bedarf sind zusätzliche Tools wie OpenPGP zu nutzen, um die Vertraulichkeit der Nachricht zu gewährleisten.

- 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 [10.25](#) gezeigte Formular für eine neue Mail öffnet sich mit Klick auf den Button "Neu".

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.

Von: Anonym

An: 51uKKLjWm573IX48QyS3J8rqql → + Adressbuch...

Betreff: Test Mail

Anhänge: Anhängen

Es wird empfohlen, Anhänge kleiner als 500 kB zu halten.

Nachricht: Diese Mail ist nurein Test!
Grud

Senden Speichern

Abbildung 10.25: Neue E-Mail in I2P Bote schreiben

Eingehende Mails findet man im Ordner *Posteingang* und weitere Fragen beantworten bestimmt die FAQ von I2P Bote ¹⁸.

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 10.26: Inbox mit verifiziertem Absender

¹⁸ <http://i2pbote.net/faq.html>

SusiMail-2-Bote und Web-2-Bote

HQ Postman entwickelt einen Forward-Service von SusiMail Accounts zu I2P-Bote Adressen. Um diesen Service zu nutzen, ist als erstes ein neuer SusiMail Account auf der Seite http://hq.postman.i2p/?page_id=16 (Creating a Mailbox) anzulegen. Anschließend konfiguriert man auf der Seite http://hq.postman.i2p/?page_id=74 (Change Bote settings) die Weiterleitung. Dort ist die kryptische Bote-Adresse anzugeben. Alle Mails an diesen SusiMail Account sollen an die Bote-Adresse weitergeleitet werden.

Da der SusiMail Account auch unter der E-Mail Adresse *username@i2pmail.org* aus dem normalen Web erreichbar ist, können auf diesem Weg auch Mails von herkömmlichen E-Mail Absendern empfangen werden.

Hinweis: Die Ende-zu-Ende-Verschlüsselung ist nur innerhalb des I2P-Bote Netzes gewährleistet. Beim Übergang zu SusiMail sind zusätzliche Tools wie z.B. OpenPGP zu nutzen, um die Vertraulichkeit der Nachricht zu gewährleisten.

10.10.6 I2P IRC

IRC ist ein öffentlicher Chat Service. Auf den IRC-Servern gibt es verschiedene Chat-Räume, sogenannte Channels, in denen man sich zu einem bestimmten Thema austauschen kann. Die Unterhaltung ist in der Regel öffentlich, aber auch private Nachrichten können zwischen Nutzern ausgetauscht werden.

Das I2P-Netz bietet zwei anonyme Chat-Server, die direkt über den I2P-Router erreichbar sind. Die Konfiguration der verschiedenen Clients wie XChat (Linux/UNIX), Kopete (KDE), Colloquy (MacOS) oder Mirc (Windows) ist einfach. Man nutzt als Chat-Server folgende Adresse und ist anonym:

```
Host: localhost  
Port: 6668
```

Die wichtigsten Chat-Kommandos

Der Chat wird in der Regeln komplett durch Kommandos gesteuert. Alle Kommandos beginnen mit einem Slash. Eine kurze Liste der wichtigen 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 man einem Nicknamen unterwegs. Die Nicknamen werden registriert und mit einem Passwort geschützt, damit kein Dritter einen bekannten Nicknamen nutzen kann, um sich eine Identität zu erschleichen.

Die Registrierung erfolgt mit folgendem Kommando:

```
/msg nickserv register <Password> fake-email-addr
```

Um einen registrierten Nicknamen zu nutzen, muss man sich identifizieren:

```
/msg nickserv identify <Password>
```

#anonops

Die Channels von *Anonymous* stehen auch auf den I2P-IRC Servern zur Verfügung. Für die Diskussionen in diesen Channels sollten sie die Regeln von *Anonymous* beherzigen:

Basics: Tauchen Sie in der Masse unter ohne ein besonders smarter Typ sein zu wollen. Es gibt keine Helden, die alt geworden sind, es gibt nur junge Helden und "tote" Helden.

Geben sie keine persönlichen Informationen im public IRC preis.

- keine Anhaltspunkte im Nicknamen und Realnamen veröffentlichen
- keine persönlichen Informationen im Chat diskutieren
- keine Informationen über die Herkunft diskutieren (Land, Stadt usw.)
- keine Beschreibung von Tattoos, Piercings oder anderer Merkmale
- keine Informationen über Beruf und Hobbys
- keine Sonderzeichen wie äöü verwenden, die nur in Ihrer Sprache verfügbar sind
- veröffentlichen Sie nichts im normalen Netzm 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

10.10.7 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.

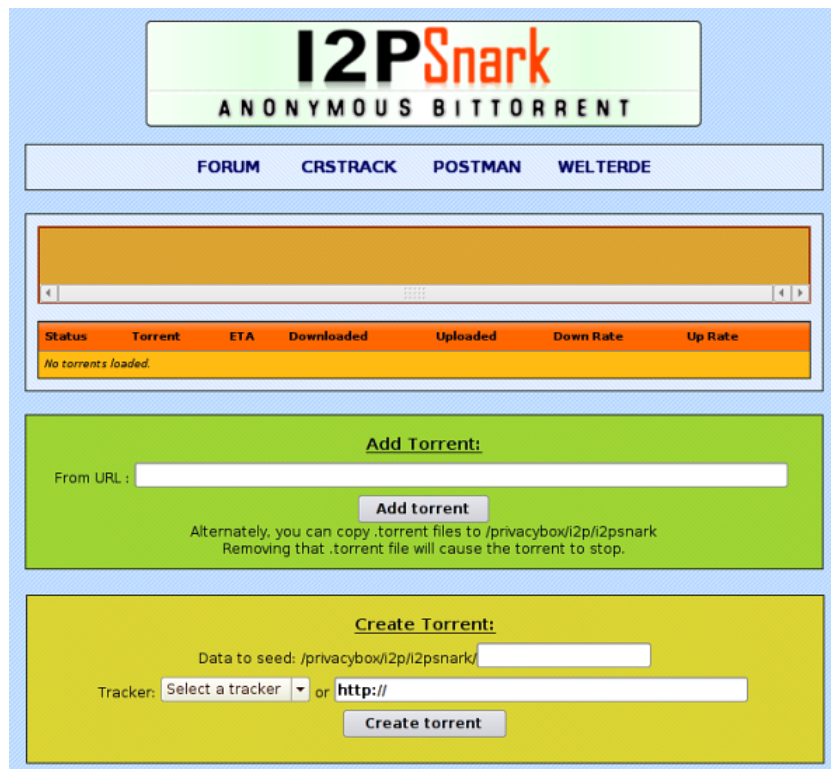


Abbildung 10.27: I2PSnark BitTorrent-Client im Webinterface

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.

Ein Stand-alone-Client steht mit I2P-BT unter <http://i2p-bt.postman.i2p> zum Download bereit.

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 herunter geladene Dateien mindestens für 1 Woche zum Upload anbieten.

10.11 Finger weg von unserösen Angeboten

Neben Projekten, die sich wirklich um eine anonyme Lösung für Surfer bemühen, gibt es immer wieder Angebote, die unbedarfte Anwender ködern wollen.

10.11.1 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 einfachen Javascripten ist es möglich, die meisten Web-Proxys zu umgehen 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. Bei einigen Web-Proxys hilft es auch nicht, Javascript usw. zu deaktivieren. Sie können mit kruden HTML-Elementen umgangen werden.

Betreiber	HTML/CSS	Javascript	Java
Anonymouse	gebrochen	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

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.

10.11.2 Free Hide IP

Free Hide IP wird von der Computerbild als Anonymisierungsdienst angepriesen.

Mit *Free Hide IP* bleiben Sie beim Surfen im Internet anonym. So sind Sie vor Datensammeln und anderen Gefahren geschützt. Die Free-Version der Software verbindet Sie nach einem Klick auf die Schaltfläche *Hide IP* mit einem amerikanischen Proxy-Server und vergibt eine neue IP-Adresse für Ihren Rechner.

Der Dienst erfüllt nicht einmal einfachste Anforderungen. Nutzer können in mehreren Varianten deanonymisiert werden beispielsweise ganz einfach mit verborgenen HTTPS-Links.

Als Tool zur Umgehung von Zensur ist der Dienst auch nicht geeignet. Die amerikanischen Proxy-Server setzen das Filtersystem *Barracuda* ein und werden die aus dem COICA-Zensurgesetz resultierenden Internetsperren umsetzen.

10.11.3 5socks.net

Im Forum der GPF tauchte vor einiger Zeit die Frage auf, was wir von *5socks.net* halten. 5socks.net ist ein Provider, die die Nutzungs von SOCKS-Proxies im Abbo anbietet.

Eine kurze Recherche brachte folgende Ergebnisse:

1. Fagen 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?

10.11.4 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. Wir raten davon ab, diese Projekte zu nutzen.

Tor BlackBelt Privacy verspricht durch eine Voodoo artige Anpassung 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 statt der üblichen drei Tor-Nodes in einer Verbindung wird die Anonymität der Nutzer stark eingeschränkt und nicht die nächste Stufe der Anonymität erreicht, wie ein schnell aufgezogenes 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 Schlüssel-fertige 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.”

10.11.5 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. Im Internet kursierende Proxy-listen 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 11

Daten verschlüsseln

Dass die Verschlüsselung von Daten der Erhaltung einer 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 Mitglieder-daten 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 wieder herstellen

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 TrueCrypt für WINDOWS 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. Wer eine **Manipulation der Sytemdaten** befürchtet, kann seinen Rechner komplett verschlüsseln (mit Truecrypt für WINDOWS, DM-Crypt für

Linux oder GELI für FreeBSD).

Zur **Herausgabe von Schlüsseln** im Fall einer Beschlagnahme des Rechners oder verschlüsselten Datenträgers gibt es immer wieder Missverständnisse.

In Deutschland gelten folgende gesetzlichen Regelungen:

- Richten sich die Ermittlungen gegen den Besitzer des Rechners oder Datenträgers muss man grundsätzlich keine Keys 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. Das die Anwendung des Gesetzes nicht auf die bösen Terroristen beschränkt ist, kann man bei [Heise](#) nachlesen. Es wurde als ersten gegen eine Gruppe von Tierschützern angewendet.

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 aber zur weiteren Untersuchung einziehen, wenn man das Passwort nicht heraus geben will. Die EFF.org rät, mit einer leeren, unverschlüsselten Festplatte einzureisen und ein datenloses Handy zu nutzen: <https://www.eff.org/wp/defending-privacy-us-border-guide-travelers-carrying-digital-devices>

11.1 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. Anschließend ist das unverschlüsselte Original NICHT(!) in den Papierkorb sondern in den Reißwolf zu werfen.

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.

11.1.1 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 **GpgSX** enthält neben einer aktuellen Version von GnuPG auch einige grafische Tools, welche die Arbeit vereinfachen. Neben einer Schlüsselverwaltung wird auch eine Erweiterung für den Explorer installiert, die Verschlüsseln und Entschlüsseln von Dateien mit wenigen Mausklicks ermöglicht.

Download: <http://gpgsx.berlios.de/>

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 für mitgenommen werden. Sie speichern die OpenPGP-Keys auf dem Stick und integrieren sich nicht in den Explorer.
3. Die Programme **GnuPG** und **GPGShell**: GPGshell ist ein grafisches Tool, welches auch das Kontextmenü des Explorers erweitert. Kai Raven hat unter <http://hp.kairaven.de/pgp/gpg/gpg7.html> eine ausführliche Anleitung zur Nutzung geschrieben.

Das Erzeugen und Verwalten der Schlüssel ist im Kapitel *E-Mails verschlüsseln* beschrieben.

Sollen mehrere Dateien in einem Container verschlüsselt werden, erstellt man ein neues 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. Es sind danach alle(!) Originaldateien in den Reißwolf zu werfen.

11.2 Truecrypt für WINDOWS

Truecrypt basiert auf dem Projekt *Encryption for the masses*. Die Software bietet transparente Ver- und Entschlüsselung beim Laden oder Speichern von Daten unter WINDOWS XP/2000/2003 und Linux. Neben der Verschlüsselung von Daten auf der Festplatte ist es auch für USB-Sticks geeignet.

Eine passende Metapher für das Konzept von Truecrypt ist der Container. Ein Container steht rum und nimmt Platz weg, egal ob er leer oder voll ist. In diesem Fall belegt der Container Platz auf der Festplatte oder dem USB-Stick.

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.

Mit doppeltem Boden

Ein Feature von Truecrypt ist das Konzept des *versteckten Volumes*, eine Art doppelter Boden für den 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 hinter dem 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 Index verschiedener Programme für die Indexierung der Dokumente auf dem lokalen Rechner (WINDOWS Suche, Google Desktop Search...)

liefern möglicherweise Hinweise auf den versteckten Container.

Wie gulli.com am 6.10.08 berichtete, ist es unter Umständen möglich, die Existenz des versteckten Volumes nachzuweisen. Also Vorsicht bei Nutzung dieses Features.

11.2.1 Truecrypt installieren

Für die Installation von Truecrypt werden folgende Pakete benötigt:

- Truecrypt von der Site des Projektes www.truecrypt.org
- Deutsche Sprachanpassung aus den [Language Packs](#) von Truecrypt

Nach dem Download sind die ZIP-Archive zu entpacken. In dem neuen Ordner *truecrypt-x.y* findet man die Setup-Datei. Diese ist als Administrator zu starten und in dem Install-Assistenten sind die Vorgaben evtl. anzupassen.

Ein Klick auf den Button *Install* startet den Prozess. Im Anschluß findet man ein Icon auf dem Desktop und einen neuen Eintrag im Menü.

Anschließend ist die Datei *Language.de.xml* aus dem Paket der Sprachanpassung in das Verzeichnis der installierten EXE-Datei zu kopieren.

11.2.2 Gedanken zum Schlüssel

Bevor man einen verschlüsselten Container erstellt, sollte man sich Gedanken über den Schlüssel zum Öffnen des Containers machen.

- Eine **Passphrase** sollte gut merkbar sein und mindestens 20 Zeichen lang sein. Außer Buchstaben sollte sie auch Sonderzeichen und Ziffern enthalten. Das schüttelt man nicht einfach aus dem Ärmel. Wie wäre es mit folgender Phrase:

das geht nur %mich% _AN_

- Ein **Keyfile** kann eine beliebige Datei mit mindestens 1024 Byte Größe sein. Truecrypt bietet die Möglichkeit, gute Keyfiles zu generieren (Menüpunkt: *Schlüsseldateien -> Schlüsseldatei aus Zufallswerten erstellen* im Hauptfenster).

Man kann z.B. einen USB-Stick mit Keyfile(s) vorbereiten. Dieser Stick enthält eine oder mehrere Dateien, welche als Keyfile(s) genutzt werden. Diese Datei(en) können als Standardschlüssel definiert werden (Menüpunkt: *Schlüsseldateien -> Standardschlüsseldateien festlegen*). Zukünftig ist vor dem Öffnen eines Containers lediglich der Stick einzustecken. Es funktioniert wie ein mechanischer Schlüssel und man wird nicht mehr mit einer Passwortabfrage belastigt.

11.2.3 Verschlüsselten Container erstellen

Startet man Truecrypt oder klickt auf das blaue Symbol im Systray, so öffnet sich das Hauptfenster. Der Button *Volume erstellen* ruft einen Assistenten auf, der schrittweise alle nötigen Angaben zur Erstellung eines Volumes abfragt und umfangreiche Erläuterungen bietet.

Eingeschränkte Nutzer können lediglich verschlüsselte reguläre Containerdateien erstellen.

Administratoren können außerdem Festplattenpartitionen und USB-Sticks verschlüsseln, Hidden Volumes (versteckte Container) erstellen und WINDOWS komplett verschlüsseln.



Abbildung 11.1: Assistent zur Erstellung eines Containers

Im Folgenden wird der Ablauf zur Erstellung einer verschlüsselten Containerdatei beschrieben:

1. Auswahl des Containertypes (reguläres oder verstecktes Volume). Soll ein verstecktes Volume erstellt werden, ist zuerst ein normales Volume zu erstellen, in dem anschließend das zweite Volume versteckt werden kann.
2. Im zweiten Schritt ist der Dateiname für den Container anzugeben oder als Datenträger die Festplattenpartition bzw. der USB-Sticks (nur als Administrator). Es ist auch als eingeschränkter Nutzer möglich, eine Datei auf einem USB-Stick zu erstellen. Diese Datei könnte 2/3 des Sticks einnehmen. Der Stick kann dann bei Notwendigkeit auch ohne Truecrypt genutzt werden.
3. Im dritten Schritt ist die Größe der Datei anzugeben. Dieser Schritt entfällt, wenn eine Partition oder USB-Stick komplett verschlüsselt wird.

4. Im vierten Schritt ist der Schlüssel für das Öffnen des Containers festzulegen. Ein gutes Passwort sollte mindestens 20 Zeichen lang sein. Wer Probleme mit Passwörtern hat, läßt die Eingabefelder leer und nutzt Key-files (z.B. vom vorbereiteten USB-Stick).
5. Die Verschlüsselungseinstellungen im fünften Schritt sind mit den Defaultwerten sinnvoll vorbelegt.
6. Im letzten Schritt ist das Dateisystem festzulegen, mit welchem der verschlüsselte Bereich formatiert wird. FAT32 ist in den meisten Fällen ausreichend und kann auch unter Linux gelesen werden. Lediglich für sehr große Container oder die Verschlüsselung der *Eigenen Dateien* würden wir NTFS empfehlen.
7. Im Anschluß wird der Container erstellt. Es ist empfehlenswert, dabei mit der Maus einige sinnlose Bewegungen auszuführen, um hinreichend Entropie für die Zufallsinitialisierung anzusammeln.

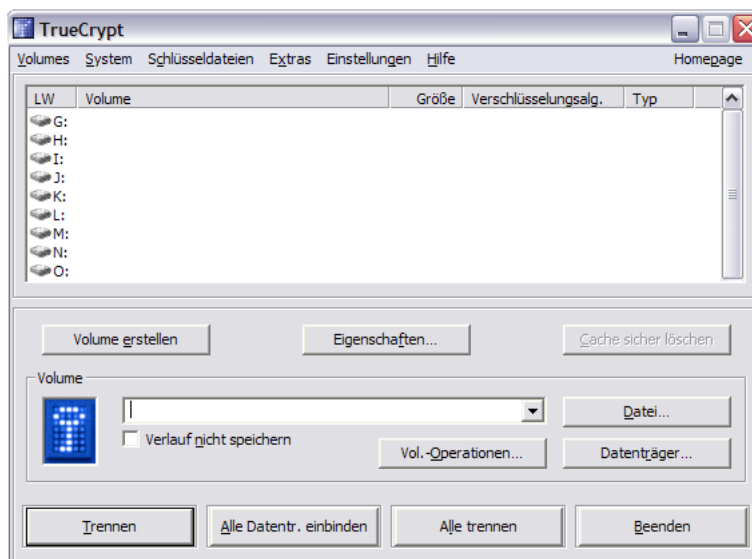


Abbildung 11.2: Hauptfenster von Truecrypt

11.2.4 Verschlüsselten Container öffnen

Truecrypt-Container werden beim Öffnen grundsätzlich als neue Laufwerke eingehängt. Das in Bild 11.2 dargestellte Hauptfenster von Truecrypt bietet die Möglichkeit, einen Buchstaben für das Laufwerk und die einzubindende Container-Datei bzw. den Datenträger zu wählen.

Zu beachten ist die Option *Verlauf nicht speichern*. Ist diese Option aktiv, wird die Historie der geöffneten Container ständig gelöscht. Die Container sind auf der Festplatte oder dem USB-Stick nicht anhand eines speziellen

Header als verschlüsselte Bereiche erkennbar. Sie sehen aus, wie zufälliger Datenmüll.

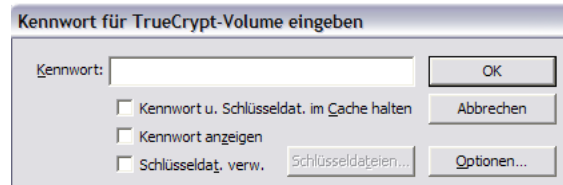


Abbildung 11.3: Eingabe des Schlüssels

Anschließend ist der Button *Einbinden* zu wählen. Das in Bild 11.3 dargestellte Fenster zur Eingabe der Schlüssel erscheint. Hier ist der Schlüssel für das Öffnen des Containers einzugeben (die Passphrase oder/und das Keyfile).

Einige Abkürzungen für das Öffnen von Containern:

- Ein Klick auf eine Datei mit der Endung .tc im Explorer öffnet das Hauptfenster von Truecrypt und setzt den Namen der Datei als zu öffnendes Volume.
- Es ist möglich, Favoriten zu definieren und diese alle zusammen über den Menüpunkt *Volumes -> Favoriten einbinden* einzubinden. Favoriten definiert man, indem diese Container eingebunden werden und anschließend die Konfiguration über den Menüpunkt *Volumes -> als Favoriten speichern* gesichert wird.
- Als Favoriten definierte Container können bei Start von Truecrypt automatisch eingebunden werden. Unter *Einstellungen -> Voreinstellungen* ist hierfür die entsprechende Option zu aktivieren.
- Wird Truecrypt bei der Anmeldung automatisch gestartet, können auch die Favoriten bei Anmeldung eingebunden werden.
- Der Button *Alle Datentr. einbinden* untersucht alle Partitionen und USB-Sticks auf Verschlüsselung. Es erscheint nacheinander der Dialog für die Schlüsseingabe. Der Vorgang kann einige Zeit dauern.

11.2.5 Verschlüsselten Container schließen

Alle geöffneten Container werden standardmäßig bei der Abmeldung geschlossen. Außerdem gibt es mehrere Möglichkeiten, einen geöffneten Container während der Arbeit wieder zu schließen:

- Ein Klick mit der rechten Maustaste auf das Truecrypt-Icon im Systray öffnet ein Menü, welches für alle eingebundenen Container das Trennen anbietet.
- Im Hauptfenster von Truecrypt kann man mit der rechten Maustaste auf einen eingebundenen Container klicken und ihn trennen.

- Der Button *Alle trennen* im Hauptfenster von Truecrypt schließt alle eingebundenen Container.

ACHTUNG: Auch ein Beenden von Truecrypt im Systray schließt die Container nicht(!). Der Dämon läuft weiter. Erst die Abmeldung des Nutzers oder ein Ausschalten des Systems schließt alle Container.

11.2.6 WINDOWS komplett verschlüsseln

Die aktuelle Version von Truecrypt ermöglicht es, WINDOWS bei laufenden Betrieb in einen verschlüsselten Container zu verschieben. Damit ist es für einen heimlichen Besucher sehr schwer, das System im ausgeschalteten Zustand zu kompromittieren. Es ist jedoch nicht unmöglich, wie das Stoned Bootkit zeigt, siehe <http://www.stoned-vienna.com>.

Wichtig: Voraussetzung für die Nutzung dieses Features ist die Möglichkeit, ein CD-ISO-Image zu brennen. Dieses Image, welches während der Installation angelegt und geprüft wird, enthält wesentliche Daten für die Wiederherstellung, wenn es zu Bitfehlern im Header der Systempartition kommt.

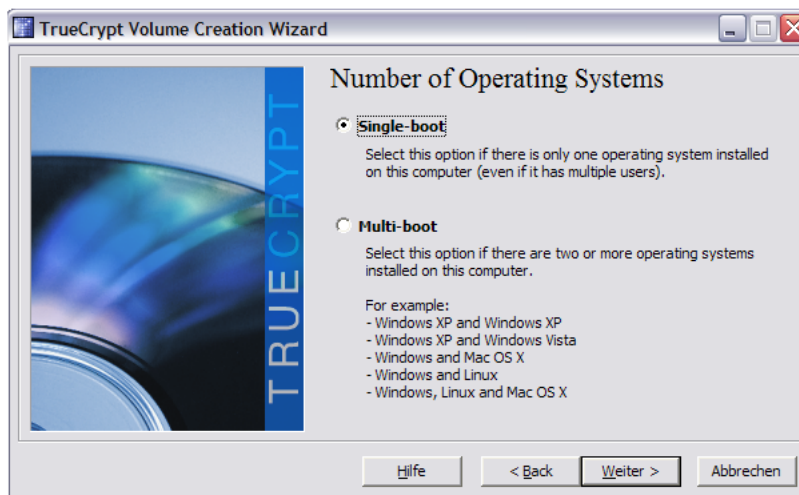


Abbildung 11.4: Assistent für die System-Verschlüsselung

Den Assistent für die Systemverschlüsselung startet man im Hauptfenster von Truecrypt über den Menüpunkt *System - Encrypt System Partition*. Als Erstes wird abgefragt, ob nur die Partition von WINDOWS verschlüsselt werden soll oder die gesamte Festplatte. Die Verschlüsselung der gesamten Festplatte funktioniert nicht, wenn die Platte eine erweiterte Partition mit logischen Partitionen enthält oder wenn mehrere Betriebssysteme installiert sind.

Da der Masterboot-Record modifiziert wird, bemüht sich Truecrypt, häufige Kombinationen verschiedener Betriebssysteme zu berücksichtigen.

Nach der Abfrage des Algorithmus für die Verschlüsselung, der Passphrase (Die mindestens 20 Zeichen lang sein sollte, Keyfiles können nicht genutzt werden!), und der Generierung von Zufallszahlen folgt die Erstellung der Rescue Disk (Bild 11.5).

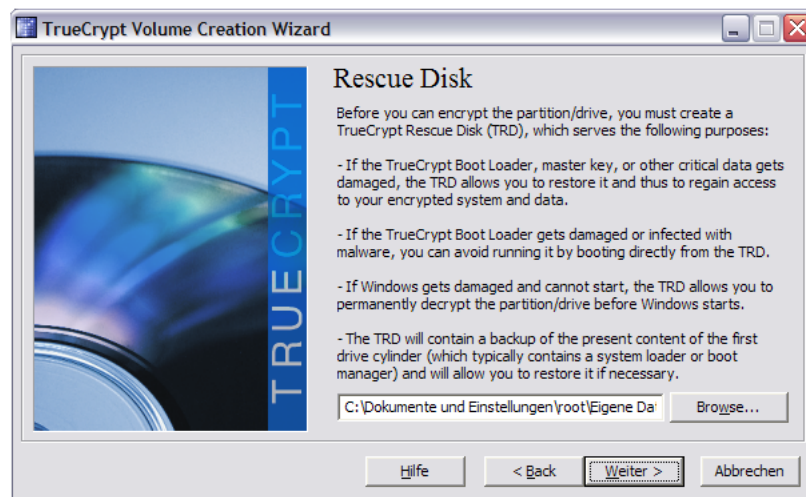


Abbildung 11.5: Erstellung der Rescue-Disk

Die Rescue-Disk wird als ISO-Image auf der Festplatte abgelegt und ist auf eine CD zu brennen. Die neue CD ist ins Laufwerk einzulegen. Truecrypt arbeitet erst weiter, wenn es die korrekte Erstellung der CD überprüft hat.

Im vorletzten Schritt, stellt Truecrypt mehrere Möglichkeiten zum Löschen der alten, unverschlüsselten Daten zur Auswahl. Es genügt, die Daten einmal zu überschreiben. Dabei werden nicht die einzelnen Dateien überschrieben, sondern die Platte wird sektorenweise bearbeitet. Das garantiert, dass auch Fragmente gelöschter Dateien beseitigt werden.

Da es sich bei der Systemverschlüsselung um einen tiefen Eingriff handelt, führt Truecrypt als nächstes einen Test durch. Der PC wird neu gebootet und der Anwender muss am Bootloader sein Passwort eingeben.

Erst wenn dieser Test erfolgreich war, erfolgt die Verschlüsselung des Systems. Dieser Vorgang nimmt je nach Größe der Platte einige Zeit in Anspruch, ca 1-2min pro GByte.

Nach Abschluß der Operation ist das System neu zu booten. Dabei wird vom Bootloader wieder das Passwort für den Zugriff auf die Systempartition abgefragt.

11.2.7 Traveller Disk erstellen

Truecrypt ermöglicht es, unter dem Menüpunkt *Extras* -> *Traveller Disk erstellen* einen USB-Stick zu verschlüsseln und zusätzlich die Software selbst in einem unverschlüsselten Bereich hinzuzufügen.

Der Stick kann so konfiguriert werden, dass beim Anschließen des Sticks mit Hilfe der Autostart Funktion Truecrypt startet, den verschlüsselten Container einbindet und den Explorer öffnet.

Dieses Feature soll es ermöglichen, einen verschlüsselten USB-Stick auch an Computern zu nutzen, auf denen Truecrypt nicht installiert ist.

Da man für diese Funktion Rechte als Administrator auf dem fremden Rechner benötigt, halte ich das Feature eher für Spielerei. Ein verantwortungsvoller Eigentümer hat mir noch nie diese Rechte eingeräumt und auch ich würde mir gut überlegen, ob jemand auf meinem Rechner Software installieren darf. Für viele Nutzer könnte es aber ein sinnvolles Feature sein.

11.3 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 Befehlen 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, das 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.

11.3.1 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 20 Zeichen lang sein. Soetwas 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.

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.

11.3.2 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 `luksformat`, 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-cbc-essiv:sha256 -s 256 -y
/dev/loop0 [ keyfile ]
```

4. Das formatierte 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
```

11.3.3 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.

Für das Hinzufügen eines Passwortes zu der verschlüsselten Imagedatei *geheim.img* im aktuellen Verzeichnis ist diese zuerst einzuhängen, beispielsweise als */dev/loop5*. Dieser Schritt entfällt für 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/hda5* für eine Festplattenpartition anzugeben ist. Das Keyfile ist optional.

```
# cryptsetup 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 bis 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
```

11.3.4 Verschlüsselten Container öffnen/schließen

Aktuelle Distributionen wie Debian oder Ubuntu erkennen verschlüsselte Partitionen auf Festplatten und USB-Sticks automatisch und fragen die Passphrase ab, sobald das Gerät erkannt wird. Einfach Anschließen, auf den Passwort-Dialog wie im Bild [11.6](#) warten - fertig.



Abbildung 11.6: Passwort-Abfrage für verschlüsselten USB-Stick

Auf der Kommandozeile

Sollte es mit dem automatischem Öffnen des verschlüsselten USB-Sticks nicht funktionieren, kann man auf der Kommandozeile nachhelfen. *pmount* arbeitet mit User-Privilegien und bindet die Partition unter */media* ein. *pmount* kann keine Containerdateien öffnen.

```
> pmount /dev/sda1
Enter LUKS passphrase:
```

Geschlossen wird der Container mit *pumount*:

```
> pumount /dev/sda1
```

Die Sammlung *pam-mount* enthält zwei weitere Skripte, welche die Arbeit mit verschlüsselten Containerdateien vereinfachen. Wurde außerdem *sudo* entsprechend konfiguriert, stehen die folgenden Kommandos jedem Nutzer zur Verfügung. Eine verschlüsselte Partition (beispielsweise der USB-Stick unter */dev/sda1*) kann mit folgendem Kommando geöffnet und im Verzeichnis */mnt* eingebunden werden:

```
> sudo /sbin/mount.crypt /dev/sda1 /mnt
Enter LUKS passphrase:
```

Das folgende Kommando öffnet die verschlüsselte Imagedatei *geheim.luks* aus dem aktuellen Verzeichnis und hängt sie unter */mnt* in das Dateisystem ein:

```
> sudo /sbin/mount.crypt geheim.luks /mnt -o loop
Enter LUKS passphrase:
```

Geschlossen wird der Container mit folgendem Kommando:

```
> sudo /sbin/umount.crypt /mnt
```

Für häufig genutzte Container könnte man einen Menüeintrag oder ein Desktop-Icon anlegen. Dabei ist zu beachten, dass die Option *Im Terminal ausführen* aktiviert wird! Anderenfalls kann man keine Passphrase eingeben.

Für jene, die es genau wissen wollen

Das Öffnen einer Containerdatei auf der Komandozeile erfordert drei Schritte als *root*. Als erstes ist die verschlüsselte Imagedatei einzuhängen. Dieser Schritt entfällt für Partitionen. Im zweiten Schritt ist das verschlüsselte Device dem Device-Mapper zu unterstellen. Der Name kann dabei frei gewählt werden. Im dritten Schritt kann es mit *mount* in das Dateisystem eingehängt werden, beispielsweise nach */mnt*.

```
# losetup /dev/loop5 geheim.luks
# cryptsetup luksOpen /dev/loop5 <name> [ keyfile ]
# mount /dev/mapper/<name> /mnt
```

Das Schließen des Containers erfolgt in umgekehrter Reihenfolge:

```
# umount /mnt
# cryptsetup luksClose <name>
# losetup -d /dev/loop5
```

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.

11.3.5 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
```

Ubuntu-Nutzer können die **alternate desktop cd** nutzen, die kein Live-System enthält, dafür aber mehr Optionen für die Installation bietet. Die Standard-Edition von Ubuntu bietet dieses Feature nicht!

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 Verzeichnisses */boot* und bootet in Zukunft immer von der CD. (Oder man geht zum Psychater 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.

11.3.6 HOME-Verzeichnis verschlüsseln

Die Verschlüsselung der persönlichen Daten im *\$HOME*-Verzeichnis bieten alle Linux-Distributionen bei der Installation an. Wer keine Kompletterschlüsselung 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.

11.3.7 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
```

11.4 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 haben 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.

11.4.1 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 Backup Medien befürchtet, findet vielleicht eine Anregung bei [true-random](http://true-random.com/homepage/projects/usbsticks/small.html)¹.

Das Backup-Medium sollte man mit TrueCrypt 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 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 öffnen². Viele USB-Sticks mit Verschlüsselung verwenden zwar starke Algorithmen (in der Regel AES256), legen aber einen zweiten Schlüssel zur Sicherheit

¹ <http://true-random.com/homepage/projects/usbsticks/small.html>

² <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 Heise³ zeigt.

Unison-GTK

Für die Synchronisation der Daten steht z.B. Unison-GTK⁴ 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.

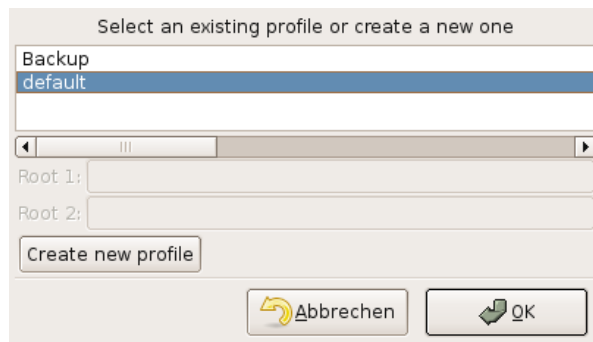


Abbildung 11.7: Profil nach dem Start von Unison-GTK auswählen

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 11.7).

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.

³ <http://heise.de/-894962>

⁴ <http://www.cis.upenn.edu/~bcpierce/unison/>

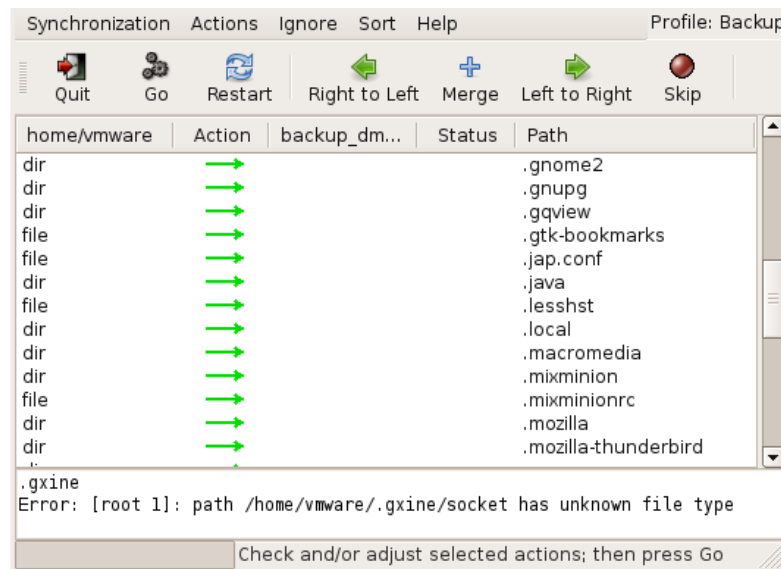


Abbildung 11.8: Hauptfenster von Unison-GTK

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 grafischen Interface für rsync. Auch dieses Tool ist in allen Linux/Unix Distributionen enthalten.

Nach dem Start kann man mit dem Button “+” mehrere Profile für verschiedene, wiederkehrende Aufgaben anlegen. Jedem Profil wird ein Quell- und ein Zielverzeichnis sowie die rsync-Parameter zugeordnet. Ein Klick auf die kleine Rakete oben rechts startet die Synchronisation (Bild 11.9).

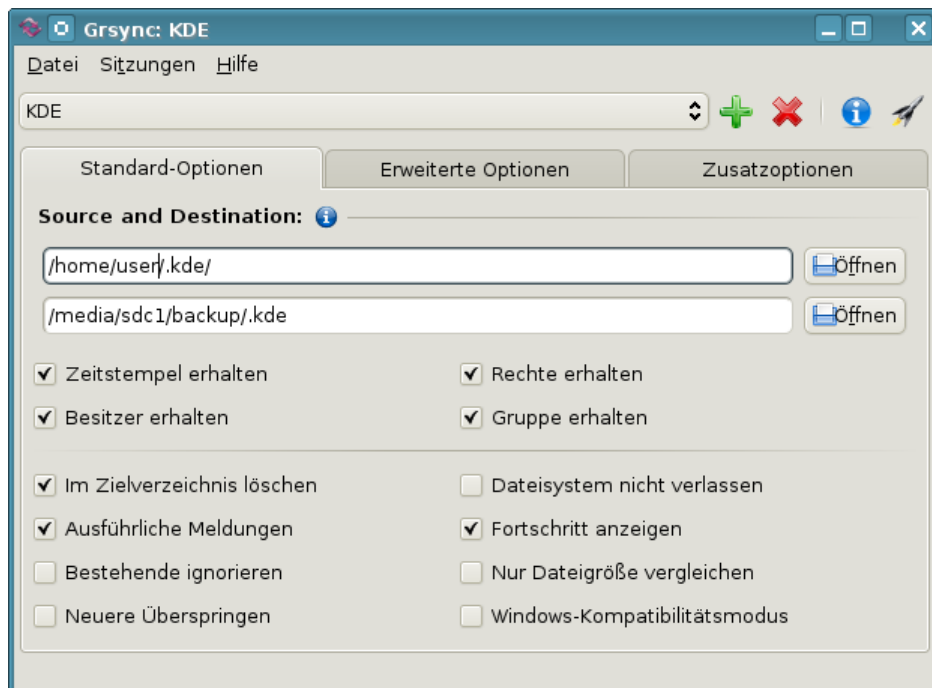


Abbildung 11.9: Hauptfenster von Grsync

11.4.2 Backups mit aespipe verschlüsseln

aespipe ist Teil des AES-Loop Projektes und steht in fast allen Linux Distributionen zur Verfügung. Das Paket kann mit den Paketmanagern der Distribution installiert werden.

Verschlüsseln

Das Programm *aespipe* tut, was der Name vermuten läßt. Es ver- und entschlüsselt einen Datenstrom in einer Pipe mit dem AES-Algorithmus. Ein ganz einfaches Beispiel:

```
> tar -cj datadir | aespipe > data.tar.bz2.enc
```

Der Inhalt des Verzeichnisses *datadir* wird in ein komprimiertes TAR-Archiv gepackt und anschließend verschlüsselt in die Datei *data.tar.bz2.enc* geschrieben. Dabei wird eine mindestens 20 Zeichen lange Passphrase abgefragt.

Wer eine etwas stärkere Verschlüsselung nutzen möchte:

```
> tar -cj datadir | aespiped -C 10 -e aes256 > data.tar.bz2.enc
```

Die Option *-C 10* bewirkt, dass der Schlüssel selbst 10.000x mit AES bearbeitet wird. Das erschwert Brute-Force-Attacken. Mit *-e aes256* nutzt das Programm 256 Bit lange Schlüssel.

Es ist auch möglich, eine asymmetrische Verschlüsselung mit einem GnuPG-Key zu nutzen. Das Passwort wird dabei mit dem Programm *gpg* verschlüsselt:

```
> tar -cj data_dir | aespiped -K gpgkey > data.tar.bz2.enc
```

Der GnuPG-Key kann dabei mit seiner ID (z.B. 0x35AD65GF) oder mit einer E-Mail Adresse spezifiziert werden und sollte als vertrauenswürdiger Key im Keyring vorhanden sein.

Entschlüsseln

Entpacken kann man das verschlüsselte Archiv mit folgendem Kommando:

```
> aespiped -d < data.tar.bz2.enc | tar -xj
```

Für Maus-Schubser

Die Dateimanager der Linux-Desktops KDE und Gnome bieten mit sogenannten *Aktionen* die Möglichkeit, zusätzlich Befehle in das Kontextmenü der Dateien zu integrieren. Für Konqueror (KDE) erstellt man eine kleine Textdatei und speichert sie mit der Endung *.desktop* im Verzeichnis */kde/share/apps/konqueror/servicemenus*

Die Datei *encryptfileaespipe.desktop* könnte folgenden Inhalt haben:

```
[Desktop Entry]
ServiceTypes=all/allfiles
Actions=encryptfileaespipe

[Desktop Action encryptfileaespipe]
TryExec=aespipe
Exec=konsole -e bash -c "cat %f | aespiped -T > %f.enc"
Name=Datei verschlüsseln (aespipe)
Icon=encrypted
```

Zukünftig findet man im Kontextmenü einer Datei unter *Aktionen* den Menüpunkt *Datei verschlüsseln (aespipe)* (Bild 11.10). Wählt man diesen Punkt, öffnet sich ein Terminal zur doppelten Passwortabfrage. Anschließend findet man eine neue Datei im Verzeichnis mit der zusätzlichen Endung *.enc*, die man auf das Backup-Medium schieben kann. Verzeichnisse sind zuerst zu komprimieren. Einträge dafür sind im Servicemenü bereits vorhanden.

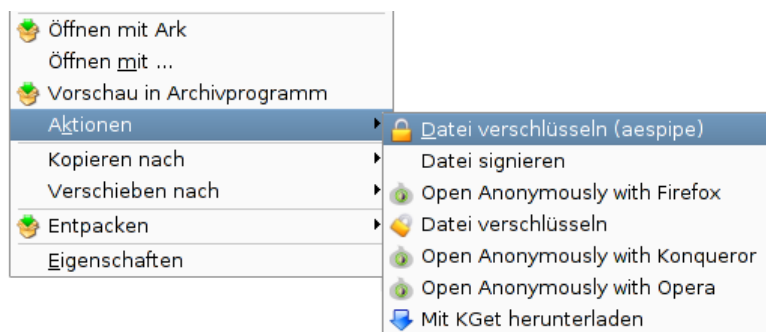


Abbildung 11.10: Neue Aktion im Servicemenü von Konqueror

11.4.3 Verschlüsselte Backups mit dar

Der Disk Archiver *dar* steht auf der Projektwebseite⁵ zum Download bereit und ist auch in fast allen Linux Distributionen enthalten. Mit KDar⁶ (für KDE) und DarGUI⁷ (für GTK) stehen grafische GUIs zur Verfügung.

Ich möchte hier nicht das 30-seitige Manual-Page von *dar* wiedergeben, das Programm bietet viele Möglichkeiten, und beschränke mich auf die einfache Erstellung eines verschlüsselten, komprimierten Backups für ein abgeschlossenes Projekt. Neben diesem einfachen Voll-Backup sind auch inkrementelle Backups möglich, eine Manager zur Verwaltung verschiedener Backups steht zur Verfügung, spezielle Optionen für Cron-Jobs...

Standardmäßig erstellt *dar* ein Backup der Dateien des aktuellen Verzeichnisses:

```
> cd $HOME/Projekt_X
> dar -c $HOME/backup/projekt_full -K bf:
```

Mit der Option “-K bf:” aktiviert man die Verschlüsselung. Es wird beim Erstellen des Backups nach einer Passphrase gefragt.

Nach dem Durchlauf des Programms findet man im Verzeichnis \$HOME/backup die Dateien *projekt_full.1.dar*, *projekt_full.2.dar*.... usw. Das gesamte Backup wird Brenner-freundlich in mehrere Slices aufgeteilt, die man auf eine CD oder DVD brennen kann. Die weiteren Parameter können in einer Konfigurationsdatei festgelegt werden.

Um ein inkrementelles Backup zu erstellen, das auf ein älteres Backup aufbaut und nur geänderte Dateien sichert, ist die Option -A mit den Pfad zum alten Backup anzugeben:

```
> cd $HOME/Projekt_X
> dar -c $HOME/backup/projekt_diff1 -A $HOME/backup/projekt_full -K bf:
```

⁵ <http://dar.linux.free.fr>

⁶ <http://sourceforge.net/projects/kdar/>

⁷ <http://sourceforge.net/projects/dargui/>

Das Wiederherstellen des Backups von den CD-ROMs ins aktuelle Verzeichnis erfolgt mit folgendem Kommando:

```
> mkdir Projekt_X
> cd Projekt_X
> dar -x -p /media/cdrom
```

Die Option -p sorgt dafür, dass nach jedem Slice eine Pause gemacht wird, um dem User die Möglichkeit zu geben, die CD zu wechseln.

Um nicht bei jedem Aufruf einen Rattenschwanz von Optionen angeben zu müssen, bietet dar die Möglichkeit, Standards in den Dateien /etc/darrc oder \$HOME/.darrc zu speichern. Die folgende kommentierte Vorlage kann in einen Editor übernommen und gespeichert werden:

```
# Allgemeine Optionen
all:

# Backups mit gzip komprimiert
-z9
# Backups mit Blowfish verschlüsselt
-K bf:

# Option für das Anlegen von Backups
create:

# Größe einer Slice (für DVDs: -s 4G)
-s 700M
# Komprimierte Dateien nicht nochmals komprimieren
-Z *.gz
-Z *.bz2
-Z *.mp3
# Keine BAK-Dateien sichern
-X *~
-X *.bak

# Option für das Extrahieren von Backups
extract:

# ein Beep nach jedem Slice
-b
```

Weitere Optionen findet man in der Dokumentation.

11.4.4 Online Backups

Neben dem Backup auf einem externen Datenträger kann man auch Online-Speicher nutzen. Angebote ab 3,- Euro monatlich bieten DataStorageUnit.com, ADrive.com, rsync.net u.v.a.m. Wer einen eigenen (V)Server gemietet hat, kann seine Backups auch dort ablegen.

Ein Online-Backup ist praktisch, wenn man mit Laptop in ein Land wie USA reist. Bei der Einreise werden möglicherweise die Daten der Laptops gescannt und auch kopiert. Die EFF empfiehlt, vor der Reise die Festplatte zu "reinigen"⁸. Man könnte ein Online-Backup erstellen und auf dem eigenen Rechner die Daten sicher(!) löschen, also *shred* bzw. *wipe* nutzen. Bei Bedarf holt man sich die Daten wieder auf den Laptop. Vor der Abreise wird das Backup aktualisiert und lokal wieder alles gelöscht.

An ein Online-Backup werden folgende Anforderungen gestellt:

- Das Backup sollte verschlüsselt werden, um die Vertraulichkeit zu gewährleisten.
- Es sollten nur geänderte Daten übertragen werden, um Zeitbedarf und Traffic auf ein erträgliches Maß zu reduzieren.

Die denkbar schlechteste Variante ist es, einen reichlich überdimensionierten Truecrypt Container zu erzeugen, die zu sichernden Daten hinein zu kopieren und bei jedem Backup den ganzen Container in den Online-Speicher zu kopieren. Bei einigen 100 GB dauert der Upload mehrere Stunden.

Etwas weniger Ballast erhält man, wenn die zu sichernden Daten in ein komprimiertes Archiv verpackt werden. Dieses Archiv wird verschlüsselt, z.B. mit OpenPGP oder *aespipe*. Dann überträgt man es in den Online-Speicher. Diese Variante ist aber auch nur suboptimal.

Die alltagstauglichste Variante sind Backup-Tools, die nur geänderte Daten synchronisieren und beim Upload die Daten automatisch 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 *Verz* 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:

⁸ (<http://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t>)

```
#!/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 garnicht 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 12

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.

12.1 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.

12.2 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 -rcf 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.

12.3 Dateireste nachträglich beseitigen

Mit Bleachbit¹ 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 12.1). 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*.

¹ <http://bleachbit.sourceforge.net/download>

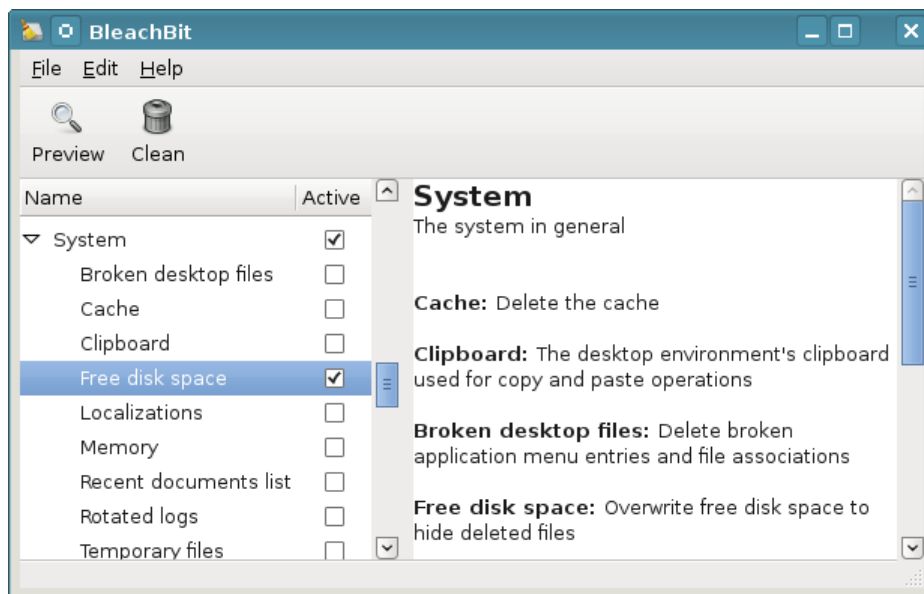


Abbildung 12.1: Bleachbit

Die Säuberung einer größeren Festplatte dauert einige Zeit. Dabei werden nur die als *frei* gekennzeichneten Bereiche überschrieben, das Dateisystem bleibt intakt.

12.4 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* ².

Für SSDs ist die Trim Funktion zu aktivieren. Dabei werden den 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 Betriebssysteme 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:

² http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf

```
> fsutil behavior query disableddeletenotify
```

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 disableddeletenotify 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.

Hinweise: Debian *squeeze* verwendet noch einen Kernel 2.6.32. und kann mit der Option `discard` nichts anfangen.

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.

12.5 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) ³ 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.

³ <http://www.dban.org/>

Eine beliebige Linux Live-CD tut es auch (wenn man bereits eine Live-CD nutzt). Nach dem Booten des Live Systems öffnet man ein Terminal (Konsole) und überschreibt die gesamte Festplatte. Bei einem Aufruf wird der Datenträger 4x überschrieben, es dauert einige Zeit.

Für die erste IDE-Festplatte:

```
> wipe -kq /dev/hda
```

Für SATA- und SCSI-Festplatte:

```
> wipe -kq /dev/sda
```

Wenn die Live-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.)

12.6 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/sdc1
```

Kapitel 13

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 finden¹.

Der *StolenCameraFinder*² 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.

13.1 Fotos und Bilddateien anonymisieren

- **Irfan View**³ (Windows) kann in Fotos mit *Öffnen* und *Speichern* die Metatags entfernen. Im Batchmode kann man die Funktion *Konvertieren* nut-

¹ <http://www.tech-review.de/include.php?path=content/news.php&contentid=14968>

² <http://www.stolencamerafinder.com>

³ <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.

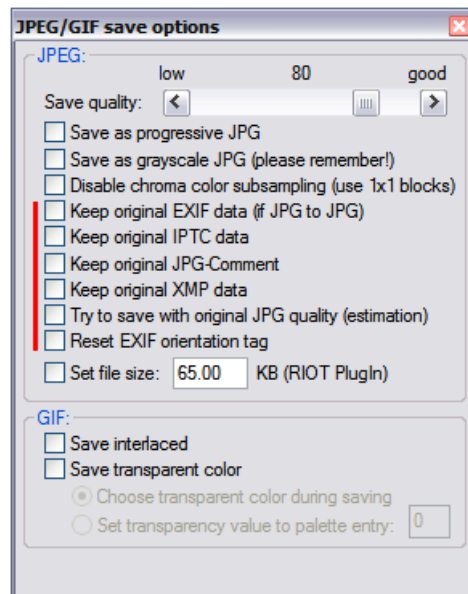


Abbildung 13.1: Informationen in Fotos löschen mit Irfan View

- **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
```

13.2 PDF-Dokumente säubern

Für Windows gibt es das Tool **BeCyPDFMetaEdit** ⁴ 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.

13.3 Metadata Anonymisation Toolkit (MAT)

Metadata Anonymisation Toolkit (MAT) ⁵ wurde im Rahmen des GSoC 2011 unter Schirmherrschaft von TorProject.org entwickelt. Es ist vor allem unter

⁴ http://www.becyhome.de/download_ger.htm

⁵ <https://mat.boum.org/>

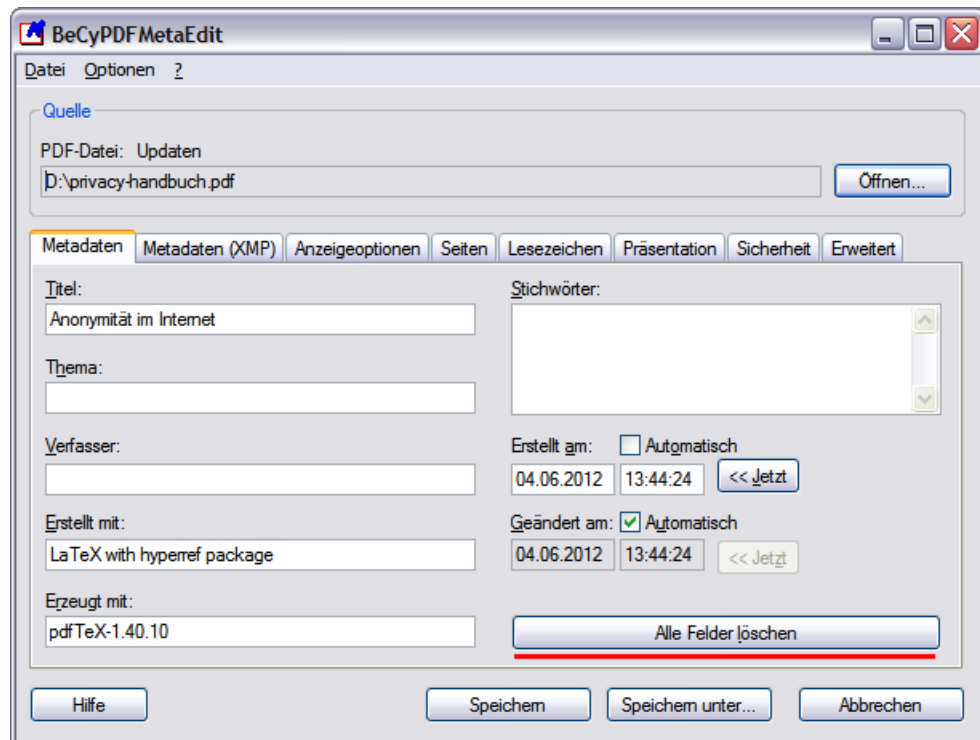


Abbildung 13.2: Metadaten in PDF-Dokumenten löschen

Linux einfach einsetzbar und kann folgende Datentypen säubern: PNG und JPEG Bilder, PDF-Dokumente, OpenOffice und Microsoft Office Dokumente, MP3 und FLAC Dateien. Das Tool ist in Python geschrieben und braucht einige Bibliotheken. Unter Debian, Ubuntu und Linux Mint installiert man zuerst die nötigen Bibliotheken mit:

```
> sudo aptitude install libimage-exiftool-perl python-hachoir-core
python-hachoir-parser python-poppler python-cairo python-mutagen
python-pdfrw
```

Danach entpackt man das herunter geladene 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 -b /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. Die gesäuberten Dateien findet im gleichen Verzeichnis, wie die Originale mit der Erweiterung *.cleaned*. im Namen.

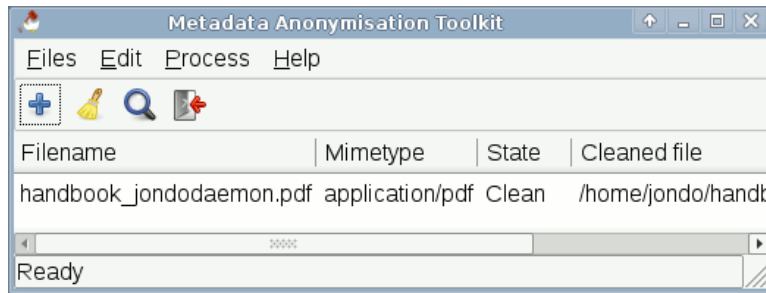


Abbildung 13.3: Dateien säubern mit MAT

Kapitel 14

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 Online¹, wieder einmal viel heiße Luft.)

Wie funktioniert diese Technik, über die Zeit Online bereits 1996 berichtete und können Nicht-Terroristen das auch nutzen?

Ein Beispiel

Statt Bits und Bytes werden in diesem Beispiel Buchstaben genutzt, um das Prinzip der Steganografie zu erläutern. Nehmen wir mal an, Terrorist A möchte an Terrorist B die folgende kurze Botschaft senden:

Morgen!

Statt die Nachricht zu verschlüsseln, was auffällig sein könnte, versteckt er sie in dem folgenden, harmlos aussehenden Satz:

Mein olles radio geht einfach nicht!

Wenn der Empfänger weiss, dass die eigentliche Botschaft in den Anfangsbuchstaben der Wörter kodiert ist, wäre es ganz gut, aber nicht optimal.

Ein Beobachter könnte auf den Gedanken kommen: *“Was - wieso Radio? Der zahlt doch keine GEZ!”* Er wird aufmerksam und mit ein wenig Probieren kann

¹ <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:

I1pcmg!

und ein neuer, halbwegs sinnvoller Satz wird konstruiert und verschickt.

Das Beispiel verdeutlicht, welche Voraussetzungen für die Nutzung von Steganografie zum Austausch von Nachrichten gegeben sein müssen:

1. Sender und Empfänger müssen sich darüber verständigt haben, wie die Nutzdaten versteckt und verschlüsselt werden.
2. Die Nutzdaten sollte man grundsätzlich verschlüsseln, da nicht ausgeschlossen ist, dass ein Beobachter aufmerksam wird.
3. Die Cover-Datenmenge muss viel größer als die Datenmenge der Nutzdaten sein.

Steganografie-Tools

Kleine Softwaretools vereinfachen die Nutzung der Steganografie. Derartige Tools wurden schon im vergangenen Jahrhundert entwickelt und sind keineswegs neu, wie Scotland Yard behauptete. Es steht eine umfangreiche Palette zur Verfügung. *steghide*² und *outguess*³ sind auf dem Stand der Technik, andere meist nicht mehr gepflegt und veraltet.

Diese Tools verstecken Text oder kleine Dateien in Bildern bzw. Audiodateien. Diese Trägermedien sind besonders geeignet, da kleine Modifikationen an Farbwerten oder Tönen nicht auffallen und auch Redundanzen genutzt werden können.

Die Nutzdaten werden häufig mit starken kryptografischen Algorithmen verschlüsselt. Auch darum braucht der Anwender sich nicht selbst kümmern, die Eingabe einer Passphrase reicht, um dieses Feature zu aktivieren.

Besitz und Nutzung dieser Tools ist nicht verboten. Sie dienen der digitalen Selbstverteidigung (sind ungeeignet, um fremde Rechnersysteme anzugreifen).

Wasserzeichen

Man kann Tools für Steganografie auch nutzen, um unsichtbare Wasserzeichen an Bildern oder Audiodateien anzubringen (Copyright-Hinweise u.ä.)

² <http://steghide.sourceforge.net/>

³ <http://niels.xtdnet.nl/>

14.1 steghide

Steghide ist ein Klassiker unter den Tools für Steganografie. 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*.

steghide ist ein Kommandozeilen-Tool

Um die Datei *geheim.txt* zu verschlüsseln und in dem Foto *bild.jpg* zu verstecken, ruft man es mit folgenden Parametern auf (mit *-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 *-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
```

Die Passphrase kann mit dem Parameter *-p* "Das geheime Passwort" auch auf der Kommandozeile übergeben werden. Das erleichtert die Nutzung in Scripten.

14.2 stegdetect

Auch die Gegenseite ist nicht wehrlos. Manipulationen von steghide, F5, outguess, jphide usw. können z.B. mit *stegdetect*⁴ 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.

⁴ <http://www.outguess.org/download.php>

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.

Kapitel 15

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.

Abhörschnittstellen

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 Abhörschnittstellen zwingend vorschreiben. In den USA war es der *CALEA Act* ¹ von 1994. In Deutschland wurde 1995 auf Initiative des Verfassungsschutz die *Fernmeldeverkehr-Überwachungsverordnung* (FÜV) ² beschlossen, die 2002 durch die *Telekommunikations-Überwachungsverordnung* (TKÜV) ³ ersetzt wurde.

2005 wurde der CALEA Act durch das höchste US-Gericht so interpretiert, dass er auch für alle VoIP-Anbieter gilt, die Verbindungen in Telefonnetze weiterleiten können. Skype zierte sich anfangs, die geforderten Abhörschnittstellen zu implementieren. Mit der Übernahme von Skype durch Ebay im Nov. 2005 wurde die Diskussion beendet. Heute bietet Skype Abhörschnittstellen in allen westeuropäischen Ländern und zunehmend auch in anderen Ländern wie Indien. In Deutschland sind Abhörprotokolle aus Skype Gesprächen

¹ <https://secure.wikimedia.org/wikipedia/en/wiki/Calea>

² <http://www.online-recht.de/vorges.html?FUEV>

³ <https://de.wikipedia.org/wiki/Telekommunikations-%C3%9Cberwachungsverordnung>

alltägliches Beweismaterial ⁴.

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.

15.1 Open Secure Telephony Network (OSTN)

Das Open Secure Telephony Network (OSTN) ⁵ 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 ⁶ 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-CD schützen. Die JonDo-Live-CD enthält z.B. den VoIP-Client Jitsi.

⁴ <http://www.lawblog.de/index.php/archives/2010/08/17/skype-staat-hort-mit>

⁵ <https://guardianproject.info/wiki/OSTN>

⁶ <https://tools.ietf.org/html/draft-zimmermann-avt-zrtp-22>

OSTN-Provider

Um diese sichere Variante der Internettelefonie zu nutzen, benötigt man einen Account bei einem OSTN-kompatiblen Provider. Derzeit gibt es 3 Anbieter: Tanstagi⁷, PillowTalk⁸ und Ostel.me⁹, wobei Ostel.me der Test- und Entwicklungsserver des Projektes ist. Die Serversoftware OSTel ist Open Source, man kann auch seinen eigenen Server betreiben. Weitere Anbieter werden folgen.

Am einfachsten kann man einen anonymen Account bei *PillowTalk* erstellen. Es werden keine Daten erfragt (auch keine E-Mail Adresse). Der Server speichert keine Daten. Wenn er einmal down geht sind sämtliche Accounts weg und müssen neu erstellt werden.

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*¹⁰, einen Java-basierter VoIP- und IM-Client für viele Betriebssysteme.
- Für Linux (Ubuntu, SUSE und Redhat) gibt es das SFLphone¹¹.
- Für Android-Smartphones ist *CSipSimple*¹² am besten geeignet, das ebenfalls vom Guardian Project entwickelt wird. (OSTN-Support in den Nightly Builds der Beta Version.)
- Apple iPhone Nutzer können Groundwire¹³ für \$9,99 im App Store kaufen.

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 ein Java Runtime Environment (JRE).

- Für Windows findet man ein Installationsprogramm auf www.java.com.

⁷ <https://tanstagi.net>

⁸ <https://intimi.ca:4242>

⁹ <https://ostel.me>

¹⁰ <https://jitsi.org>

¹¹ <http://sflphone.org>

¹² <http://nightlies.csipsimple.com>

¹³ <https://itunes.apple.com/us/app/groundwire-business-caliber/id378503081?mt=8>



Abbildung 15.1: Account Daten eintragen

- Unter Linux installiert man das Paket *default-jre* mit dem bevorzugten Paketmanager der Distribution.

Hinweis: zusammen mit der JRE wird auch ein Java-Plugin für die Browser installiert. Dieses Plugin ist ein Sicherheitsrisiko! Es ist nach der Installation von Java im Browser zu deaktivieren. Im Firefox kann man das in der Plugin-Verwaltung unter *Extras - Add-ons* erledigen.

Anschließend installiert man Jitsi, indem man das zum Betriebssystem passende Paket von der Downloadseite 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 15.1 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

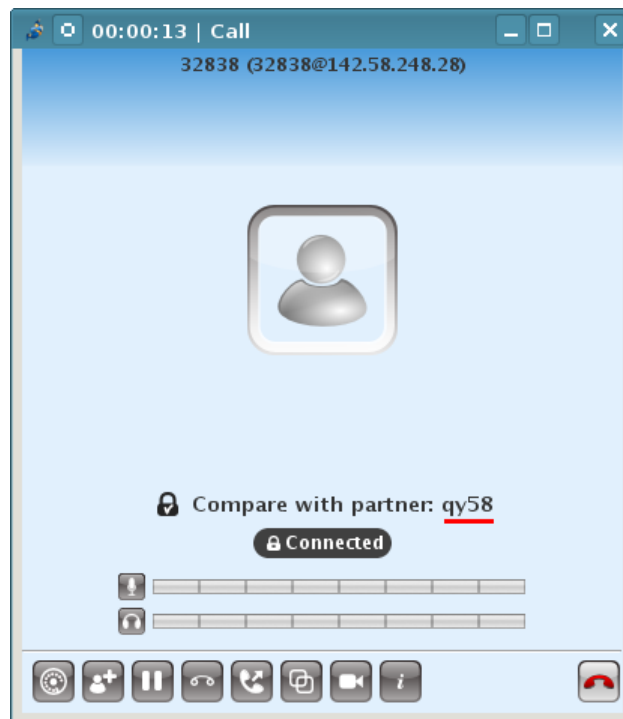


Abbildung 15.2: SAS Authentication

der Festplatte zu vermeiden.

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 16

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.

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 umher tragen 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.

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:

- n 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 Freigabe, 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 heraus geben muss.

Staatliches Tracking von Handys

Auch Strafverfolgungsbehörden und Geheimdienste nutzen die neuen Möglichkeiten:

- Das FBI nutzt das Tracking von Smartphones seit Jahren zur *Durchleuchtung der Gesellschaft*, wie Danger Room berichtete. Muslimisch Communities werden systematisch analysiert, ohne dass die Personen im Verdacht stehen, eine Straftat begangen zu haben.¹

¹ <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, sondern weiterhin für die Generierung von Verdachtsmomenten genutzt ².
- 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 ³.
- 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.

16.0.1 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.

Bei Smartphones kann man nicht davon ausgehen, dass der Nutzer volle Kontrolle über die installierte Software hat. 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, sondern ein Teil der *Market App*.

Auch das iPhone von Apple, Windows Phone 7 und Amazons Kindle haben einen Kill Switch.

Jede Crypto-Anwendung aus den Markets muss also als potentiell kompromittiert gelten. Sie kann genau dann versagen, wenn man den Schutz am nötigsten braucht.

² <http://www.heise.de/tp/artikel/34/34973/1.html>

³ <http://www.heise.de/tp/artikel/35/35043/1.html>

Einige Crypto-Apps

Wer trotzdem ein besseres Gefühl im Bauch hat, wenn die Kommunikation verschlüsselt wird, kann folgende Apps nutzen:

- **WhisperSystems** bietet Apps für verschlüsselte Telefonie, SMS und Datenverschlüsselung für Android ⁴.
- **CSipSimple** ist VoIP Softphone für das iPhone mit ZRTP-Verschlüsselung der Gespräche (derzeit nur in der Entwicklerversion verfügbar).

16.0.2 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.

Apps im Android Market

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.
- **Orweb** ist ein privacy-freundlicher Browser für Android, der von beiden Projekten für anonymes Surfen empfohlen wird. Im Abschnitt Spurenarm Surfen ist beschrieben, warum das Verschleiern der IP-Adresse für anonymes Surfen nicht ausreicht.

Etwas mehr Sicherheit

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 ⁵.

⁴ <http://www.whispersys.com/>

⁵ <https://guardianproject.info/code/lildebi/>

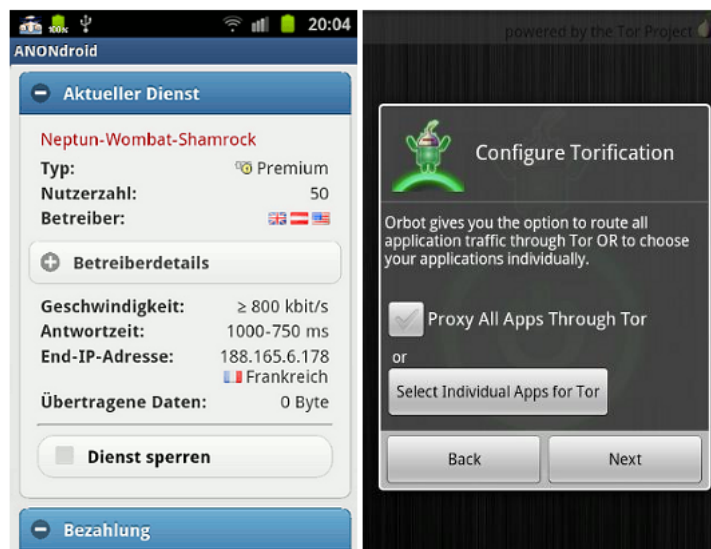


Abbildung 16.1: ANONdroid und Orbot

Da keine grafische Oberfläche zur Verfügung steht, ist man 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 ⁶.

⁶ https://anonymous-proxy-servers.net/wiki/index.php/JonDoDaemon_für_Debian

Kapitel 17

Umgehung von Zensur

Die Zensur Neusprech: Access-Blocking) sollte in Deutschland unter dem Deckmantel des Kampfes gegen Kinderpornografie im Internet eingeführt werden. Inzwischen hat die Zivilgesellschaft diesen Versuch gestoppt. Trotzdem wird dieser Abschnitt Bestandteil des Privacy-Handbuches bleiben, als Beispiel für eine Kampagne und erfolgreichen Widerstand der Bürger.

Besonders verknüpft mit dem Versuch der Einführung einer Internetzensur sind Frau von der Leyen als Familienministerin, Herr Schäuble als Innenminister und Herr v. Guttenberg. Frau von der Leyen wurde dafür mit dem Big Brother geehrt. Sie wurde nicht müde zu behaupten, es gäbe einen Millionen Euro schweren Massenmarkt, der durch Sperren von Websites ausgetrocknet werden kann. Ihre Aussagen wurden überprüft und für falsch befunden.

Die Ermittler vom LKA München sind der Meinung, dass bei der Verbreitung von Kinderpornographie Geld kaum eine Rolle spielt. Es gibt selten organisierte Strukturen:

Die überwältigende Mehrzahl der Feststellungen, die wir machen, sind kostenlose Tauschringe, oder Ringe, bei denen man gegen ein relativ geringes Entgelt Mitglied wird, wo also nicht das kommerzielle Gewinnstreben im Vordergrund steht. Von einer Kinderpornoindustrie zu sprechen, wäre insofern für die Masse der Feststellungen nicht richtig. (Quelle: Süddeutsche Zeitung)

Ermittler des LKA Niedersachsen bestätigten gegenüber Journalisten der Zeitschrift ct die Ansicht, dass es keinen Massenmarkt von Websites im Internet gibt. Die sogenannte "harte Ware" wird nach ihrer Einschätzung überwiegend per Post versendet. Das Internet (vor allem E-Mail) wird nur genutzt, um Kontakte anzubahnen.

Auch die *European Financial Coalition* kommt zu dem Schluss, dass es keinen Massenmarkt für Kinderpornografie gibt. In den Jahren 2009/2010 ist die Zahl der Angebote im Netz außerdem deutlich gesunken.

Kann es sein, dass diese Erkenntnisse in der Regierung nicht bekannt sind?

In der Antwort auf eine parlamentarische Anfrage beweist die Regierung jedenfalls ein hohes Maß an Unkenntnis zu dem Thema:

Frage: In welchen Ländern steht Kinderpornographie bislang nicht unter Strafe?

Antwort: *Dazu liegen der Bundesregierung keine gesicherten Kenntnisse im Sinne rechtsvergleichender Studien vor.*

Frage: Über welche wissenschaftlichen Erkenntnisse verfügt die Bundesregierung im Zusammenhang mit der Verbreitung von Kinderpornographie.

Antwort: *Die Bundesregierung verfügt über keine eigenen wissenschaftlichen Erkenntnisse...*

Frage: Auf welche Datengrundlage stützt sich die Bundesregierung bei der Einschätzung des kommerziellen Marktes für Kinderpornographie in Deutschland?

Antwort: *Die Bundesregierung verfügt über keine detaillierte Einschätzung des kommerziellen Marktes für Kinderpornographie...*

Und basierend auf diesem Nicht-Wissen wird....

Die erste Stufe

Am 17.04.09 unterzeichneten die fünf Provider Deutsche Telekom, Vodafone/Arcor, Hansenet/Alice, Telefonica/O2 und Kabel Deutschland freiwillig einen geheimen Vertrag mit dem BKA. Dieser Vertrag verpflichtet die Provider, eine Liste von Websites (bzw. Domains) umgehend zu sperren, die das BKA ohne rechtstaatliche Kontrolle zusammenstellt. Statt der gesperrten Website soll ein Stopp-Schild angezeigt werden. Soweit bekannt geworden ist, soll die Sperrung soll durch eine Kompromittierung des DNS-Systems umgesetzt werden.

Die zweite Stufe

Am 18.06.09 hat der Deutsche Bundestag ein *Gesetz zur Bekämpfung der Kinderpornografie in Kommunikationsnetzen* verabschiedet. Das Gesetz ist technikkoffen formuliert. Neben den (ungeeigneten) DNS-Sperren sollen auch tiefere Eingriffe in die Kommunikation zulässig und angemessen sein. Diskutiert werden IP-Adress-Sperren, kombiniert mit einer genauen Analyse des Datenverkehrs.

Das Gesetz zwingt Provider mit mehr als 10.000 Kunden dazu, die im Geheimen vom BKA erstellten Sperrlisten umzusetzen und bei Aufruf einer entsprechenden Website eine Stopp-Seite anzeigen. Die Sperrliste soll durch ein zahlloses Experten-Gemium stichprobenartig mindestens vierteljährlich überprüft werden. Diese Experten soll der Bundesdatenschutzbeauftragtem

berufen.

Eine Begrenzung der Sperrmaßnahmen auf kinderpornografische Angebote außerhalb der Möglichkeit der Strafverfolgung ist nicht vorgesehen. Es wurde bereits im Vorfeld die Ausweitung der Internetsperren von verschiedenen Politikern gefordert. Die Aussage von Herrn Bosbach (CDU) ist eigentlich an Eindeutigkeit nicht zu überbieten:

*Ich halte es für richtig, sich **erstmal** nur mit dem Thema Kinderpornografie zu befassen, damit die öffentliche Debatte nicht in eine Schieflage gerät.*

Eine konsequente Umsetzung des Subsidiaritätsprinzips *Löschen vor Sperren* ist im Gesetz ebenfalls nicht vorgesehen. Es soll der Einschätzung des BKA überlassen bleiben, ob zu erwarten ist, dass der Provider ein indexiertes Angebot in angemessener Zeit vom Netz nimmt oder eine Internet-Sperre eingerichtet wird. Es besteht keine Verpflichtung für das BKA, die Hosts der beanstandeten Websites zu kontaktieren und um Löschung der Angebote zu bitten.

Ein Schritt zurück

Im Oktober 2009 hat die Regierungskoalition von CDU und FDP beschlossen, das Gesetz erst einmal nicht umzusetzen. Das BKA soll für ein Jahr keine Sperrlisten an die Provider liefern, sondern die Webseiten nach Möglichkeit löschen lassen. Nach Ablauf der Evaluierung soll das Ergebnis geprüft und über die Einführung von Sperren nochmals beraten werden.

Mit einem "Anwendungserlass" für das BKA hat die Bundesregierung ein vom Deutschen Bundestag beschlossenes Gesetz nicht umgesetzt sondern erst einmal aufgeschoben. Die Ansammlung von Adressen und Mitgliedern der Hochfinanz in unserer Regierung glaubt also, über dem Parlament zu stehen. Formal sicher eine seltsame Auffassung von Demokratie.

Im April 2011 wurde das Zugangserschwerernsgesetz endgültig beerdigt. Auch die Befürworter der Zensur mussten einsehen, dass ein Löschen von Bildmaterial über dokumentiertem Missbrauch durch internationale Zusammenarbeit möglich ist.

Umweg über die EU

Nachdem die Zensurmaßnahmen in Deutschland nicht durchsetzbar waren, begann eine Kampagne der EU-Kommission. Alle Mitgliedsländer sollten zum Aufbau einer Sperrinfrastruktur gegen Kinderpornografie verpflichtet werden. Besonders hervorgerufen als Befürworterin einer solchen Regelung hat sich Cecilia Malström, die EU-Kommissarin für innere Angelegenheiten.

Das Vorgehen erinnert stark an die Vorratsdatenspeicherung. Der deutsche Bundestag lehnte 2001 die VDS als nicht verfassungskonform ab und kurze Zeit später kommt eine EU-Richtlinie, die alle Mitgliedsländer zur Umsetzung der VDS verpflichten sollte. Das gleiche Spiel beim Zugangserschwerernsgesetz?



Abbildung 17.1: Quelle: <http://i227.photobucket.com/albums/dd41/Scoti17/Malmstrm.jpg>

ACTA, Urheberrecht und Glücksspiel

Parallel zu dieser Entscheidung werden auf internationaler Ebene Abkommen vorbereitet, welche die Einführung einer Zensurinfrastruktur für Deutschland verbindlich vorschreiben sollen. In Dokumente zu den ACTA-Geheimverhandlungen wird eine Zensurinfrastruktur zur Verhinderung von Urheberrechtsverletzungen gefordert, die internationale Konferenz zum Schutz der Kinder fordert eine Zensurinfrastruktur und auch die Absicherung des staatlichen Glücksspiel Monopols soll als Vorwand für Sperren im Netz dienen.

Wie bei der Einführung der Vorratsdatenspeicherung verfolgen die Verfechter des Überwachungsstaates ihre Ziele hartnäckig und auf mehreren Wegen.

Die Zensur erfolgt auf vielen Ebenen

Die Einführung der Zensur umfasst nicht nur effektive technische Sperrmaßnahmen. Sie wird auch durch juristische Schritte begleitet. Einige Beispiele:

- Das Forum *Politik global* sollte auf Betreiben des LKA Berlin im Mai 2009 wegen Volksverhetzung geschlossen werden. Das AG Tiergarten in Berlin hat der Klage stattgegeben. Das Urteil des AG Tiergarten ist uns nicht im Wortlaut bekannt. Auf der Website haben wir aber keine Nazi-Propaganda gefunden sondern Israel- und NATO-kritische Themen sowie Hinweise auf Missstände in Deutschland und International.

Die Domain wurde gelöscht. Da helfen auch keine unzensierten DNS-Server. Die Webseite war für einige Zeit weiterhin noch unter der IP-Adresse erreichbar, da der Server nicht in Deutschland stand. Eine neue Domain wurde registriert, ist derzeit aber auch nicht mehr erreichbar.

- Am 21. Mai 2009 veröffentlichte Spiegel-Online einen Artikel über Bestechung von Politikern durch den Telekom Konzern. Dr. Klemens Joos

sowie die EUTOP International GmbH wurden in dem Artikel genannt und schickten ihre Anwälte los, um den Artikel zu entfernen. Sie sahen ihre Rechte in erheblicher Weise beeinträchtigt. (Der Artikel stand bei Wikileaks weiterhin zum Download zur Verfügung.)

- Wikipedia ist immer wieder das Ziel von Zensurbemühungen. Unliebsame Artikel werden unterdrückt oder modifiziert. *Man bemühe sich um Neutralität*, sagte Gründer J. Wales bei der letzten Wikipedia-Konferenz. Aber das ist scheinbar nicht leicht umsetzbar. In der israelischen Wikipedia fehlt jegliche kritische Bemerkung an der Politik Israels, wie der Blogger Richard Silverstein kritisch feststellte. Pakistan hat anlässlich der 2011 Balochistan International Conference Informationen über Occupation in der englischen Wikipedia entfernen lassen und vieles andere mehr.
- Das Suchmaschinen ihre Links zensieren ist seit längerem bekannt. Die bei Wikileaks aufgetauchte Sperrliste des ehemaligen Suchdienstes Lycos oder die Sperrlisten von Baidu sind interessant.

17.1 Strafverfolgung von Kinderpornografie

Während die Einführung von Internet-Sperren für die derzeitige Regierung „ein in vielerlei Hinsicht wichtiges Thema ist“, (v. Guttenberg), scheint die Verfolgung der Anbieter eher niedrige Priorität zu genießen.

Wo stehen die Server?

Im scusiblog <https://scusiblog.org> findet man Analysen zu verschiedenen europäischen Filterlisten. In der Länderwertung belegt Deutschland stets einen beachtlichen vorderen Platz bei der Veröffentlichung von Material mit dokumentiertem Kindesmissbrauch. Eine Zusammenfassung der Sperrlisten der Schweiz, Dänemark, Finnland und Schweden (2008) lieferte folgende Zahlen:

Land	Anzahl der Websites
USA	3947
Australien	423
Niederlande	333
Deutschland	321
Süd-Korea	95
Kanada	88

Da diese in Deutschland gehosteten illegalen Angebote bei befreundeten Polizeien bekannt sind, stellt sich die Frage, warum sie bisher nicht entfernt und die Betreiber zur Rechenschaft gezogen wurden. Nahezu alle Provider unterstützen Maßnahmen gegen Kinderpornos. Es genügt ein Anruf, um das Angebot innerhalb weniger Stunden zu schließen. Auch die bei regierungskritischen Themen als *bullet proof* geltenden Hosters wie z.B. MediaOn und noblogs.org kennen bei KiPo kein Pardon.

Wenn das BKA kinderpornografische Websites kennt, die auf eine zukünftige Sperrliste gesetzt werden sollen, warum werden die Seiten nicht

abgeschaltet und die Betreiber zur Verantwortung gezogen? Eine internationale Zusammenarbeit sollte bei diesem Thema kein Problem sein.

Zwei Jahre später war ein Teil der Webangebote noch immer online. Der AK Zensur ließ ganz ohne polizeiliche Vollmacht einige der seit zwei Jahren auf der dänischen Sperrliste stehenden Webseiten innerhalb von 30min schließen. Warum hat das BKA zwei Jahre lang nichts unternommen?

Der lange Dienstweg des BKA

In einer Studie der Universität Cambridge wurde untersucht, wie lange es dauert, um strafrechtlich relevante Websites zu schließen. Phishing-Websites werden innerhalb von 4 Stunden geschlossen. Bei Websites mit dokumentiertem Kindesmissbrauch dauert es im Mittel 30 Tage!

Frau Krogmann (CDU) antwortete auf eine Frage bei abgeordnetenwatch.de, dass das BKA kinderpornografische Websites nicht schneller schließen kann, weil **der Dienstweg** eingehalten werden muss.

Noch mal ganz langsam:

1. Weil das BKA den Dienstweg einhalten muss, können Websites mit dokumentiertem Kindesmissbrauch nicht kurzfristig geschlossen werden?
2. Das mit dem Gesetz zur Einführung von Internet-Sperren rechtsstaatliche Prinzipien verletzt und Grundrechte eingeschränkt werden sollen (Grundgesetz Artikel 5 und 10), ist nebensächlich, wenn auch nur einem Kind damit geholfen werden kann?

Das Gutachten des Wissenschaftlichen Dienstes des Bundestages (WD 3 - 3000 - 211/09) zeigt, dass das BKA auch ohne Zensur wesentlich mehr gegen dokumentierten Kindesmissbrauch tun könnte.

Wie frustrierend dieser lange Dienstweg und die mangelhafte Unterstützung der Strafverfolger sind, zeigt Oberstaatsanwalt Peter Vogt. Die Sueddeutsche Zeitung bezeichnet ihn als Pionier der Strafverfolgung von Kinderpornografie. Ab Jan. 2010 steht Herr Vogt für diese Aufgabe nicht mehr zur Verfügung. Er hat wegen unhaltbarer Zustände in den Polizeidirektionen das Handtuch geworfen.

Interessant ist, dass das BKA eine mit hohen Kosten verbundene Sperr-Infrastruktur aufbauen möchte, selbst aber nur 6,3 (!) Planstellen für die Verfolgung von dokumentiertem Missbrauch bereitstellt.

Die Internet-Sperren sind kontraproduktiv

Die geplanten Sperren von Websites mit Anzeige einer Stopp-Seite sind für die konsequente Verfolgung der Straftaten kontraproduktiv.

Mit der Anzeige der Stopp-Seite sollen die Daten des Surfers an das BKA zwecks Einleitung der Strafverfolgung übermittelt werden. Gleichzeitig wird

der Konsument kinderpornografischen Materials jedoch gewarnt und kann alle Spuren beseitigen. Ohne Nachweis der Straftat ist eine rechtsstaatliche Verurteilung jedoch nicht möglich.

17.2 Die Medien-Kampagne der Zensursula

Der Gesetzgebungsprozess wurde von einer breiten Medien-Kampagne begleitet. Die Gegner der Zensur wurden direkt und indirekt als Pädophile oder deren Helfer verunglimpft, es wurde ein Gegensatz von *„Meinungsfreiheit im Internet“* versus *„Schutz der Kinder“* konstruiert und viel mit fragwürdigem Zahlenmaterial, unwahren Behauptungen und suggestiven Umfragen argumentiert.

Das fragwürdige Zahlenmaterial für die Kampagne wurde überwiegend von Innocence in Danger geliefert. Diese Organisation unter Führung von Julia v. Weiler und Stefanie v.u.z. Gutenberg war auch wegen undurchsichtiger Geschäftsgebaren und undokumentierter Verwendung von Spendengeldern in öffentliche Kritik geraten.

In den Mainstream-Medien wurde die Argumentation der Befürworter der Zensur prominent und ohne kritische Nachfrage wiedergegeben:

Es macht mich schon sehr betroffen, wenn pauschal der Eindruck entstehen sollte, dass es Menschen gibt, die sich gegen die Sperrung von kinderpornographischen Inhalten sträuben. (Karl Theodor v.Guttenberg)

Lassen Datenschützer und Internet-Freaks sich vor den Karren der Händler und Freunde von Kinderpornografie spannen? Diese Frage muss sich nicht nur Franziska Heine stellen. (Teaser der Zeitschrift *„Emma“*)

Wir können es doch als Gesellschaft nicht hinnehmen, das - so wie es die Piratenpartei fordert- Jugendliche und Erwachsene ungehindert Zugang zu Kinder pornos im Internet haben können... (S. Raabe, SPD)

Das Motto der Gegner der Zensur im Internet lautete **Löschen statt Sperren**. Das stand auch deutlich in der von Franziska Heine initiierten Petition und wurde auf dem Piraten-Parteitag ebenfalls deutlich gesagt.

Weitere Beispiele:

Wir vermissen die Unterstützung der Internet Community, die uns sagt, wie wir dem wachsenden Problem der Kinderpornografie Herr werden können. Diese Stimmen sind bisher kaum zu hören. (v.d.Leyen)

Heinrich Wefing, der uns schon öfter aufgefallen ist, sinniert in der Zeit:

Nun könnte man die lärmende Ablehnung jeder staatlichen Regulierung vielleicht sogar als romantische Utopie belächeln, wenn die Ideologen der Freiheit gelegentlich mal selbst einen Gedanken darauf verwenden würden, wie sich der Missbrauch des Mediums eindämmen ließe.

Die Nerds vom AK Zensur haben nicht nur Hinweise gegeben, sie haben es auch vorgemacht. **Innerhalb von 12 Stunden wurden 60 kinderpornographische Internet-Angebote gelöscht** (ganz ohne polizeiliche Vollmacht). Was wird noch erwartet. Sollen wir die Dienstanweisung für das BKA formulieren? Ein Gutachten des Wissenschaftlichen Dienstes des Bundestages zeigt, dass das BKA diesem Beispiel folgen könnte.

Die bittere Wahrheit ist, dass bisher nur die Hälfte der Länder Kinderpornographie ächtet. (v.d.Leyen)

Auf der "Konferenz zum Schutz vor sexueller Gewalt gegen Kinder und Jugendliche mit Fokus auf neue Medien" behauptet v.d.Leyen:

Nur rund 160 Staaten haben überhaupt eine Gesetzgebung gegen die Vergewaltigung von Kindern, die von den Tätern aufgenommen und übers Netz verbreitet wird. 95 Nationen hätten keine solche Gesetze.

Netzpolitik.org hat sich diese Zahlen genauer angesehen. 193 Staaten haben die UN-Konvention zum Schutz der Kinder ratifiziert und in geltendes Recht umgesetzt. Artikel 34 definiert den Schutz vor sexuellem Missbrauch.

Von den 95 Nationen, die lt. v.d.Leyen keine Gesetze gegen Missbrauch Minderjähriger haben sollen, verbieten 71 Pornografie generell. Das schließt dokumentiert Missbrauch ein. Weitere befinden sich im Bürgerkrieg oder in einem verfassungsgebenden Prozess nach einem Krieg. Der Rest hat keine nennenswerte Infrastruktur, um Webserver zu betreiben.

Wer die Stopppseite zu umgehen versucht, macht sich bewusst strafbar, weil er dann aktiv nach Kinderpornografie sucht. (v.d.Leyen)

Moment mal - es war im III. Reich verboten, Feindsender zu hören. Einen vergleichbaren Paragraphen sucht man im Strafgesetzbuch vergeblich. Es steht jedem Nutzer frei, vertrauenswürdige Internet-Server zu nutzen.

17.3 Löschen statt Sperren ist funktioniert

Die Aktionen des AK-Zensur haben gezeigt, dass Löschen statt Sperren möglich ist. in einer ersten Aktion wurden innerhalb von 12 Stunden 60 kinderpornografische Internet-Angebote gelöscht, ohne polizeiliche Vollmachten. In einer zweiten Aktion wurde die dänische Sperrliste analysiert. Seit 2 Jahren gesperrte Webseiten konnten innerhalb von 30min gelöscht werden. Das Beispiel zeigt, dass eine Sperrliste auch oft als Alibi dient und eine weitere Strafverfolgung nicht betrieben wird.

Der eco Verband konnte im Jahr 2010 von den gemeldeten Webseiten 99,4% entfernen. Es wurden 256 Websites mit dokumentiertem Missbrauch gemeldet. Davon wurden 448 im Wirkungsbereich von INHOPE umgehend gelöscht. 204 wurden auf ausländischen Server nach kurzem Hinweis vom Provider gelöscht. Bei zwei Meldungen handelte es sich nicht um strafbares Material.

17.4 Simple Tricks

Die besten Möglichkeiten zur Umgehung von Zensur sind *Anonymisierungsdienste* mit Anti-Censorship Funktion wie JonDonym oder Tor. Stehen diese Dienste nicht zur Verfügung, kann man es auch mit den Simple Tricks versuchen. Die *Simple Tricks* wurden bereits an der "Great Firewall" in China erprobt und sind teilweise recht erfolgreich. Das einfache Prinzip ist im Bild 17.2 dargestellt.

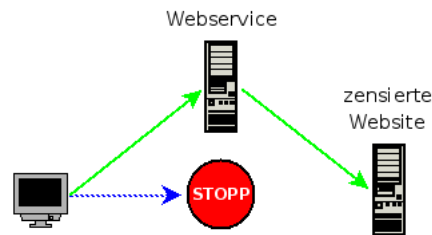


Abbildung 17.2: Prinzip der Simple Tricks

Wenn man auf eine Website nicht zugreifen kann (oder man befürchtet, nicht zugreifen zu können) kann man einen Webdienst im Ausland nutzen. Der Webdienst unterliegt anderen Zensurbedingungen und kann häufig auf die gewünschte Seite zugreifen und über den kleinen Umweg unzensiert liefern.

Hinweis: Es ist ratsam, Web-Services zu nutzen, die eine SSL-Verschlüsselung des Datenverkehrs anbieten. Wer Anonymisierungsdienst wie Tor oder JonDonym nutzen kann, sollte diese Möglichkeit bevorzugen.

Einige Vorschläge für Webdienste:

1. **RSS-Aggregatoren:** sind geeignet, um regelmäßig eine Website zu lesen, die RSS-Feeds anbietet, bspw. Blogs. Man kann sich selbst seine Feeds auf einem Web-Aggregator wie www.bloglines.com zusammenstellen oder nutzt fertig, themenspezifische Aggregatoren wie z.B. den Palestine Blog Aggregator über den Gaza-Krieg.
2. **SSL-Web-Proxys** bieten ein Formular für die Eingabe einer URL. Die Website wird von dem Proxy geholt und an den Surfer geliefert. Dabei werden alle Links der Webseite vom Proxy umgeschrieben, so dass bei einem Klick die folgende Website ebenfalls über den Proxy geholt wird. Flüssiges Surfen ist möglich. Um die Filterung des Datenverkehr nach gesperrten Wörtern zu verhindern, sollte man SSL-verschlüsselte Web-Proxys nutzen. Eine Liste von Web-Proxys mit SSL-Verschlüsselung findet man bei Proxy.org oder mamproxy.com oder www.privax.us/.

Web-Proxies sind keine Anonymisierungsdienste! Die Admins könnten den gesamten Traffic mitlesen, auch bei SSL-verschlüsselten Websites. Sie sind ungeeignet für Webangebote, die ein Login mit Passwort erfordern. Viele Web-Proxys speichern die Daten und geben sie auch an Behörden weiter, wie der Sahara-Palin-Hack zeigte. Außerdem können Webmaster die meisten Web-Proxys austricksen, um Nutzer zu deanonymisieren.

3. **Übersetzungsdienste:** Man fordert bei einem Web-Translator die Übersetzung einer Website von einer willkürlichen Sprache (z.B. koreanisch) in die Originalsprache des Dokumentes an. Der Web-Translator ändert praktisch nichts. Man kann <http://babelfish.yahoo.com> oder <http://translate.google.com> nutzen.
4. **Low-Bandwidth-Filter:** bereiten Websites für Internetzugänge mit geringer Bandbreite auf. Sie entfernen Werbung, reduzieren die Auflösung von Bildern usw. und senden die bearbeitete Website an den Surfer. Man kann sie auch mit High-Speed-DSL nutzen. Steht ein solcher Server im Ausland, hat er häufig die Möglichkeit, die gewünschte Seite zu liefern, z.B. <http://loband.org>.
5. **Cache der Suchmaschinen:** Die großen Suchmaschinen indexieren Webseiten nicht nur, sie speichern die Seiten auch in einem Cache. Da man Google, Yahoo usw. fast immer erreichen kann: einfach auf den unscheinbaren Link cache neben dem Suchergebnis klicken.
6. **E-Mail Dienste:** sind etwas umständlicher nutzbar. Sie stellen die gewünschte Website per Mail zu. Ein Surfen über mehrere Seiten ist damit natürlich nicht möglich. Sie sind aber gut geeignet, unauffällig einen Blick auf eine gesperrte Website zu werfen. Dem E-Mail Dienst pagegetter.com kann man eine Mail mit der gewünschten URL der Website im Betreff senden und man erhält umgehend eine Antwort-Mail mit der Website. Der Dienst bietet folgende Adresse:
 - [web\(ÄT\)pagegetter.com](mailto:web@pagegetter.com) für einfache Webseiten.
 - [frames\(ÄT\)pagegetter.com](mailto:frames@pagegetter.com) für Webseiten die aus mehreren Framen bestehen.
 - [HTML\(ÄT\)pagegetter.com](mailto:HTML@pagegetter.com) liefert die Webseite ohne grafische Elemente aus.

17.5 Unzensierte DNS-Server nutzen



Am 17.04.09 unterzeichneten diese Provider einen geheimen Vertrag mit dem BKA, in welchem sie sich verpflichteten, den Zugriff auf eine vom BKA bereitgestellte Liste von Websites zu sperren. Soweit bekannt wurde, soll die Sperrung hauptsächlich durch Kompromittierung des DNS-Systems erfolgen.

Hinweis: Diese leicht zu umgehende Sperre ist im internationalen Vergleich die Ausnahme. Lediglich Australien hat einen vergleichbaren Weg gewählt. Die folgenden Hinweise zur Umgehung der Zensur durch Nutzung unzensierter DNS-Server können nicht auf andere Länder mit technisch hochgerüsteter Zensur-Infrastruktur übertragen werden.

Bevor man als Kunde dieser Provider ernsthaft über die Nutzung alternativer DNS-Server nachdenkt, sollte man die Möglichkeit eines **Provider-Wechsels** prüfen. Das hat folgende Vorteile:

1. Man unterstützt Provider, die sich gegen die Einschränkung der Grundrechte wehren, und übt Druck auf die Zensur-Provider aus.
2. Es ist auf für IT-Laien eine sichere Lösung, unzensierte DNS-Server zu nutzen, da möglicherweise Zensur-Provider den Datenverkehr auf eigene, zensierte DNS-Server umlenken, ohne dass man es als Nutzer bemerkt. So leitet Vodafone bspw. bereits seit Juli 09 im UMTS-Netz DNS-Anfragen auf die eigenen Server um. Im DFN Forschungsnetz soll die Nutzung unzensierter DNS-Server durch Sperrung des Port 53 unterbunden werden.

Die deutschen Provider Manitu (<http://www.manitu.de>) und SNAFU (<http://www.snafu.de>) lehnten die Sperren ab und werden sie auch nicht umsetzen. SNAFU bietet seinen Kunden an, via Webinterface alternative, unzensierte DNS-Server für den eigenen Account zu konfigurieren. Damit entfallen die im folgenden beschriebenen Spielereien am privaten Rechner und man hat mit Sicherheit einen unzensierten Zugang zum Web.

Was ist ein DNS-Server

1. Der Surfer gibt den Namen einer Website in der Adressleiste des Browsers ein. (z.B. <https://www.awxcnx.de>)
2. Daraufhin fragt der Browser bei einem DNS-Server nach der IP-Adresse des Webserver, der die gewünschte Seite liefern kann.
3. Der DNS-Server sendet eine Antwort, wenn er einen passenden Eintrag findet. (z.B. 62.75.219.7) oder NIXDOMAIN, wenn man sich vertippt hat.
4. Dann sendet der Browser seine Anfrage an den entsprechenden Webserver und erhält als Antwort die gewünschte Website.

Ein kompromittierter DNS-Server sendet bei Anfrage nach einer indexierten Website nicht die korrekte IP-Adresse des Webserver an den Browser, sondern eine manipulierte IP-Adresse, welche den Surfer zu einer Stop-Seite führen soll.

Die Anzeige der Stop-Seite bietet die Möglichkeit, die IP-Adresse des Surfers zusammen mit der gewünschten, aber nicht angezeigten Webseite zu loggen. Mit den Daten der Vorratsdatenspeicherung könnte diese Information personalisiert werden.

(Diese Darstellung ist sehr vereinfacht, sie soll nur das Prinzip zeigen. Praktische Versuche, das DNS-System zu manipulieren, haben meist zu komplexen Problemen geführt.)

Nicht-kompromittierte DNS-Server

Statt der kompromittierten DNS-Server der Provider kann man sehr einfach unzensierte Server nutzen. Einige DNS-Server können auch auf Port 110 (TCP-Protokoll) angefragt werden, falls einige Provider den DNS-Traffic auf Port 53 zum eigenen Server umleiten oder behindern. Wir gehen bei der Konfiguration für Windows und Linux darauf näher ein.

Die GPF betreibt einige unzensierte DNS-Server.

87.118.100.175 (DNS-Ports: 53, 110)
94.75.228.29 (DNS-Ports: 53, 110)

Die Swiss Privacy Foundation stellt folgende unzensierten DNS-Server:

62.141.58.13 (DNS-Ports: 53, 110)
87.118.104.203 (DNS-Ports: 53, 110)
87.118.109.2 (DNS-Ports: 53, 110)

Der Server awxcnx.de bietet auch unzensierten DNS:

62.75.219.7 (DNS-Ports: 53, 110)

Der FoeBud bietet einen unzensierten DNS-Server:

85.214.20.141

Und der CCC hat natürlich auch einen Unzensierten:

213.73.91.35

17.5.1 WINDOWS konfigurieren

Wir bezweifeln, dass es zur Umgehung der Zensur ausreicht, einfach einen unzensurierten DNS-Server zu nutzen. Das am 18.06.09 verabschiedete Gesetz zur Einführung der Zensur ist ausdrücklich technik-offen formuliert. Es sieht vor, dass die DSL-Provider alle nötigen Maßnahmen ergreifen, um den Zugriff auf indexierte Webseiten effektiv zu sperren. Die Nutzung unzensurierter DNS-Server kann relativ einfach unterbunden werden. Vodafone leitet im UMTS-Netz bereits alle Anfragen auf eigene DNS-Server um, die Pläne des DFN Forschungsnetzes sehen eine Sperrung von Port 53 vor.

Eine Möglichkeit bietet die Verwendung eines nicht üblichen TCP-Ports für DNS-Anfragen. Die DNS-Server der GPF können neben dem üblichen Port 53 auch auf Port 110 angefragt werden. Da WINDOWS die Konfiguration vom Standard abweichender Einstellungen nicht ermöglicht, ist etwas mehr Aufwand nötig, als die bekannten 27sec.

bind9 installieren

Der Nameserver *bind9* steht auch für WINDOWS beim ISC unter der Adresse <https://www.isc.org/download/software/current> zum Download bereit. Nach dem Entpacken des ZIP-Archives ruft man *BINDInstall.exe* als Administrator auf. Als Target-Directory für die Installation wählt man am besten *C:/bind* und nicht die Voreinstellung.

Nach der Installation sind auf der Kommandozeile noch ein paar Nacharbeiten als Administrator nötig:

```
c:
cd \bind\bin
rndc-confgen -a
mkdir c:\bind\zone
mkdir c:\bind\log
cacls c:\bind /T /E /C /G named:F
```

Im Verzeichnis *C:/bind/zone* müssen die drei Dateien angelegt werden:

1. localhost.zone

```
$TTL 86400
@ IN SOA @ root ( 1 ; serial
3H ; refresh
15M ; retry
1W ; expiry
1D ) ; minimum

IN NS @
IN A 127.0.0.1
IN AAAA ::1
```

2. localhost.rev


```
$TTL 86400
@ IN SOA localhost. root.localhost. ( 1 ; Serial
3H ; Refresh
15M ; Retry
1W ; Expire
1D ) ; Minimum

IN NS localhost.
1 IN PTR localhost.
```

3. Die Datei *db.cache* lädt man von <ftp://ftp.internic.net/domain/db.cache> und speichert sie in dem Verzeichnis *C:/bind/zone*. Diese Datei enthält die Informationen zu den DNS-Root-Servern.

Abschließend konfiguriert man in der Datei *named.conf* in der Sektion *options* die für die Weiterleitung genutzten DNS-Server als *forwarders*, welche auch auf Port 110 angefragt werden können, ein Beispiel:

```
options {
    directory "C:\bind\zone";
    allow-query { localhost; };
    max-cache-size 16M;
    cleaning-interval 60;
    listen-on { 127.0.0.1; };

    forwarders {
        87.118.100.175 port 110;
        94.75.228.29 port 110;
    };
};
```

Wenn die Konfiguration fertig ist, kann man den Dienst mit dem Befehl *net start named* auf der Kommandozeile starten oder über die Taskleiste unter *Start - Systemsteuerung - Verwaltung - Dienste* hochfahren.

Einstellungen der Internetverbindungen anpassen

In den Einstellungen der Internetverbindungen wird der lokale bind9 als DNS-Server konfiguriert. In der *Systemsteuerung* ist die Liste der Netzwerkverbindungen zu öffnen. Ein Klick mit der rechten Maustaste öffnet das Kontext-Menü, wo man den Eintrag *Eigenschaften* wählt. Der in Bild 17.3 gezeigte Dialog öffnet sich.

Hier wählt man die *TCP-Verbindung* und klickt auf *Eigenschaften*. In dem folgenden Dialog kann man eigene DNS-Server konfigurieren. In dem folgenden Dialog kann man den lokalen bind9 als DNS-Server konfigurieren, indem man als *Bevorzugten DNS-Server* die Adresse *127.0.0.1* eingibt.

17.5.2 Linux konfigurieren

Unter Linux sind nichts-standardmäßige Einstellungen leichter realisierbar. Es ist auch relativ einfach, einen lokalen DNS-Cache zu nutzen, um die

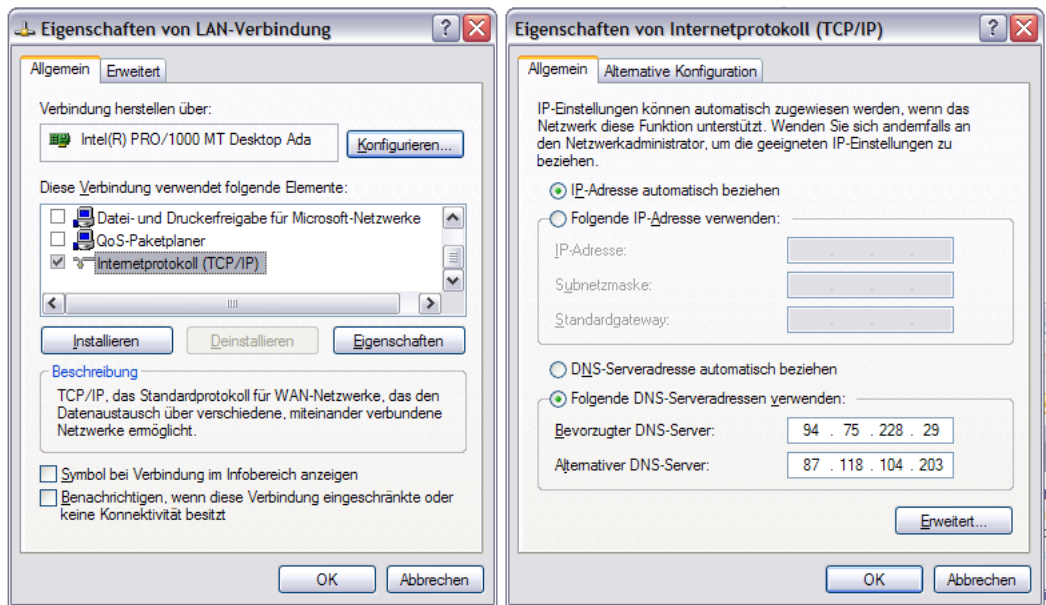


Abbildung 17.3: Konfiguration der DNS-Server (WINDOWS)

zensurfreien DNS-Server nicht übermäßig zu belasten.

pdnsd und resolvconf verwenden

Der *pdnsd* ist ein leichtgewichtiger DNS-Cache-Daemon. Er steht auf allen Linux-Distributionen zur Verfügung. Unter Debian und Ubuntu installiert man ihn zusammen mit *resolvconf*:

```
> sudo aptitude install resolvconf pdnsd
```

Bei der Installation des *pdnsd* wird man gefragt, wie die Namensauflösung erfolgen soll. Wählen Sie zuerst einmal *recursive*. Laden Sie die vorbereitete Konfigurationsdatei <https://www.awxcnx.de/download/pdnsd-gpfserver.conf> herunter und speichern Sie die Datei im Verzeichnis */usr/share/pdnsd*.

Anschließend in der Datei */etc/default/pdnsd* den *AUTO_MODE* anpassen:

```
START_DAEMON=yes
AUTO_MODE=gpfserver
OPTIONS=
```

Den Eigentümer der Config-Datei auf *root* setzen und den Daemon neu starten:

```
sudo chown root:root /usr/share/pdnsd/pdnsd-gpfserver.conf
sudo invoke-rc.d pdnsd restart
```

Der DNS-Traffic geht via TCP-Protokoll auf Port 110 zu den unzensierten DNS-Servern. Es ist schwer zu erkennen, dass es sich DNS-Traffic handelt und eine Umleitung auf DNS-Server der Provider ist wenig wahrscheinlich. Zur Sicherheit gelegentlich testen.

bind9 und resolvconf verwenden

Die Pakete *bind9* und *resolvconf* sind in allen Distributionen fertig konfiguriert vorhanden und bieten einen vollständigen DNS-Nameserver. Nach der Installation mit der Paketverwaltung läuft der Nameserver und ist unter der Adresse 127.0.0.1 erreichbar. Die Tools aus dem Paket *resolvconf* sorgen für die automatische Umkonfiguration, wenn *bind9* gestartet und gestoppt wird. Für Debian und Ubuntu können die Pakete mit *aptitude* installiert werden:

```
> sudo aptitude install resolvconf bind9
```

Die unzensierten DNS-Server sind in der Datei */etc/bind/named.conf.options* einzutragen. Die Datei enthält bereits ein Muster. Dabei kann optional auch ein nicht üblicher Port angegeben werden:

```
forwarders {
    94.75.228.29 port 110;
    62.75.219.7  port 110;
};
listen-on { 127.0.0.1; };
```

(Standardmäßig lauscht der Daemon an allen Schnittstellen, auch an externen. Die Option *listen-on* reduziert das auf den lokalen Rechner.)

Wer etwas ratlos ist, mit welchem Editor man eine Konfigurationsdatei anpasst, könnte *"kdesu kwrite /etc/bind/named.conf.options"* oder *"gksu gedit /etc/bind/named.conf.options"* probieren.

Nach der Anpassung der Konfiguration ist *bind9* mitzuteilen, dass er die Konfigurationsdateien neu laden soll:

```
> sudo invoke-rc.d bind9 reload
```

17.5.3 DNS-Server testen

Wir haben uns Gedanken gemacht, wie man möglichst einfach feststellen kann, ob man bei der Konfiguration der DNS-Server alles richtig gemacht hat. Möglicherweise hat man zwar alles richtig gemacht, aber der DSL-Provider leitet den DNS-Traffic auf Port 53 zu den eigenen Servern um, wie es z.B. Vodafone im UMTS-Netz macht. Der einfache Nutzer wird diese Umleitung in der Regel nicht bemerken.

Die DNS-Server der German Privacy Foundation und der Swiss Privacy Foundation können die Test-Adresse welcome.gpf auflösen und sind auf Port 53 und Port 110 erreichbar:

```
87.118.100.175
62.141.58.13
62.75.219.7
94.75.228.29
87.118.104.203
87.118.109.2
```

Hat man zwei dieser Server als DNS-Server ausgewählt, so kann man recht einfach testen, ob auch wirklich diese Server genutzt werden. Einfach im Browser die Adresse <http://welcome.gpf> aufrufen. Wenn man unsere Welcome-Seite sieht, ist alles Ok.

Congratulation

You are using a censorchip free DNS server!

Auf der Kommandozeile kann man *nslookup* nutzen. Die IP-Adresse in der Antwort muss 62.75.217.76 sein.

```
> nslookup welcome.gpf
```

```
Non-authoritative answer:
```

```
Name:    welcome.gpf
```

```
Address: 62.75.217.76
```

Sollte im Webbrowser nicht unsere Welcome-Seite angezeigt werden oder *nslookup* eine andere IP-Adresse liefern, so wurde keiner der oben genannten DNS-Server genutzt. Es ist die Konfiguration zu prüfen oder hmmm.

Kapitel 18

Lizenz und Spenden

Das erste Kapitel *Scroogled* wurde vom Autor Cory Doctorow und dem Übersetzer Christian Wöhrle unter Creative Commons für kostenfreie Nutzung freigegeben. Alle anderen Kapitel sind Public Domain.

18.1 Spenden

Das Privacy-Handbuch in der vorliegenden Form ist das Ergebnis mehrjähriger Freizeitarbeit. Wer diese Arbeit honorieren möchte, kann mir gern eine kleine Gratifikation senden.

Bitcoin nehmen ich gern. Wenn ihr ein paar Bitcoins übrig habt, könnt ihr sie als Spende an folgende Adresse senden:

1MAQ6KDTxwYaQo5gytHcrySpi1LiPYv8h

Liberty Reserve kann als Bezahl Dienstleister genutzt werden. Mein Account bei Liberty Reserve ist:

U4462834

PayPal.com kann auf Wunsch eines Lesers auch genutzt werden. Man kann einen kleinen Betrag an folgende Adresse senden:

danke[at]awxcnx.de

Vielen Dank.