GERMAN PRIVACY FOUNDATION e.V.

Privacy-Handbuch

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

Gedruckt mit Unterstützung des
bündnis für politik- und meinungsfreiheit

bpm
bündnis für politik- und meinungsfreiheit

Privacy-Handbuch

German Privacy Foundation

27. April 2011

bündnis für politik- und meinungsfreiheit

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

Privacy-Handbuch

Erste Auflage: 50 Stück, April 2010
Aktuelle Version: https://www.awxcnx.de/handbuch.htm

Redaktion:
German Privacy Foundation
https://www.privacyfoundation.de/

Herausgeber:
bündnis für politik- und meinungsfreiheit c/o AStA der FH Frankfurt
Kleiststrasse 5
60318 Frankfurt/Main
Telefon: +49 177 4127987
E-Mail: pm-buero@studis.de
Web: http://www.pm-buendnis.de

Inhaltsverzeichnis

1 Vorwort

Parallel zum rasanten Anstieg der Nutzung des Internets sind die Möglichkeiten zur automatischen Überwachung der Nutzer*innen gestiegen. Private Unternehmen, wie Google und Facebook, und staatliche Behörden versuchen angestrengt Informationen über möglichst viele Menschen zu sammeln und auszuwerten.

Gegen diese Angriffe auf den Datenschutz wurden aber auch viele Techniken entwickelt. So ist es heute prinzipiell leicht möglich, seine Daten, seine E-Mails und andere Kommunikationswege zu verschlüsseln, fast ohne Spuren im Internet zu Surfen und den Datensammler*innen so ein Schnippchen zu schlagen.

Dieses von der German Privacy Foundation (GPF)[1] erstellte Handbuch bietet einen guten und sehr detaillierten Überblick über die zahlreichen Möglichkeiten und ihre Anwendung.

Auch wenn wir vielleicht nicht mit jedem einzelnen Text bis in das letzte Detail politisch übereinstimmen mögen, möchten wir an dieser Stelle der GPF nocheinmal herzlich für die Erstellung des Handbuches und die Unterstützung beim Druck danken.

Das bündnis für politik- und meinungsfreiheit (bpm)

[1] https://www.privacyfoundation.de/

2 Scroogled

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

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

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

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

Googeln an der Grenze - Allmächtiger. Greg hatte sich vor sechs Monaten von Google verabschiedet, nachdem er seine Aktienoptionen zu Barem gemacht hatte, um sich eine Auszeit zu gönnen, die dann allerdings nicht so befriedigend 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 anfingen, machten ein paar Kollegen und ich es zu unserem 20-Prozent-Projekt, ihnen in die Suppe zu spucken." (Eine von Googles unternehmerischen Innovationen war die Regel, dass alle Angestellten 20 Prozent ihrer Arbeitszeit in anspruchsvolle Projekte nach eigenem Gusto zu investieren hatten.) "Wir nennen es den Googleputzer. Er greift tief in die Datenbanken ein und normalisiert dich statistisch. Deine Suchanfragen, Gmail-Histogramme, Surfmuster. Alles. Greg, ich kann dich googleputzen. Eine andere Möglichkeit hast du nicht."

"Ich will nicht, dass du meinetwegen Ärger bekommst."

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

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

"Tu es", sagte er.

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

Nun gut, das sollte ihm recht sein.

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

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

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

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

"Pack deine Sachen", stieß sie heiser hervor.

"Was?"

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

"Wohin willst . . . "

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

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

Sie starrte ihn an und wischte ihre Haare aus dem Gesicht. "Der Googleputzer lebt. Als ich dich gesäubert hatte, habe ich ihn runtergefahren und bin verschwunden. Zu riskant, ihn noch weiter zu benutzen. Aber er

schickt mir Mailprotokolle, sooft er läuft. Und jemand hat ihn sechs Mal verwendet, um drei verschiedene Benutzerkonten zu schrubben - und die gehören zufällig alle Mitgliedern des Senats-Wirtschaftskomitees, die vor Neuwahlen stehen."

"Googler frisieren die Profile von Senatoren?"

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

"Du schnüffelst in Gmail-Konten?"

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

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

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

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

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

"Über den Googleputzer?"

"Über meine Freunde und Familie. Meine Such-Geschichte. Meine persönliche Geschichte."

“Jesus.”

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

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

“Wir müssen jetzt los”, beharrte sie.

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

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

“Greg, kommst du nun?”

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

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

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

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

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

. . . angefangen mit all den Dingen, um die Sie Ihr Profil bereinigt haben."

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

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

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

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

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

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

"Ich gehe zur Presse", sagte er.

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

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

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

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

"Wir stellen ein Team für Haus 49 zusammen …"

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

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

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

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

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

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

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

"Der Typ kommt also nach einem brutalen Wahlkampf-Tag voller Klinkenputzen ins Hotel, fährt den Laptop hoch und tippt *knackige Ärsche* in die

Suchleiste. Ist doch kein Drama, oder? Wir sehen es so: Wenn man wegen so was einen guten Mann daran hindert, weiterhin seinem Land zu dienen, wäre das schlichtweg unamerikanisch."

Greg nickte langsam.

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

"Ja."

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

Er betrachtete das Suchprofil des Kandidaten.

"Denke ich auch", erwiderte Greg.

Der neue Kongress benötigte elf Tage, um das Gesetz zur Sicherung und Erfassung von Amerikas Kommunikation und Hypertext zu verabschieden. Es erlaubte dem DHS und der NSA, bis zu 80 Prozent der Aufklärungs- und Analysearbeit an Fremdfirmen auszulagern. Theoretisch wurden die Aufträge über offene Bietverfahren vergeben, aber in den sicheren Mauern von Googles Haus 49 zweifelte niemand daran, wer den Zuschlag erhalten würde. Wenn Google 15 Milliarden Dollar für ein Programm ausgegeben hätte, Übeltäter an den Grenzen abzufangen, dann hätte es sie garantiert erwischt - Regierungen sind einfach nicht in der Lage, richtig zu suchen.

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

Als er am Googleplex zwischen all den Hybridautos und überquellenden Fahrradständern parkte, hatte er sich selbst überzeugt. Während er sich noch fragte, welche Sorte Bio-Fruchtshake er heute in der Kantine bestellen würde, verweigerte seine Codekarte den Zugang zu Haus 49. Die rote LED blinkte immer nur blöde vor sich hin, wenn er seine Karte durchzog. In jedem

anderen Gebäude würde immer mal jemand raus- und wieder reinkommen, dem man sich anschließen könnte. Aber die Googler in 49 kamen höchstens zum Essen raus, und manchmal nicht einmal dann.

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

"Greg, kann ich Sie bitte sprechen?"

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

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

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

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

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

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

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

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

Wir danken dem Autor Cory Doctorow und dem Übersetzer Christian Wöhrl dafür, dass sie den Text unter einer Creativ Commons Lizenz zur Nutzung durch Dritte bereitstellen.

3 Angriffe auf die Privatsphäre

Im realen Leben ist Anonymität die tagtäglich erlebte Erfahrung. Wir gehen eine Straße enlang, kaufen eine Zeitung, ohne uns ausweisen zu müssen. 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.

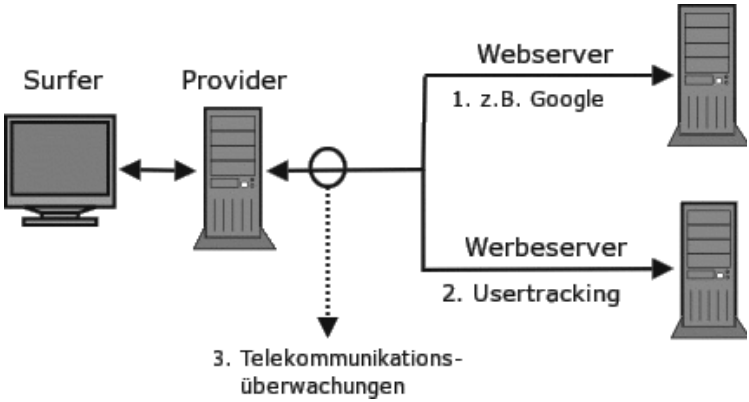


Abbildung 3.1: Möglichkeiten zur Überwachung im WWW

Staatliche Maßnahmen zur umfassenden, globalen Überwachung der Bevölkerung werden scheibchenweise ausgebaut und müssen von Providern unterstützt werden. (Vorratsdatenspeicherung, Access-Blocking...)

3.1 Beispiel Google

Das Beispiel Google wurde aufgrund der Bekanntheit gewählt. Auch andere Firmen versuchen ähnliche Dienste zu etablieren, die vergleichbar arbeiten. (MSN, Yahoo, Amazon...).

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 Firmanpolitik wird von iner 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 Milliaden 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 Ineressenprofil 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.

80% der wesentlichen 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 3.2 zur Besucherstatistik wurde vom Google Ad-Planner für eine (hier nicht genannte) Website erstellt. Man erkennt, das der überwiegende 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

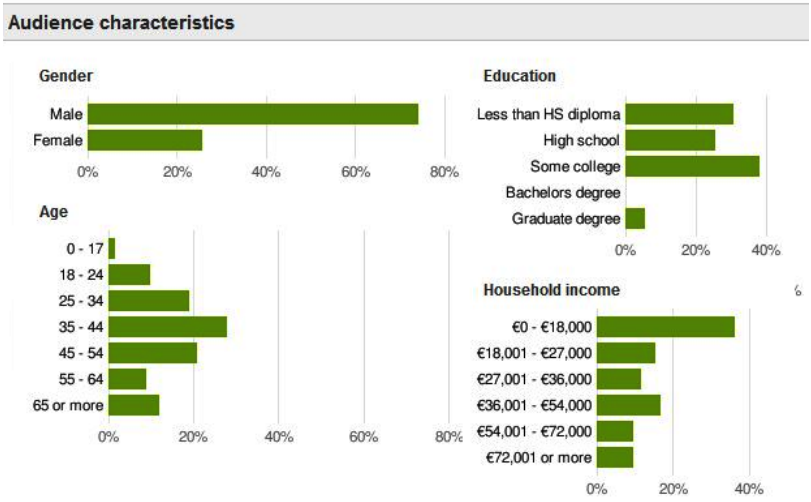


Abbildung 3.2: Ad-Planner Besucherstatistik (Beispiel)

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 detailierte 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... (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 allgemeine 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 eMail 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.)

Google Chrome und Google Toolbar

Noch immer gibt es Millionen Surfer, die bisher keinen Google-Account eingerichtet haben. Um auch für diese Nutzer eindeutige Profile generieren zu können, hat Google den Webbrowser *Chrome* und die *Google-Toolbar* für diverse andere Webbrowser entwickelt.

Diese Applikationen senden zusammen mit einer nutzerspezifischen ID die Infomationen über jede besuchte Website an Google. (kein weiterer Kommentar nötig - oder?)

Google Chrome bietet einen sogenannten Privacy-Mode. In diesem

Modus (auch Porno-Mode genannt) werden keine Daten auf die Festplatte geschrieben. Die Datenübertragung an Google bleibt davon aber unberührt.

Smartphones und Android

Nach dem Erfolg von Apples iPhone hat Google die Zeichen der Zeit erkannt und sucht mit dem Smartphone G1 auf dem Markt der mobilen Kommunikation ähnliche Erfolge wie im Web.

Das G1 ist ein in Hardware gegossenes Pendant zum Webbrowser Google Chrome. Bei der Markteinführührung 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. Von 70 Mio. Dollar Einnahmen der Mozilla Foundation stammen 65 Mio. Dollar von Google.

Das ist natürlich in erster Linie ein Angriff auf Microsoft und den dominierenden Internet Explorer. Die Entwickler von Firefox kommen ihrem datensammelden 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 *Iceweasel* 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.

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 Frankfuhrt und Zürich. In Council Bluffs (USA), Thailand, Malaisia 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.

Das Image ist (fast) alles

Die Archillesferse von Google ist das Image. In Ländern, die traditionell skeptisch gegenüber amerikanischen Unternehmen eingestellt sind, konnte Google längst nicht diese Markbeherrschung aufbauen wie in den USA und Westeuropa.

In Russland und China beantwortet der Suchdienst weniger als 20% der Anfragen. Primus in Russland ist die Suchmaschine *Yandex*, in China dominiert *Baidu*, in Tschechien *Seznam*.

3.2 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 Onlin-Versand von Brautkleidern möchte Frauen im Alter von 24-30 Jahren ansprechen, die verlobt sind. Das ist heute möglich.

Eine weitere Analyse des Wall Street Journal nimmt die Firma Rapleaf näher unter die Lupe. Diese Firma ist auf die Auswertung von Cookies spezialisiert. Neben den genannten Persönlichkeitsprofilen kann Rapleaf auch den realen Namen und viele genutzte E-Mail Adressen aufdecken. Diese Informationen werden meist durch Nutzung von Facebook o.ä verraten.

Häufig werden *Werbeeinblendungen* für das User-Tracking genutzt. Die in Webseiten darstellte 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 Institute für Software Systeme beschreiben in einer wiss. Veröffentlichung, wie man homosexuelle Männer anhand der Klicks auf Werbung erkennen kann. Das Verfahren kann für verschiedene Fragestellungen angepasst werden.

Neben Werbung und Cookies werden auch *HTML-Wanzen* (so genannten *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 hinterlassenen in den Logs des Servers Spuren für eine Verfolgung des Surfverhaltens.

Außerdem gibt es spezielle Tracking-Dienste wie Google Analytics, die oft mit Javascipt arbeiten.

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 Dokuentes vom Server der Firma nachgeladen und erlauben somit eine Konrolle, 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.....

3.3 History Sniffing

Die aktuellen Browser speichern Informationen über besuchte Webseiten in einer History.

Eine empirische Untersuchung der University of California zeigt, dass ca. 1% der Top 50.000 Websites versuchen, diese Daten über zuvor besuchte Websites auszulesen. Daneben gibt es spezielle Anbieter wie Tealium oder Beencounter, die einem kleineren Webmaster in Echtzeit eine Liste der Websites liefern, die ein Surfer zuvor besucht hat.

Die dabei übermittelten Informationen erlauben ein ähnlich detailiertes Interessenprofil zu erstellen, wie das User Tracking über viele Websites. Ein Experiment des Isec Forschungslabors für IT-Sicherheit zeigt, dass diese History-Daten 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 Deanonymiserung erfolgen. Die Realnamen sowie E-Mail Adressen wurden ohne Mithilfe des Surfer nur durch den Aufruf der präparierten Webseite ermittelt.

In der Regel wird obfuscated Javascript Code für den Angriff genutzt. Die

Websites werden bewusst so gestaltet, dass sie ohne Javascript nicht benutzbar sind, um eine Deaktivierung von Javascript zu verhindern. Außerdem können für moderne Browser CSS-Hacks für das History-Sniffing verwendet werden.

Die derzeit einzig wirksame Verteidigung gegen diesen Angriff besteht in der Deaktivierung der Browser History.

3.4 Geotagging

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

1. **Standortdaten** sind die wertvollsten Informationen für die Werbewirtschaft, um zukünftig den Markt zu vergrößern. Ein Online-Versand von Brautkleidern richtet seine Werbung an Frauen zwischen 24-30 Jahren, die verlobt sind. Ein Ladengeschäft stellt zusätzlich die Bedingung, 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.

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

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. VÜber 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.

- Mit Einführung des iPhone 4 hat Apple seine Datenschutzbestimmungen geändert. Die gesamte Produktpalette von Apple (iPhone, Laptops, PC…) wird in Zukunft den Standort des Nutzers laufend an Apple senden. Apple wird diese Daten Dritten zur Verfügung stellen. Wer Zugang zu diesen Daten hat, wird nicht näher spezifiziert. http://www.apple.com/chde/legal/privacy/

  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 Firma Heypic, die mit Risikokapital ausgestattet die Fotos von Twitter durchsucht und auf einer Karte darstellt.

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

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

Abbildung 3.3: Lokalisierung eines Smartphone durch Facebook

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

Nichts zu verbergen?

Wer ein praktisches Beispiel braucht: Einer Kanadierin wurde das Krankengeld gestrichen, weil sie auf Facebook fröhliche Urlausbfotos 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 nutze keine technischen Geo-Informationen sondern stellte visuell durch Beobachtung des Facebook-Profils den Aufenthaltsort fest. Aber das Beispiel zeigt, dass die automatisierte Auswertung Konsequenzen haben könnte. http://www.magnus.de/news/krankengeld-gestrichen-wegen-verfaenglichen-facebook-bildern-208271.html

3.5 Überwachungen im Internet

Unter http://www.daten-speicherung.de/index.php/ueberwachungsgesetze findet man eine umfassende Übersicht zu verschiedene 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!** (http://www.dubistterrorist.de)

Vorratsdatenspeicherung oder Mindest-Speicherfristen Ohne jeglichen Verdacht sollen die Verbindungsdaten jeder Kommunikation gespeichert werden (beispielsweise Absender und Empfänger jeder E-Mail, jedes Telefonat, jede SMS und die Standortdaten von Handys). Der Wissenschaftliche Dienst des Bundestages hat ein Rechtsgutachten mit schweren Bedenken hierzu vorgelegt. Trotzdem hat der Bundstag das Gesetz am 18.4.2007 verabschiedet.

Die Versuche zur Einführung der VDS begannen bereits im letzten Jahrhundert. 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). Entgegen diesem Auftrag des Bundestages war die deutsche Regierung eine treibende Kraft zur Einführung der VDS auf EU-Ebene.

Der Zugriff auf die gespeicherten Daten sollte nicht nur zur Verfolgung schwerer Verbrechen möglich sein, sondern bei allen Vergehen, die mittels Telekommunikation begangen werden. Auch präventiv, also ohne jeden Tatverdacht, sollten Ermittler und Geheimdienste in den Daten schürfen dürfen. Diesen Vorhaben hat das BVerfG im März 2010 einen Riegel vorgeschoben und das Gesetz für nichtig erklärt. Seitdem trommeln Bundesinnenminister de Maizière und BKA-Chef Ziercke für eine neue Gesetzesinitiative.

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.

	2007 (o. VDS)	2008 (o. VDS)	2009 (**mit VDS**)
Straftaten im Internet	179.026	167.451	206.909
Aufklärungsrate (Internet)	82.9%	79.8%	75.7%

In einem offenen Brief sprachen sich Richter und Staatsanwälte der Neuen Richtervereinigung (NRV) gegen die VDS aus und widersprechen der Darstellung des Bundesinnenminister und des BKA-Chef, wonach die VDS für die Kriminalitätsbekämpfung unbedingt nötig wäre.

Zensur im Internet Die Zensur wird in Deutschland im Namen des Kampfes gegen Kinderpornografie im Internet eingeführt. Man wird 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 befunden. http://blog.odem.org/2009/05/quellenanalyse.html

1. In der ersten Stufe unterzeichneten die fünf großen Provider freiwillig einen geheimen Vertrag mit dem BKA. Sie verpflichteten sich, eine Liste von Websites zu sperren, die vom BKA ohne jegliche Kontrolle erstellt wird.
2. In der zweiten Stufe wurde am 18.06.09 das *Zugangserschwernisgesetz* verabschiedet. Alle Provider mit mehr als 10.000 Kunden sollen diese geheime Liste von Websites zu sperren. Neben den (ungeeigneten) DNS-Sperren sollen auch IP-Sperren und Filterung der Inhalte zum Einsatz kommen.
3. Die CDU/FDP-Regierung ist im Herbst 2009 einen halben Schritt zurück gegangen und hat mit einem Anwendungserlass die Umsetzung des Gesetzes für ein Jahr aufgeschoben. Diese Regierung meint also, über dem Parlament zu stehen und ein beschlossenes Gesetz nicht umsetzen zu müssen.
4. Im Rahmen der Evaluierung des Gesetzes geht das BKA nur halbherzig gegen dokumentierten Missbrauch vor, wie eine Veröffentlichung des AK-Zensur zeigt. Gleichzeitig wird weiter Lobbyarbeit für das Zensurgesetz betrieben. http://ak-zensur.de/2010/08/kapitulation.html
5. Die Auswertung des eco Verband zeigt, dass Webseiten mit dokuemtiertem Missbrauch effektiv gelöscht werden können. 2010 wurden 99,4% der gemeldeten Webseiten gelöscht. Trotzdem wird der verfassungswidrige Zustand eines nicht angewandten Gesetzes durch die Regierung nicht durch Rücknahme des Gesetzes beendet. http://www.eco.de/verband/202_8727.htm

Der Aufbau einer Infrastruktur für Zensur im Internet wird auf vielen Wegen betrieben. Neben dem Popanz *Kinderpornografie* engagiert sich

die Content Maffia im Rahmen der geheimen ACTA Verhandlungen für eine verbindliche Verpflichtung zum Aufbau der Infrastruktur für Websperren.

Die verfassungsrechlichen Bedenken gegen die Zensur hat der wissenschaftliche Dienst des Bundestages in einem Gutachten zusammengefasst. (http://netzpolitik.org/wp-upload/bundestag_filter-gutachten.pdf) 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 wird eine Polizei mit den Kompetenzen eines Geheimdienstes geschaffen. Zu diesen Kompetenzen gehören neben der heimlichen Online-Durchsuchung von Computern der Lauschangriff außerhalb und innerhalb der Wohnung (incl. Video), Raster- und Schleierfahndung, weitgehende Abhörbefugnisse, Einsatz von V-Leuten, verdeckten Ermittlern und informellen Mitarbeitern...

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

Damit wird sich das BKA bis zu einem gewissen Grad jeglicher Kontrolle, der justiziellen und erst recht der parlamentarischen, entziehen können. Wolfgang Wieland (Grüne)

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.)

Elektronisicher 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

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

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

> *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?*

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.*

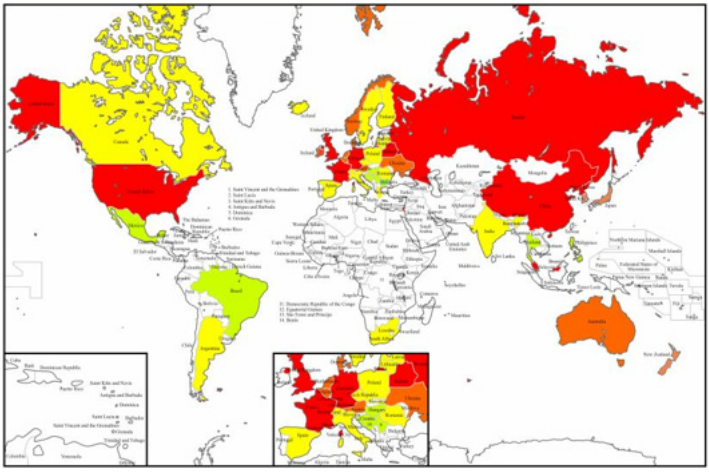


Abbildung 3.4: Vergleich der elektronischen Polizeistaaten

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 einer Verurteilung.

Ähnliche Meldungen hatten in den letzten Jahren viel weniger Resonanz in der Presse:

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...* (05.03.2009)

Der Springer-Presse standen im Fall Tauss umfangreiche Informationen zur Verfügung. Woher kamen diese Informationen? Jemand hat die Ermittlungsakten an die Presse weitergegeben! http://blog.fefe.de/?ts=b74d1e08

3.6 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 endgültig abgefahren ist.

Das Post- und Fernmeldegeheimnis, die Unverletzlichkeit der Privatsphäre und der ungehinderte Zugang zu Informationen sind in der UN-Resolution 217 A (III) [5] als grundlegende Menschenrechte definiert. Diese Resolution wurde 1948 unmittelbar nach den Erfahrungen der Diktatur verabschiedet und hat unser Grundgesetz maßgeblich beeinflusst.

Eine verfassungskonforme Gesetzgebung müsste den Intentionen des Grundgesetzes folgen und die in den Artikeln 2, 10 und 13 definierten Grundrechte anerkennen.

1. Ein Eingriff in die vom Grundgesetz geschützten Rechte ist nur zur Verfolgung schwerer Verbrechen zulässig. Es sind vom Gesetzgeber klare Festlegungen zu treffen, was ein *schweres Verbrechen* ist.

2. Der Eingriff muss im Einzelfall gründlich geprüft und genehmigt werden. Es kann nicht sein, dass der Verfassungsschutz selbst entscheidet, welche Rechner er hacken darf, oder dass das BKA ohne juristische Kontrolle unliebsame Websites sperrt.

3. Ähnlich wie bei Hausdurchsuchungen ist eine Offenheit der Maßnahme anzustreben. Um Betroffen die Gelegenheit zu geben, Rechtsmittel gegen ungerechtfertigte Bespitzelung einzulegen, ist eine Informationspflicht nach Abschluss der Maßnahme vorzusehen.

Das Bundesverfasungsgericht hat mehrfach die Einhaltung verfassungsrechtlicher Vorgaben angemahnt. Leider werden diese Grundsatzurteile immer wieder ignoriert. Ausschnitte aus einigen lesenswerten Begründungen:

- *"Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."* (Bereits 1983 wies der 1. Senates des Bundesverfassungsgerichts in seiner Urteilsbegründung zum Volkszählungsgesetz darauf hin, dass durch die grenzenlose Nutzung moderner Datenverarbeitungsanlagen ein psychischer Druck auf den Einzelnen entsteht, sein Verhalten aufgrund der öffentlichen Anteilnahme anzupassen.)

- *"Inzwischen scheint man sich an den Gedanken gewöhnt zu haben, dass mit den mittlerweile entwickelten technischen Möglichkeiten auch deren grenzenloser Einsatz hinzunehmen ist. Wenn aber selbst die persönliche Intimsphäre ... kein Tabu mehr ist, vor dem das Sicherheitsbedürfnis Halt zu machen hat, stellt sich auch verfassungsrechtlich die Frage, ob das Menschenbild, das eine solche Vorgehensweise erzeugt, noch einer freiheitlich- rechtsstaatlichen Demokratie entspricht."* (Aus dem Sondervotum der Richterinnen R. Jaeger und C. Hohmann- Dennherdt des 1. Senates des Bundesverfassungsgerichts zum Großen Lauschangriff 2004.)

3.7 Ich habe doch nichts zu verbergen

Dies Argument hören wir 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 folgenden vom Verfassungsschutz gesammelten Fakten konfrontiert: http://www.pilotundflugzeug.de/artikel/2006-02-10/Spitzelstaat
    1. Er wurde 1994 auf einer Demonstration kontrolliert. Er wurde nicht angezeigt, angeklagt oder einer Straftat verdächtigt, sondern nur als Teilnehmer registriert.
    2. Offensichtlich wurde daraufhin sein Bekanntenkreis durchleuchtet.
    3. Als Geschäftsführer einer GmbH für Softwareentwicklung habe er eine vorbestrafte Person beschäftig. 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. http://blog.kairaven.de/archives/998-Datenstigmaanekdote.html

- 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 nur schwer zu beziffern. http://www.lawblog.de/index.php/archives/2008/03/11/provider-liefert-falsche-daten-ans-bka/

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

- "Leimspur des BKA": Wie schnell man in das Visier der Fahnder des BKA geraten kann, zeigt ein Artikel bei Zeit-Online. Die Websites des BKA zur Gruppe "mg" ist ein Honeypot, der dazu dient, weitere Sympathiesanten 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 personenbeziehbarer Nutzerinformationen wie IP-Adressen, die bei der Online-Kommunikation zwischen Bürgern und Verwaltungseinrichtungen des Bundes anfallenden. Wir können daraus nur den Schluss ziehen, diese und ähnliche Angebote in Zukunft ausschließlich mit Anonymisierungsdiensten zu nutzen.

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

Politische Aktivisten

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

1. Erich Schmidt-Eenboom veröffentliche 1994 als Publizist und Friedensforscher ein Buch über den BND. In den folgenden Monaten wurden er und seine Mitarbeiter vom BND ohne rechtliche Grundlage intensiv überwacht, um die Kontaktpersonen zu ermitteln. Ein Interview unter dem Titel *"Sie beschatteten mich sogar in der Sauna"* steht online: http://www.spiegel.de/politik/deutschland/0,1518,384374,00.html

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 wurd 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.

4 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 Zensur-Maßnahmen 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 persönliche 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.

4.1 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. Ausgangspungt 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.)

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…

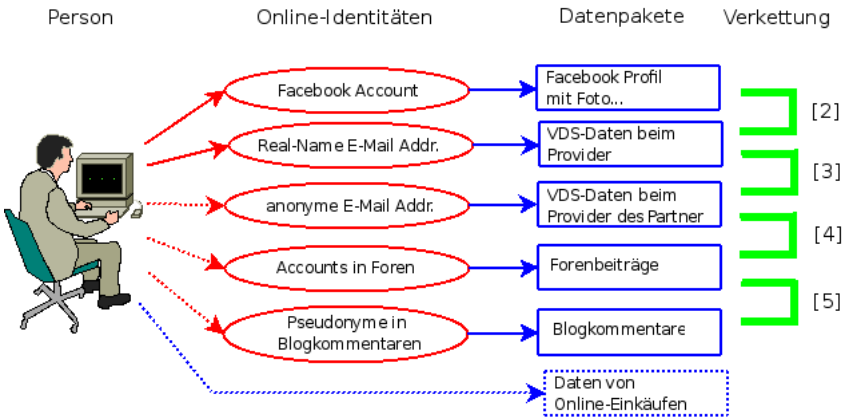


Abbildung 4.1: Datenverkettung

- Bei der Nutzung von vielen Webdiensten fallen kleine Datenkrümel an. Auch E-Mails werden von den Datensammlern ausgewertet. Die IP-Adresse des Absenders 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 Blog findet man Postings und Kommentare, häufig mit den gleichen Pseudonymen, die auch für die E-Mail Adressen verwendet werden.
- Online-Einkäufern erforden in der Regel die Angaben zur Kontoverbindung und einer Lieferadresse, die der Person zugeordnet werden können.

Verkettung der Informationen und Datenpäkchen

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. http://www.heise.de/tp/r4/artikel/31/31691/1.html
   - MIT-Studenten erkennen homosexuelle Neigungen ihrer Kommilitonen anhand der Informationen über Freundschaften in den Facebook-Profilen. http://www.heise.de/tp/r4/artikel/31/31181/1.html
   - Das der Grünen-Vorsitzende Özdemirs eine Freundschaft mit dem Intensivstraftäter Muhlis Ari pflegt, ist an seinem Facebook-Profil erkennbar. http://www.heise.de/tp/r4/artikel/32/32138/1.html
2. Dem Facebook Profil kann man durch Kombination mit anderen Datenkrümeln den realen Namen und die meisten genutzten E-Mail Adressen zuordnen. Die Firma Rapleaf ist z.B. darauf spezialisiert. Auch pseudonyme Facebook Accounts können deanonymisiert werden.
3. Durch Analyse der im Rahmen der VDS gespeicherten IP-Adressen können bei zeitlicher Übereinstimmung beide E-Mail Adressen der gleichen Person zugeordnet werden. Ein einzelner passender Datensatz reicht aus. (Wenn nicht konsequent Anonymisierungsdienste für das anonyme Postfach verwendet werden.)
4. Die Verbindung zwischen anonymer E-Mail Adresse und Foren Account ergibt sich durch die Nutzung der E-Mail Adresse bei Anmeldung.
5. Durch Vergleiche von Aussagen und Wortwahl lassen sich Korrelationen zwischen verschiednen 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) http://www.netzpolitik.org/2009/exklusiv-die-buecher-der-anderen

- Die Libris Shops (Zugang zu den Bestellungen von 1000 Buchshops)
  http://www.netzpolitik.org/2009/exklusiv-die-libri-shops-der-anderen
- Sparkassen-Shops (350.000 Rechnung online einsehbar)
  http://www.netzpolitik.org/2009/zugriff-auf-350-000-rechnungen-im-sparkasse-shop
- Acht Millionen Adressen von Quelle-Kunden sollen verkauft werden.
  http://www.zeit.de/digital/datenschutz/2009-11/quelle-kundendaten-verkauf

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-anonymsiert 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 vieler Hinsicht beeinflussen, ohne das 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?*
  - 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 werden verschickt.

- Firmen verschaffen sich unrechtmäßig Zugang zu Verbindungs- und Bankdaten, um ihrer Mitarbeiter auszuforschen. (Telekom- und Bahn-Skandal)

- Identitätsdiebstahl ist eine stark wachsendes Delikte. Kriminelle duchforsten das Web nach Informationen über reale Personen und nutzen diese Identitäten für Straftaten. Wie sich Datenmissbrauch anfühlt: Man wird plötzlich mit Mahnungen für nicht bezahlte Dienstleitungen überschüttet, die man nie in Anspruch genommen hat. http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung

- 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. Ein Kommentar von Kai Bierman: Indect - der Traum der EU vom Polizeistaat.

Ich habe doch nichts zu verbergen...

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

4.2 Ein Beispiel

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

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

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

Die moderne Studentin ist sozial vernetzt. Naheliegend ist es, die verschiedenen Netzwerke wie StudiVZ usw. nach F. abzusuchen. Bei Facebook wird 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 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 *Syncron-Saufen* im Internet. Scheinbar ist sie auch vereinsamt.
- F. ist offenbar lesbisch, sie sucht nach einer Frau bei abgefuckt.de.

- F. ist im linksradikalen Spektrum aktiv. Sie hat an mehreren Demonstrationen teilgenommen und berichtet über Erfahrungen mit Hausdurchsuchungen. Möglicherweise ist das die Ursache für ihre Angstzustände.

- Öffentlich prangert sie in einem Diskussionsforum die Firma ihres Vaters an (wegen Ausspionierens von Mitarbeitern).

- Ihre linksgerichtete Grundhaltung wird durch öffentliche Unterstützung der Kampagne *Laut ficken gegen Rechts* unterstrichen.

- Von regelmäßiger Arbeit hält sie nicht viel.

- Die angebene 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? 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.

4.3 Kommunikations-Analyse

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 in der FAZ)

Kommunikationsanalyse ist ein abstrakter Begriff. Anhand eines stark vereinfachten Beispiel 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, das *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 4.2). 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 *Detlef* näher zu untersuchen. Beide sind aber vorsichtig und es besteht kein umfassender Zugriff auf die Kommunikationsdaten. Dann nimmt als Ersatz vielleicht *Frida*, um das Modell zu präzisieren.

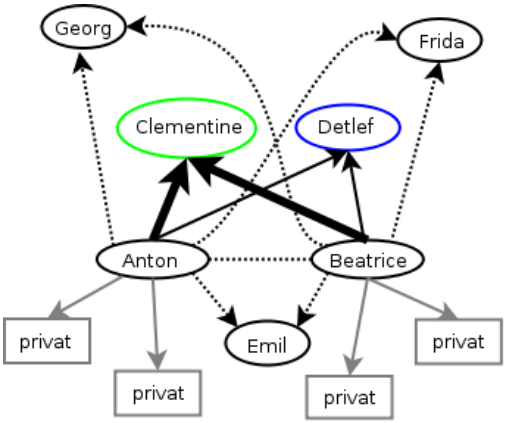


Abbildung 4.2: Soziales Netz von Anton und Beatrice

Frida unterhält vor allem einen engen Kontakt zu *Detlef*, was zu einer Umbewertung der Positionen von *Detlef* und *Clementine* führt (Bild 4.3). Bei *Emil* handelt es sich evtl. um einen zufällig gemeinsamen Bekannten von *Anton* und *Beatrice*, der nicht in die "mg" eingebunden ist.

Die Verwendung der so gewonnenen Informationen demonstriert das *Projekt "Gegenwirken"* der niederländischen Geheimdienste. In regierungskritischen Organisationen werden die Aktivisten identifiziert, deren Engagement für die Gruppe wesentlich ist. Für die Kommunikationsanalyse nötigen 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.

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, Twitter bietet ein umfangreichen Datenpool oder die Kommentare in Blogs und Foren. Teilweise werden von Unternehmen gezielt

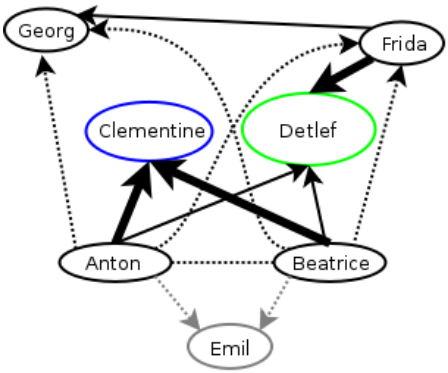


Abbildung 4.3: Präzisierte Struktur der ”mg“

Blogs und Foren zu bestimmten Themen aufgesetzt, um Daten zu generieren. In diesen Communitys wird Position einzelner Mitglieder analysiert, um die *Meinungsmacher* zu finden.

Gegenwärtig ist die Analyse von Gruppen Gegenstand intensiver Forschung (sowohl im zivilen wie auch geheimdienstlichem 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.

m Rahmen der Vorratsdatenspeicherung (VDS) sollen genau die Datenbestände angelegt werden, die den Geheimdiensten und dem BKA eine umfassende Kommunikationsanalyse ermöglichen. Zur Kriminalitätsbekämpfung und -prävention taugt die VDS nicht, wie ein Vergleich der Kriminalitätsstatistik des BKA für die Jahre 2007, 2008 und 2009 zeigt. Es wird nicht einmal die erwartete um 0,006 Prozentpunkte höhere Aufklärungsrate erreicht.

	2007 (o. VDS)	2008 (o. VDS)	2009 (**mit VDS**)
Straftaten im Internet	179.026	167.451	206.909
Aufklärungsrate (Internet)	82.9%	79.8%	75.7%

	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%

In einem offenen Brief sprechen sich Richter und Staatsanwälte der Neuen Richtervereinigung (NRV) gegen die Vorratsdatenspeicherung aus und widersprechen der Darstellung von Bundesinnenminister Thomas de Maizière und BKA-Chefs Ziercke, wonach die VDS für die Kriminalitätsbekämpfung unbedingt nötig wäre.

5 Spurenarm Surfen

Bild 5.1 zeigt ein Konzept für anonymes Surfen:

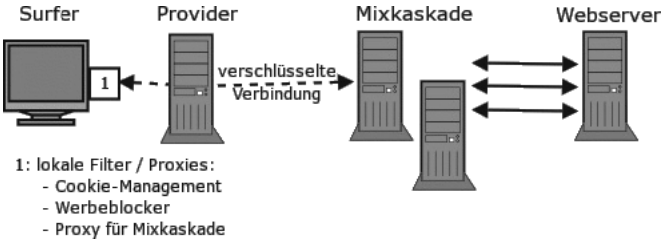


Abbildung 5.1: Konzept für anonymes Surfen

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 und HTML-Wanzen 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 *Anonymymisierungsdienste nutzen*)

Mit diesen Maßnahmen kann es vorkommen, dass Websites nicht wie erwartet funktionieren. Gute Webdesigner verzichteten auf suspekte

Technologien, JavaScript wird sinnvoll eingesetzt und der Surfer auf fehlende Freigaben hingewiesen, Cookies können für Logins nötig sein.

Schlechtes Webdesign nutzt andere Techniken (Referer, User-Agent) ohne den Surfer auf die notwendigen Freigaben hinzuweisen. Hier ist man auf Probieren und Raten angewiesen, wenn eine Website nicht wie erwartet funktioniert. Man kann schrittweise die Annahme von Cookies freigeben, JavaScript und Java aktivieren usw. Ob die Deaktivierung der Schutzmaßnahmen die volle Funktionalität aufwiegt, muss man bei Bedarf selbst entscheiden.

5.1 Auswahl des Webbrowsers

Firefox ist der Webbrowser der Mozilla Foundation. Er ist kostenfrei nutzbar und steht unter der Adresse http://www.mozilla-europe.org/de/firefox für fast alle Betriebssystem zum Download bereit. Linux-Distributionen enthalten den Browser in der Regel. Debian GNU/Linux enthält eine *rebranded version* des Browsers unter dem Namen *Iceweasel*.

Firefox kann durch viele von der Community entwickelte Plug-Ins zu einem sehr sicheren und privacy-freundlichen Browser aufgewertet werden. Er wird von den Entwicklern der Anonymisierungsdienste JonDonym und Tor Onion Router ausdrücklich empfohlen.

Im Rahmen dieser Anleitung empfehlen auch wir die Nutzung von Firefox und geben Hinweise, wie man den Browser ein wenig aufwertet. Ziel ist dabei die Erhöhung der Sicherheit und das Vermeiden von Beobachtung durch neugierige Anbieter von Webdiensten.

5.2 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.

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, weniger geeignet für Computerprobleme.

Meta-Suchmaschinen

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

- **Ixquick.com** (https://www.ixquick.com/deu/)
  ist eine niederländische Meta-Suchmaschine, die keine IP-Adressen speichert und keine Profile der Nutzer generiert. Die Suchmaschien ist nach dem Datenschutzsiegel EuroPriSe zertifiziert.

  Als kleines Schmackerl 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*:

- **starting page** (https://www.startingpage.com/)
  ist ebenfalls mit dem Datenschutzsiegel EuroPriSe zertifiziert. Die Suchmaschine bietet einen privacy-freundlichen Zugriff auf die Google Suche, ist also einen ideale Ergänzung zu Ixquick.com. Ein Proxy zum anonymen Aufruf der Webseiten aus den Ergebnissen bietet diese Suchmaschine ebenfalls.

- **Metager2.de** ist ein Klassiker vom Suma e.V. Neben klassischen Suchdiensten wird auch die Perr-2-Peer Suche Yacy einbezogen. Dadurch verzögert sich die Anzeige der Ergebnisse etwas.

- **Scroogle** (https://ssl.scroogle.org)
  Scroogle ist ein anonymisierender Proxy für Google. Scroogle reicht die Anfragen an Google weiter und entfernt dabei alle persönlichen Informationen.

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 Translater kennt neben Englisch und Deutsch weitere Sprachen.

Peer-2-Peer Suchmaschine

Yacy (http://yacy.net/) 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 unter http://java.sun.com gibt.Danach holt man sich die Yacy-Software von der Website des Projektes und startet den Installer - fertig.

Aktuelle Versionen von Yacy stehen für Debian und Ubuntu stehen im Repository des Projektes zur Verfügung. Man fügt folgende Zeile in die Datei */etc/apt/sources.list* ein oder nutzt ein GUI (*Software Quellen*)

```
deb http://debian.yacy.net ./
```

Anschließen spült am wie üblich alles auf die Platte. Das Repository von Yacy.net ist nicht mit einem OpenPGP-Key signiert. Eine Warnung erscheint bei der Installation und man muss extra bestätigen, dass diese Software installiert werden soll.

```
# aptitude update && aptitude install yacy
```

Nach dem Start von Yacy kann man im sich öffnenden Bowserfenster 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 Ergebisseite sauber dargestellt wird. Mit den Topwords unter

den Ergebnissen bietet Yacy ein ähnliches Konzept wie Clusty.com, 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.

5.2.1 Firefox konfigurieren

Für viele Suchdienste gibt es Plug-Ins zur Integration in die Suchleiste von Firefox. Die Website http://mycroft.mozdev.org/ bietet ein Suchformular, mit dem man die passenden Plug-Ins nach Eingabe des Namens der Suchmaschine schnell findet. Die Installation funktioniert nur, wenn JavaScript für diese Website freigegeben wurde. Das Addon für die Suchmaschine Startingpage gibt es unter http://www.startingpage.com/deu/download-startingpage-plugin.html

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, Wikipeadia, Startingpage u.a.m.

Außerdem empfehlen wir, die Generierung von Suchvorschlägen zu deaktivieren. 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 *Schmaschinen verwalten* in der Liste der Suchmaschinen.

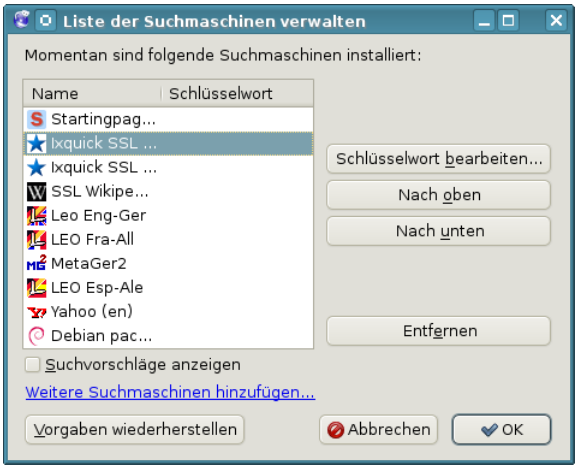


Abbildung 5.2: Suchmaschinen verwalten

5.3 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 5.3 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 drei datensammelnde Werbeserver Cookies (google.com, doubleclick.net, adition.com) und außerdem Zähldienste (quality-chanel.de, ivwbox.de), welche die Reichweiten von Online-Publikationen auswerten.

Der Screenshot wurde im Jahr 2009 aufgenommen. Das Cookie “co” von adition.com möchte gern bis 2025 auf diesem PC bleiben! Außerdem speichert adition.com offensichtlich eine eindeutige UserID und die IP-Adresse in Cookies, um den Surfer beim Besuch von weiteren Websites wiederzuerkennen.

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

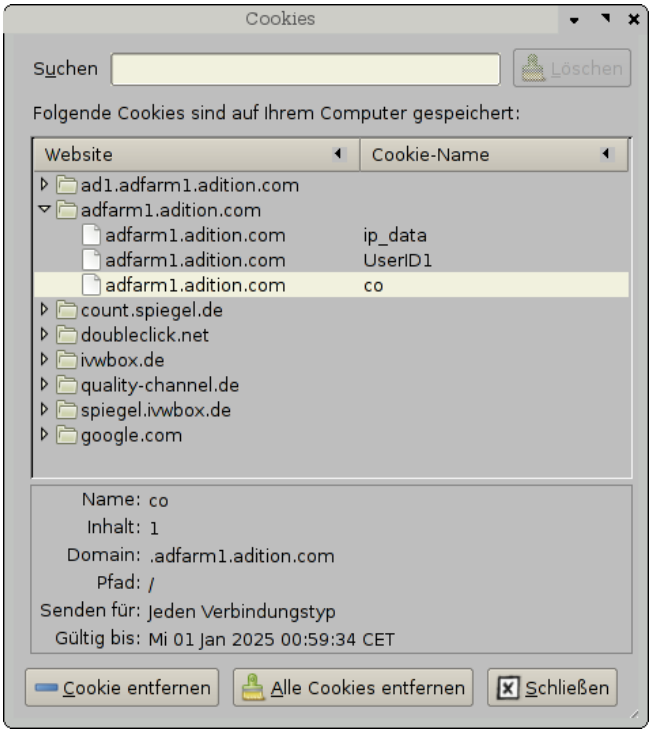


Abbildung 5.3: Liste der Cookies beim Besuch von Spiegel-Online

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 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.

5.3.1 Mozilla Firefox konfigurieren

Mozilla Firefox bietet bereits standardmäßig die Möglichkeit, die meisten Cookies ohne Einbußen am Surf-Erlebnis loszuwerden. Im Bild 5.4 gezeigte Dialog *Einstellungen* Sektion *Datenschutz* kann die Annahme von Fremd-Cookies standardmäßig deaktiviert werden.

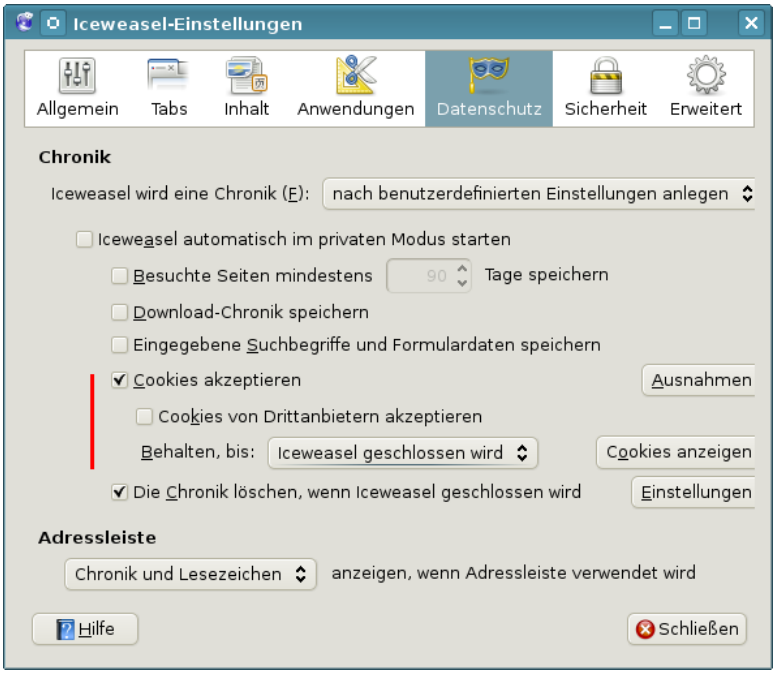


Abbildung 5.4: Cookies-Einstellungen in Firefox

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 eingebettet Werbung und Google-Analytics auf vielen Websites kann das Imperium Google unbedarfte Firefox-Nutzer 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. Wir können das Add-on **CookieMonster** empfehlen. Es erlaubt die site-spezifische Verwaltung von Cookies. Das Add-on ist zu finden unter https://addons.mozilla.org/de/firefox/addon/4703.

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 5.5 dargestellte Menü (nur wenn die Website Cookies nutzen möchte).

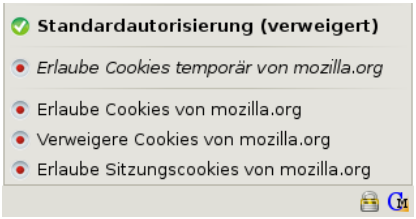


Abbildung 5.5: CookieMonster Menü

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.

5.3.2 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 die DOM-Storage an. Es reicht aus, die Cookies zu deaktivieren. Damit ist auch die clientseitige Datenspeicherung deaktiviert.

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

5.3.3 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, Google...

Flash-Player bieten unterschiedliche Möglichkeiten, diese Datenspeicherung zu deaktivieren:

1. Wer den **Adobe Flash-Player** nutzt, kann mit einer Flash Anwendung auf der Webseite von Macromedia die Einstellungen für das Speichern und Auslesen von Informationen, Mikrofons und Kamera anpassen.
   http://www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager.html

Auf der Seite *Globale Speichereinstellungen* ist die Datenspeicherung zu deaktivieren (Bild 5.6). Anschließend sind auf der Seite *Webseiten Speichereinstellungen* die bisher gespeicherten Cookies zu löschen.

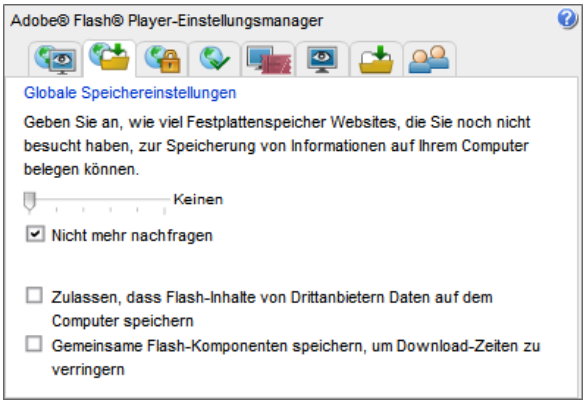


Abbildung 5.6: Einstellungsmanager für Adobe Flash-Player

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.

5.4 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 Anonymisierungsdienste nutzt. Die EFF geht davon aus, dass diese Methode bereits von Datensammlern genutzt wird.

2. Durch Einschleusen von Schadcode können Sicherheitslücken ausgenutzt und der 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.

5.4.1 NoScript für Mozilla Firefox

Die Einstellungen für JavaScript lassen sich mit dem Add-on *NoScript* komfortable verwalten. Die Erweiterung kann von der Website der Firefox-Erweiterungen installiert werden: https://addons.mozilla.org/de/firefox/addon/722. Ein einfacher Klick auf das Download-Symbol startet die Installation. Im Anschluss ist Firefox neu zu starten.

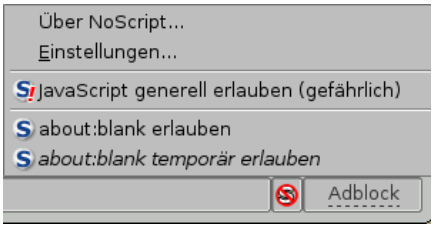


Abbildung 5.7: NoScript-Button und Menü in der Statuszeile

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 5.7 gezeigte Menü, welches JavaScript für die aktuelle Site generell oder temporär für die laufende Sitzung freigibt.

Wählt man den Punkt *Einstellungen* im NoScript-Menü, öffnet sich der Einstellungsdialog (Bild 5.8), der auf dem Reiter *Positivliste* eine Liste der Websites zeigt, für welche Java-Script freigegeben wurde. Als Erstes sollte man aus der Positivliste alles entfernen, was man nicht wirklich braucht. In der Liste findet man standardmäßig mit *googlesyndications* auch Surf-Tracker.

Abbildung 5.8: Einstellungen für NoScript

Auf dem Reiter *Benachrichtigungen* lässt sich beispielsweise konfigurieren, ob NoScript den Surfer mit einem Sound oder mit einem Info-Balken darüber informiert, dass Scripte auf der aktuellen Webseite blockiert wurden.

Der Sound nervt mich, diese Option habe ich deaktiviert. Wenn eine Webseite jedoch nicht wie erwartet funktioniert, kann die kurze Einblendung eines Info-Balkens hilfreich bei der Suche nach den Ursachen sein.

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. Bild 5.9 zeigt einen Screenshot mit NoScript in Aktion.

Abbildung 5.9: NoScript in Aktion

5.5 Werbung und HTML-Wanzen

Die auf vielen Websites eingeblendete Werbung wird von wenigen Servern bereitgestellt. Diese nutzen häufig die Möglichkeit, das Surfverhalten website-übergreifend 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.

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.

Webbugs kann man mit dem Plug-In NoScript blockieren.

Hinweis: das System METIS (http://www.vgwort.de/metis.php) der VG Wort verwendet HTML-Wanzen, um die Besucher von Online-Angeboten zu zählen und anhand der Ergebnisse Tantiemen an deutsche Autoren auszuzahlen. Wer Autoren im Web unterstützen möchte, kann in NoScript den Server *vg04.met.vgwort.de* als vertrauenswürdig definieren.

5.5.1 Adblock für Mozilla Firefox

Für Mozilla Firefox steht mit *Adblock Plus* ein Add-on für das Blockieren von Werbung zur Verfügung. Ein einfacher Klick auf das Install-Symbol der Website startet den Download der Erweiterungen und installiert sie. Download-Link: https://addons.mozilla.org/firefox/1865

Nach dem Neustart ist mindestens eine Filterliste zu abonnieren. Weitere Filterlisten können im Einstellungsdialog unter dem Menüpunkt *Extras->Adblock Plus* abboniert werden. Hier ist der Menüpunkt *Filter->Abonnement hinzufügen* zu wählen und aus der Liste der angebotenen Filter können regional passende Listen gewählt werden.

5.6 History Sniffing vermeiden

Das Schnüffeln in der Surf-History bzw. -Chronik kann wirksam nur durch ein Deaktivieren der Speicherung der besuchten Websites unterbunden werden. Im Dialog *"Einstellungen"* kann man auf dem Reiter *"Datenschutz"* die Speicherung besuchter Webseiten deaktivieren.

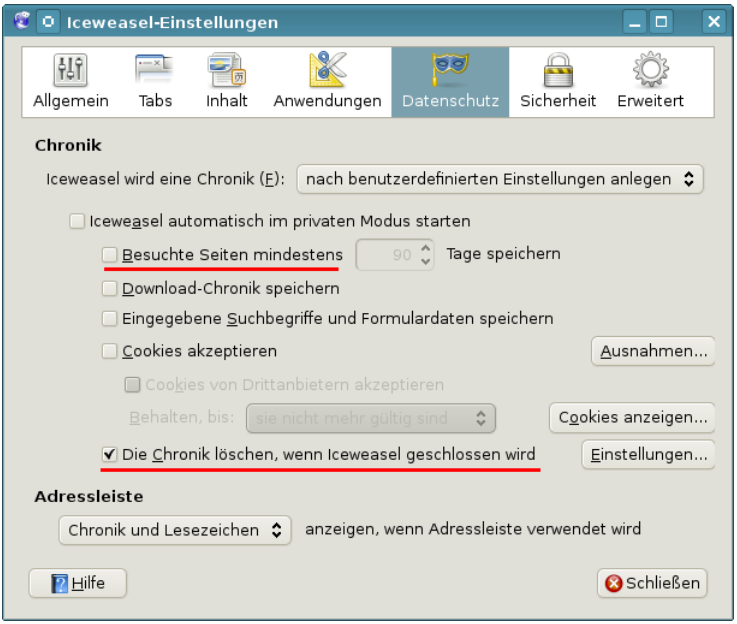


Abbildung 5.10: Speichern der Surf-Chronik deaktivieren

5.7 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.

5.7.1 PDF Reader Plugins

Viele PDF-Reader bringen Plugins für populäre Browser mit. Sie werden in der Regel ungefragt mit installiert. Diese PDF Plugins sind derzeit ein Hauptrisiko für Surfer. Nach Beobachtung der Sicherheitsdienstleister Symantec und ScanSafe richten sich die meisten Angriffe im Web gegen PDF Plugins oder erfolgen mit präparierten PDF-Dokumenten.

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. 2008 gelang es dem Ghostnet, die Rechner westlicher Regierungen, der US-Regierung und des Dalai Lama mit bösartigen PDFs zu infizieren.

Als Schutzmaßnahme können PDF Reader Plugins im Browser deativiert werden. Die Dokumente sind vor dem Öffnen zu speichern und nicht im Context des Browsers zu betrachten. Das verhindert Drive-by-Download Angriffe, bei denen PDF-Dokumente ohne Zustimmung herunter geladen und geöffnet werden. Außerdem sollte man PDFs aus unbekannter Quelle ein ähnliches Mißtrauen entgegen bringen, wie ausführbaren EXE- oder PAF-Dateien.

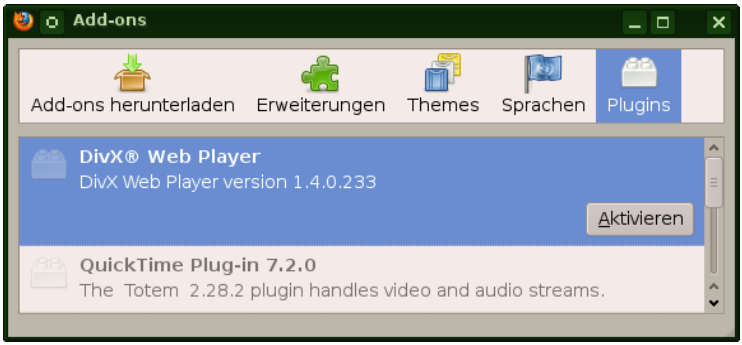


Abbildung 5.11: Plugins deaktivieren

Alle Plugins können im Addon-Manager deaktiviert werden: *Extras -> Add-ons*.

Statt funktionsüberladener Monster-Applikationen sollte man einfache PDF-Reader nutzen, die sich auf die wesentliche Funktion des Anzeigens von PDF-Dokumenten beschränken. Die FSFE stellt auf PDFreaders.org Alternativen aus der Open Source Community vor.

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.

Auf dem Reiter *Anwendungen* im Dialog *Einstellungen* können die Helper-Applications wie im Bild 5.12 für jeden Dateityp auf *"Jedes Mal nachfragen"* gesetzt werden. Diese Einstellungen sind natürlich nur sinnvoll, wenn der Surfer kritisch hinterfragt, ob die Aktion wirlich dem entspricht, was er erwartet. Wer unkritisch bei jeder Nachfrage auf *Öffnen* klickt, muss sich nicht wundern, wenn sein Computer infiziert wird.

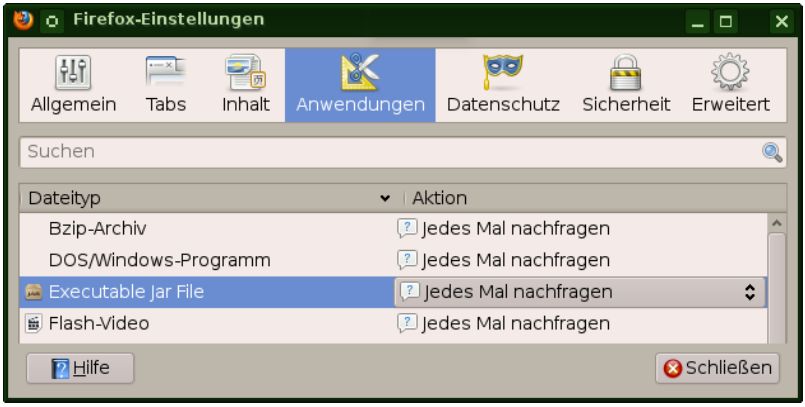


Abbildung 5.12: Externe Anwendungen nur auf Nachfrage öffnen

5.7.2 Flash und Silverlight

Auch die Plugins sind ein Sicherheits- und Privacyrisiko. Sie werden meist für die Darstellung von Videos im Web (Youtube) und Panoramdiensten 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.

2. Web Videos können mit Hilfe von Download Sites wie aTube Catcher (http://atube-catcher.dsnetwb.com/), KeepVid (http://keepvid.com)

oder ShareTube (http://www.share-tube.de/flvdownload.php) als FLV-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 Add-ons **UnPlug** oder **DownloadHelper** können Videos von vielen Websites herunter laden. Es zeigt durch drei rotierende Kugeln in der Toolbar an, das Medien gefunden wurden, die gespeichert werden können. Dabei können die Flash-Filme in ein gebräuchlicheres Format konvertiert werden. Zum Anschauen nutzt man den bevorzugten Mediaplayer.

5.8 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 ist einfach konfigurierbar, kann aber nur *http://* durch *https://* für eine Liste von Websites ersetzen.
- **HTTPSEverywhere** kann auch komplexe Umschreibungen der URLs realisieren, wie es beispw. für Wikipedia notwendig ist. Die Konfiguration ist aufwendiger und erfolgt über XML-Dateien.

Eine automatische Umschaltung von HTTP auf HTTPS ist ohne Unterstützung durch den Webmaster nicht möglich. Für beide Add-ons muss man die Liste der Websites konfigurieren, die ausschließlich per HTTPS genutzt werden sollen.

NoScript Enforce HTTPS

Das Add-on NoScript enthält eine Enforce HTTPS Implementierung. 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. Weitere Vorschläge für die Liste der HTTPS only Websites:

Presse:

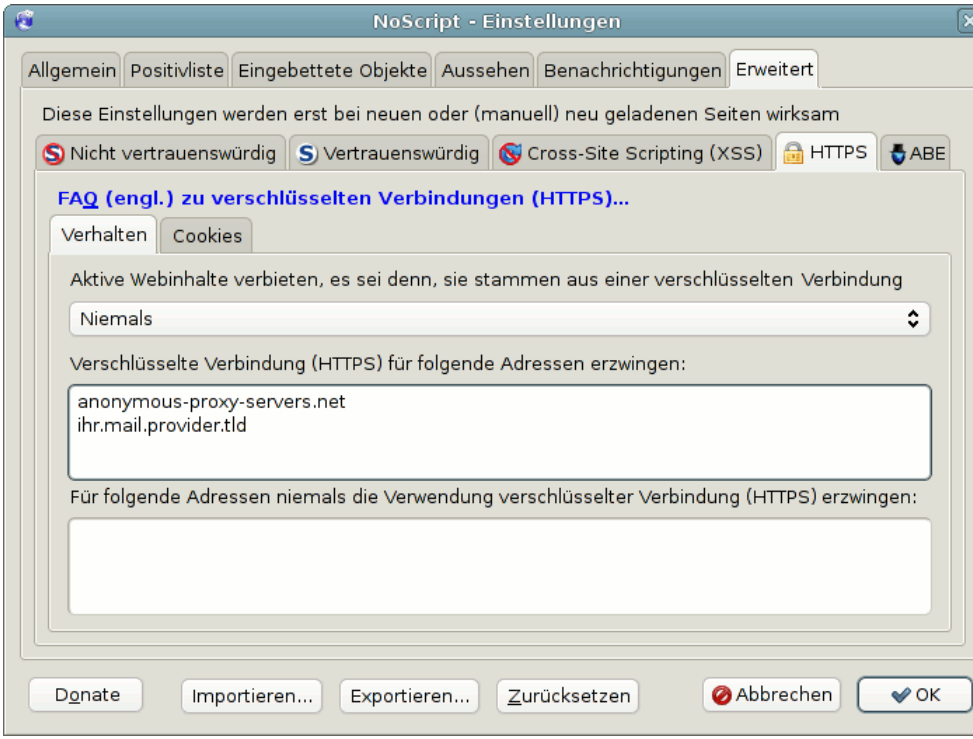


Abbildung 5.13: Einstellungen für NoScript STS

```
www.aftenposten.no
www.economist.com
www.faz.net
www.freitag.de
www.nytimes.com
www.taz.de
taz.de
blogs.taz.de
www.washingtonpost.com
voices.washingtonpost.com
```

NGOs:

```
www.accessnow.org
```

```
www.amnesty.org
www.democracynow.org
www.eff.org
www.vorratsdatenspeicherung.de
wiki.vorratsdatenspeicherung.de
www.privacyfoundation.de
```

Blogs:

```
blog.fefe.de
www.lawblog.de
www.netzpolitik.org
scusiblog.org
```

HTTPSEverywhere

Das Firefox Add-on HTTPSEverywhere der EFF kann Adressen nach komplexen Regeln umschreiben. Nach der Installation kann man in der Konfiguration die Regeln für die Umschreibung aktivieren. Das Add-on steht unter https://www.eff.org/https-everywhere zum Download bereit und bringt bereits Regeln für eine Reihe von häufig benutzten Webseiten mit (Bild 5.14).

Die Regeln for Suchmaschinen wie Google, Ixquick, DuckDuckGo oder Scroogle kann man deaktivieren. Statt Umschreibung der URLs sollte man besser die Search Add-on mit SSL-Verschlüsselung nutzen, die unter mycroft.mozdev.org bereitstehen. Das Projekt HTTPSEverywhere hat außerdem eine große Sammlung von fertigen Regeln als XML-Dateien. Entsprechend dem eigenen Bedarf kann man Dateien aus diesem Pool im Profil von Firefox im Unterverzeichnis HTTPSEverywhereUserRules speichern. Das Firefox Profil findet man unter:

- Linux: $HOME/.mozilla/firefox/<profilverzeichnis>
- Windows: C:/Dokumente und Einstellungen/<username>/ Anwendungen/Mozilla/Firefox/<profilverzeichnis>

Nach dem Speichern von zusätzlicher Rulesets ist Firefox neu zu starten, um die Regeln zu aktivieren.

Abbildung 5.14: Aktivierung von Rulesets in HTTPSEverywhere

5.9 HTTPS-Security

Die IT-Sicherheitsforscher C. Soghoian und S. Stamm kommen in einer wiss. Arbeit zu dem Schluss, dass Geheimdienste mit gültigen SSL-Zertifikaten schwer erkennbare man-in-the-middle Angriffe durchführen können. Außerdem ist es so einfach, als Unberechtigter ein gültiges SSL-Zertifikat für Mail- oder Web-Server ausstellen zu lassen.
Siehe https://bugzilla.mozilla.org/show_bug.cgi?id=556468

Ein paar kleine Erweiterungen für Firefox können die Sicherheit bei der Nutzung von verschlüsselten HTTPS-Verbindungen deutlich erhöhen.

- **SSL-Blacklist** ist ein Add-on, welches vor Websites mit unsicheren SSL-Zertifikaten warnt. Diese unsicheren SSL-Zertifikate wurden aufgrund eines Fehlers in der openssl-Version von Debian GNU/Linux generiert oder verwenden angreifbare MD5-Signaturen in der Signaturkette. Es steht bereit unter: http://www.codefromthe70s.org/sslblacklist.aspx
- **Certificates Patro**l speichert Informationen zu den Zertifikaten einer Website in einer internen Datenbank. Beim Erstbesuch präsentiert es das das Zertifikat und fordert den Surfer auf, es zu prüfen. Am einfachsten kann man das Zertifikat prüfen, wenn die Fingerprints vom Webmaster

veröffentlicht wurden.

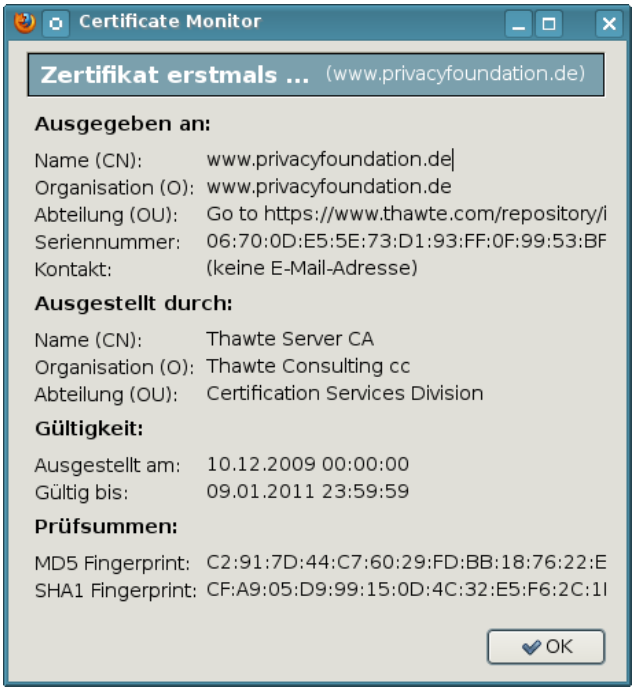


Abbildung 5.15: Certificates Patrol zeigt ein unbekanntes SSL-Zertifikat

Hat sich das Zertifikat bei späteren Besuchen der Website geändert, zeigt das Add-on Informationen zum alten und neuen Zetifikat. Der Nutzer muss das neue Zertifikat ebenfalls bestätigen. Eine Änderung des Zertifikates kann ein Hinweis auf einen man-in-the-middle Angriff sein.

Die Bewertung der dargestellten Informationen erfordert technische Kenntnisse über das Zertifikatssystem. Beim Erstkontakt oder Warnungen kann man das Zertifikat ergänzend mit Perspectives verfizieren.

- **Perspectives** vergleicht SSL-Zertifikate mit den bei Notary Servern bekannten Zertifikaten. Wenn alle Notary-Server das gleiche Zertifikat

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.

Wer häufig auf Community-Websites mit HTTPS-Zertifikaten von CAcert.org oder selbstsignierten Zertifikaten unterwegs ist, kann die Standardkonfiguration nutzen. In diesem Fall wird der SSL-Error abgefangen und das Zertifikat mit den Notary-Servern abgeglichen. Wenn alle Server das gleiche Zertifikat sehen, kann man ohne Belästigung weiter surfen.

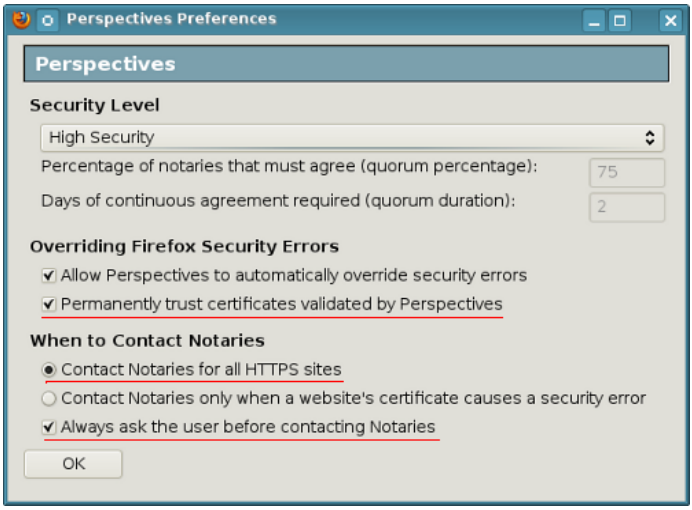


Abbildung 5.16: Perspectives zur Erkennung von man-in-the middle

Die Option *Permanetly trust certificates validated by Perspectives* und *Contact Notaries for all HTTPS sites* ist zu aktivieren. Aktiviert man auch die Option *Always ask the user...* fragt das Plugin vor jeder Validierung mit einer Informationsleiste am oberen Rand nach, bevor es die Nortary-Server kontaktiert. Das verhindert, dass die Notary-Server eine vollständige Liste der besuchten HTTPS-Websites erhalten.

5.10 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 System der Website zu erlangen. Die Passworte konnten geknackt werden. Die gleichen Account Daten 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. http://www.heise.de/ct/artikel/Ausgelacht-1195082.html
- Was ist ein starkes Passwort? Diese Frage muss man unter Beachtung des aktuellen Stand der Technik beantworten. Wörterbuch Angriffe 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** 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.

Unter https://addons.mozilla.org/de/firefox/addon/1033 steht das Plug-In zur Installation bereit.

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 https://www.pwdhash.com steht der Algorithmus auch als Javascript Applet zur Verfügung. Man kann sein Master Passwort und die Domain eingeben und erhält das generierte Login Passwort. Das kann man mit Copy & Paste in das Passwort Eingabefeld übernehmen.

5.11 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* der EEF (http://panopticlick.eff.org) zeigt, dass anhand des FIngerprint des HTTP-Headers einzelne Nutzer gut auseinander gehalten werden können. 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 Deanonymiserung möglich.

- Beispiel **Referer**: Von welcher Seite kommt der Surfer? Die Schleimspur im Internet, sehr gut geeignetet 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. Diese können manipuliert werden, um der Protokollierung und der Ausnutzung spezifischer Sicherheitslücken entgegen zu wirken.

  Ein Beispiel, welches zeigt, wie detailliert ein Browser Auskunft gibt:

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

- Ergänzende Informationen wie zum Beispiel die bevorzugte Sprache, Zeichensätze und Dateitypen können einen individuellen Fingerprint des Browsers ergeben. Die Kombination dieser Werte sollte auf möglichst häufig verwendete und nichtssagende Einstellungen gesetzt werden, beispielsweise auf das JonDoFox-Profil (für anonymes Surfen mit JAP) oder die Empfehlungen der TOR-Entwickler.

5.11.1 Plug-Ins für Mozilla Firefox

Es stehen mehrere Add-ons für diesen Browser zur Verfügung, welche jeweils eine kleine Aufgabe übernehmen. Nach der Installation findet man meist unten in der Statuszeile ein neues Symbol.

- **RefControl** modifiziert den Referer. Spezifische Einstellungen für einzelne Webeiten sind möglich. Nach der Installation des Plug-Ins sollte im Dialog *Optionen* der Standard eingestellt werden:
  1. *Ersetzen* setzt den Referer immer auf die Basisadresse der Domain. Das kann bei einigen Sites zu Problemen führen, ist nicht immer plausibel aber erschwert das Tracking innerhalb der Site.
  2. *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 von Websites einzuschränken.

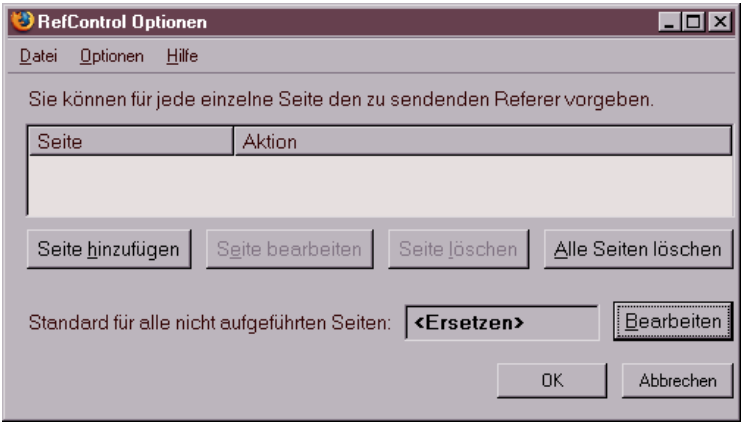


Abbildung 5.17: Einstellungen von RefControl

Das Add-on liegt bereit unter: https://addons.mozilla.org/firefox/953/.

Der **User Agent** kann unter der Adresse about:config überschrieben werden. Es ist eine neue String-Variable *general.useragent.override* mit der Kennung eines beliebigen, häufig verwendeten Browsers anzulegen. Die Auswertung des Projektes Panopticlick ergab als derzeit (Feb. 2010) häufigste Kennung:

```
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3)
Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)
```

Ob man statt en-US besser de-DE verwendet, hängt von der bevorzugten Sprache ab. Am besten testen, welche Sprache der Browser sendet.

Man sollte im normalen Betrieb nur eine veränderte Firefox-Kennung nutzen. Versucht man, einen andren Browser vorzutäuschen, kann dieser Fake leicht anhand der Anordnung der Werte im HTML-Header entlarvt werden. Jeder Browser hat eine typische Reihenfolge und Werte für die Variablen im Header.

5.12 Snakeoil für Firefox

Auf der Mozilla-Website für Add-ons findet man tausende von Erweiterungen. Wir wollen nicht alle vorstellen. Uns erreichen immer wieder Hinweise auf dieses oder jenes privacyfreundliche Add-on. Wir haben ein paar Dinge zusammengestellt, die wir nicht in unsere Empfehlungen aufnehmen.

Als Grundsicherung empfehlen wir die Kombination von CookieMonster + NoScript + AdBlock Plus + RefControl. Viele Add-ons bieten Funktionen, die von dieser Kombination bereits abgedeckt werden. Andere sind gutes Snakeoil.

Google Analytics Opt-Out

Das Add-on von Google verhindert die Ausführung der zu Google-Analytics gehörenden Scripte. Die Scripte werden jedoch trotzdem von den Google Servern geladen und man hinterlässt Spuren in den Logdaten. Google erhält die Informationen zur IP-Adresse des Surfers und welche Webseite er gerade besucht (via Referer). Außerdem gibt es über hundert weitere Surftracker, die ignoriert werden.

Die Add-ons NoScript und AdBlock erledigen diese Aufgabe besser. 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 amn 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, openstreetmap.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 nur Tracker blockiert, die der oben genannten Kombination auch bekannt sind.
- ...

Wer meint, es nutzen zu müssen - Ok. Kategorie: *harmloses Snakeoil*

6 Umgehung von Zensur

Die Zensur (Neusprech: Access-Blocking) wird in Deutschland im Namen des Kampfes gegen Kinderpornografie im Internet eingeführt. Frau von der Leyen wird nicht müde zu behaupten, es gäbe einen Millionen Euro schweren Massenmarkt, der durch Sperren von Websites empfindlich ausgetrocknet werden kann. Ihre Aussagen wurden überprüft und für falsch befunden. Für ihre Kampagne wurde sie mit dem "Big Brother" geehrt.

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, das es keinen Massenmarkt für Kinderpronografie 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 Datengrundage 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 Kinderporngraphie...*

http://blog.odem.org/2009/06/11/2009-06-11-anfrage-sperren.pdf

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 technikoffen 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 zahnloses Experten-Gemium stichprobenartig mindestens vierteljärlich 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 Subsidaritätsprinzips *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 Hoster 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 Abauf der Evaluierung soll das Ergebniss 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 Adligen 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 Zugangserschwernisgesetz endültig 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-Kommision. Alle Mitgliedsländer sollten zum Aufbau einer Sperrinfrastruktur gegen Kinderpornografie verpflichtet werden. Besonders hervorgetan als Befürworterin einer solchen Regelung hat sich Cesilia Malström, die EU-Kommisarin für innere Angelegenheiten.

Abbildung 6.1: Quelle: http://i227.photobucket.com/albums/dd41/Scoti17/Malmstrm.jp

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. Der gleiche Weg beim Zugangserschwernisgesetzt?

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 Urheberechtsverletzungen gefordert , die internationale Konferenz zum Schutz der Kinder fordert eine Zensurinfrastruktur und auch die Absicherung des staatlichen Glückspiel 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 Doamin 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 steht auf Wikileaks weiterhin zum Download zur Verfügung.)

- Das Suchmaschinen ihre Links zensieren ist seit längerem bekannt. Die bei Wikileaks aufgetauchte Sperrliste des ehemaligen Suchdienstes Lycos ist interesant.

Diese Beispiele zeigen, dass die Umgehung von Zensur oft Kreativität erfordert.

6.1 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, Dänamark, Finnland und Schweden von 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 Hoster 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 internatione 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 ds BKA zwei Jahre lang nichts unternommen?

Der lange Dienstweg des BKA

In einer Studie der Univerität Cambridge wurde untersucht, wie lange es dauert, um strafrechtlich relevante Websites zu schließen. Phishing-Websites werden innerhalb von 4 Stunden geschlossen. Bei Websites mit dokumentierten 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 dokumentierten 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 Suedeutsche 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. Zu den unhaltbaren Zuständen zählt, dass sich in Hamburg für 1450 Beamte nur 50 PC mit Internetanbindung zur Verfügung stehen.

Interessant ist, dass das BKA eine mit hohen Kosten verbundene Sperr-Infrastruktur aufbauen möchte, selbst aber nur 6,3(!) Planstellen für die Verfolgung von dok. 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.

6.2 Die Medien-Kampagne der Zensursula

Der Gesetzgebungsprozess wird von einer breiten Medien-Kampagne begleitet. Die Gegner der Zensur werden direkt und indirekt als Pädophile oder deren Helfer verunglimpft, es wird ein Gegensatz von "Meinungsfreiheit im Internet" versus "Schutz der Kinder" konstruiert und es wird 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 von und zu Guttenberg ist in letzter Zeit auch wegen undurchsichtiger Geschäftsgebaren und undokumentierter Verwendung von Spendengeldern in öffentliche Kritikik geraten.

In den Mainstream-Medien wird die Argumentation der Befürworter der Zensur prominent und ohne kritische Nachfrage wiedergegeben. Einige Beispiele:

> *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 Kinderpornos im Internet haben können...* (S. Raabe, SPD)

Das Motto der Gegner der Zensur im Internet lautet **Löschen statt Sperren**. Das steht auch deutlich in der von Franziska Heine initiierten Petition und wurde auf dem Piraten-Parteitag ebenfalls deutlich gesagt.

> *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 romatische 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 nenneswerte Infrastruktur, um Webserver zu betreiben.

> *Wer die Stoppseite 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.

6.3 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 polizeilche 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.

6.4 Simple Tricks

Die *Simple Tricks* wurden bereits an der "Great Firewall" in China erprobt und sind teilweise recht erfolgreich. Das einfache Prinzip ist im Bild 6.2 dargestellt.

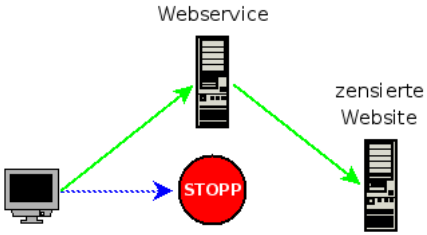


Abbildung 6.2: Prinzip der Simple Tricks

Wenn man auf eine Website nicht zugreifen kann (oder man befürchtet, nicht zugreifen zu können) kann man ein 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. Eine Liste von

Web-Proxies mit SSL-Verschlüsselung findet man auf http://proxy.org oder http://www.mamproxy.com.

Web-Proxys sind ein geeignetes Mittel, um Speren im Internet zu umgehen. Sie sind jedoch *keine Anonymisierungsdienste*. Wer anonym surfen will, sollte JonDonym oder Tor nutzen.

3. **Übersetzungsdienste:** Man fordert bei einem Web-Translater die Übersetzung einer Website von einer willkürlichen Sprache (z.B. koreanisch) in die Orginalsprache des Dokumentes an. Der Web-Translater 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 Surfen. 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, unaufällig 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 für einfache Webseiten.
   - frames(ÄT)pagegetter.com für Webseiten die aus mehreren Framen bestehen.
   - HTML(ÄT)pagegetter.com liefert die Webseite ohne grafische Elemente aus.

6.5 Unzensierte DNS-Server nutzen

Am 17.04.09 unterzeichneten diese Provider einen geheimen Vertrag mit dem BKA, in welchem sie sich verpflichten, eine vom BKA bereitsgestellte Liste von Websites durch Kompromittierung des DNS-Systems zu sperren.

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 eine sichere Lösung, unzensierte DNS-Server zu nutzen. Vodafone leitet bereits seit Juli 09 im UMTS-Netz DNS-Anfragen auf die eigenen, zukünftig zensierten 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) lehnen 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 beschrieben 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 Webservers, 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 Webservers 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. Die GPF betreibt einige unzensierte DNS-Server. Unsere DNS-Server können auch auf Port 110 angefragt werden, falls einige Provider den DNS-Traffic auf Port 53 zum eigenen Server umleiten oder behindern. Außerdem bieten unsere Server HTTPS-DNS, um den Traffic verschlüsselt an den Providern vorbei zu leiten.

```
87.118.100.175   (DNS-Ports: 53, 110)
62.75.219.7      (DNS-Ports: 53, 110, HTTPS-DNS)
94.75.228.29     (DNS-Ports: 53, 110, HTTPS-DNS)
```

Die Swiss Privacy Foundation stellt folgende unzensierten DNS-Server:

```
62.141.58.13     (DNS-Ports: 53, 110, HTTPS-DNS)
87.118.104.203   (DNS-Ports: 53, 110)
87.118.109.2     (DNS-Ports: 53, 110)
```

Der FoeBud bietet einen unzensierten DNS-Server:

```
85.214.73.63
```

Und der CCC hat natürlich auch einen Unzensierten:

```
213.73.91.35
```

Bei ValiDOM gibt es zwei weitere DNS-Server:

```
78.46.89.147
88.198.75.145
```

6.5.1 WINDOWS konfigurieren

Wir bezweifeln, das es zur Umgehung der Zensur ausreicht, einfach einen unzensierten 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 unzensierter DNS-Server kann relativ einfach unterbunden werden. Vodafon 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 6.3 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.

6.5.2 Linux konfigurieren

Unter Linux sind nichts-standardmäßige Einstellungen leichter realiserbar. Es ist auch relativ einfach, einen lokalen DNS-Cache zu nutzen, um die 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 Unbuntu installiert man ihn zusammen mit *resolvconf*:

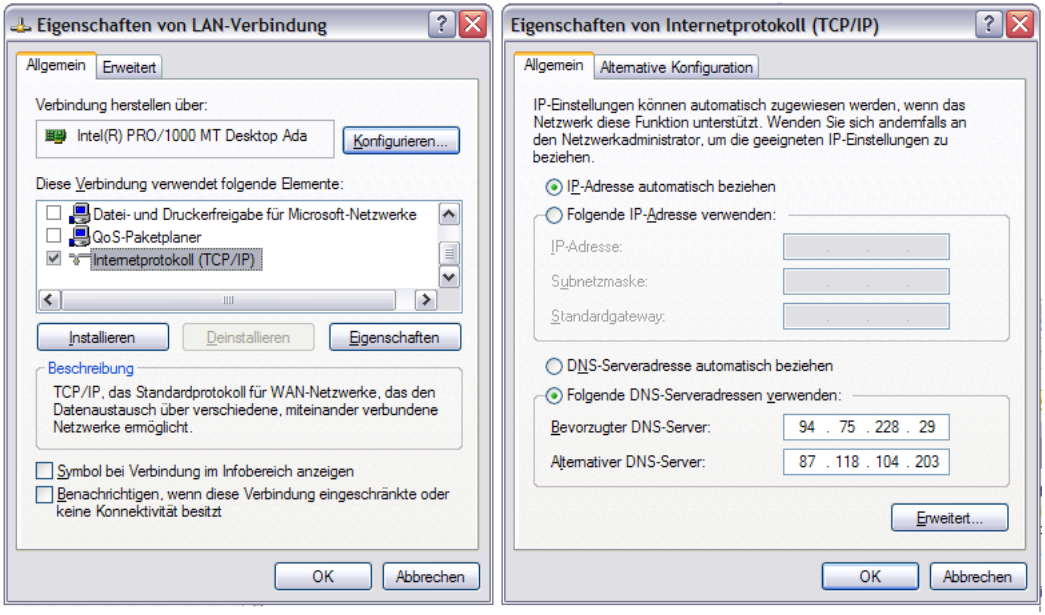


Abbildung 6.3: Konfiguration der DNS-Server (WINDOWS)

```
> 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 vorbereitet 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 bietet 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 gstoppt 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.opions* 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.opions"* oder *"gksu gedit /etc/bind/named.conf.opions"* probieren.

Nach der Anpassung der Konfiguration ist *bind9* mitzuteilen, das er die Konfigurationsdateinen neu laden soll:

```
> sudo invoke-rc.d bind9 reload
```

6.5.3 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 einfachen 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.

6.5.4 HTTPS-DNS nutzen

Mit der Anwendung der Zensur auf DNS-Server ist eine Sperrung von freien DNS-Server zu erwarten oder eine Umleitung des DNS-Traffics auf zensierte Server der Provider. Um eine zuverlässige Umgehung der DNS-Sperren zu ermöglichen, haben wir das Projekt HTTPS-DNS initiert.

Die Abbildung 6.4 zeigt das Prinzip von HTTPS-DNS. Die DNS-Daten werden per HTTPS verschlüsselt an den Zensur Providern vorbei geleitet. Ein HTTPS-DNS-Server stellt eine unzensierte Auflösung der DNS-Namen sicher. Das Projekt ist als Ergänzung zu Anonymisierungsdiensten gedacht. (https://www.privacyfoundation.de/wiki/HTTPS-DNS)

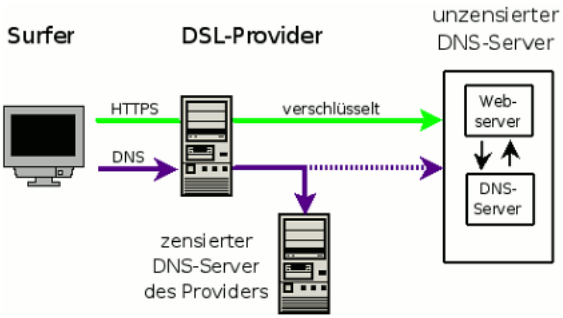


Abbildung 6.4: Prinzip von HTTPS-DNS

Software für Anwender

Das Projekt steht erst am Anfang der Entwicklung. Die Software ist längst nicht perfekt, funktioniert aber ganz gut. Sollte man unzufrieden sein, deinstalliert man die Software mit der Paketverwaltung des Systems wieder, es wird alles sauber entfernt. Über Unterstützung bei der Weiterentwicklung würden wir uns freuen.

Debian GNU/Linux und Ubuntu: Ein DEB-Paket steht in unserem Repository zur Nutzung bereit. (siehe https://www.awxcnx.de/wabbel.htm) Es wird der DNS-Cache-Daemon pdnsd als Cache genutzt, um die Antwortzeiten zu minimieren und die Server zu entlasten. Bei der Installation werden Optionen für die Konfiguration des *pdnsd* angegeben. Es ist egal, welche Option sie wählen. Die Konfiguration wird vom *https-dns-client* überschrieben.

Um Probleme mit *resolvconf* zu vermeiden, sollte man die nötigen Pakete einzeln installieren, nicht glichzeitig.

```
> sudo aptitude install resolvconf
> sudo aptitude install pdnsd
> sudo aptitude install https-dns-client
```

Die Install-Routine richtet alles fertig ein und konfiguriert das System. In Zukunft gehen alle DNS-Anfragen HTTPS-verschlüsselt an den Providern vorbei. Man kann mit Aufruf der Test-Adresse http://welcome.httpsdns prüfen, ob es funktioniert.

MacOS X: Für dieses Betriebssystem gibt es ein fertiges Paket in unserem Wiki https://www.privacyfoundation.de/wiki/HTTPS-DNS unter Software für Clients. Nach der Installation muß nur noch in den Systemeinstellungen unter *Netzwerk* der DNS-Server 127.0.0.1 eingetragen werden. Danach im Browser http://welcome.httpsdns aufrufen, um die Einstellungen zu prüfen.

WINDOWS: dafür haben wir noch keine fertige Lösung.

Kleine Optimierungen für Firefox

Bei der Nutzung von HTTPS-DNS kommt es zu geringen Verzögerungen bedingt durch das komplexere Protokoll und die nicht optimale Umsetzung in den ersten Versionen der Clients. Man kann durch kleine Anpassungen im Mozilla Firefox die Verzögerungen reduzieren.

In der Regel hat man am DSL-Anschluss kein IPv6 zur Verfügung. Unter der Adresse about:config kann man die Nutzung von IPv6 deaktivieren. Damit versucht Firefox nicht immer wieder, zuerst eine IPv6 Adresse via DNS zu erhalten, die Anzahl der DNS-Anfagen halbiert sich.

```
network.dns.disableIPv6    true
```

7 Allgemeine Hinweise zur E-Mail Nutzung

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

7.1 Mozilla Thunderbird

Informationen und Downloadmöglichkeiten für Mozilla Thunderbird stehen auf der deutschsprachigen Website des Projektes unter www.thunderbird-mail.de/ zur Verfügung. Linux Distributionen enthalten in der Regel Thunderbird. Mit der Packetverwaltung kann Thunderbird und die deutsche Lokalisierung komfortabel installiert und aktualisiert werden. Debian GNU/Linux bietet eine angepasste Version von Thunderbird unter dem Namen *Icedove*.

Nach dem ersten Start von Thunderbird führt ein Assistent durch die Schritte zur Einrichtung eines E-Mail Kontos. Nacheinander werden die E-Mail-Adresse sowie die Server für den Empfang und das Versenden von E-Mails abgefragt. Es können auch die Einstellungen eines bisher verwendeten Programms übernommen werden.

Danach sollte man sich einen Moment Zeit nehmen, um die folgenden erweiterten Features von Thunderbird zu konfigurieren.

7.1.1 Wörterbücher installieren

Nach der Installation einer lokalisierten Version von Thunderbird sind die Wörterbücher für die Standardsprache in der Regel bereits vorhanden. Für alle weiteren Sprachen können die nötigen Wörterbücher zusätzlich installiert werden. Diese stehen unter *http://www.thunderbird-mail.de/* zum Download zur Verfügung.

Nach dem Download ist Thunderbird als Administrator zu starten. Der Menüpunkt *Extras -> Erweiterungen* öffnet den Dialog für die Verwaltung der Plug-Ins. Hier ist der Button *Installieren* zu wählen und in dem sich öffnenden Dateidialog sind die gespeicherten Wörterbücher auszuwählen. Die installierten Wörterbücher erscheinen nicht in der Liste der Plug-Ins.

Nutzer von OpenOffice.org können die Wörterbücher dieser Office-Suite verwenden und müssen sie nicht erneut herunterladen. Für die deutsche Rechtschreibprüfung sind die Dateien *de_DE.aff* und *de_DE.dic* aus dem Unterverzeichnis *share/dict/ooo* der OpenOffice.org Installation in das Unterverzeichnis *components/myspell* der Thunderbird Installation zu kopieren und in *de-DE.aff* sowie *de-DE.dic* umzubenennen.

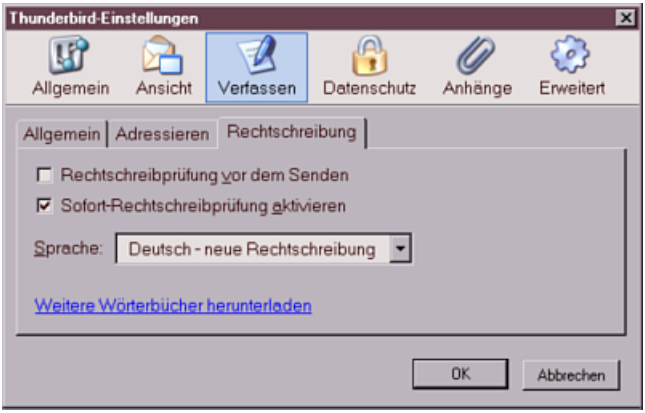


Abbildung 7.1: Sprache für Rechtschreibung wählen

Im Anschluss ist im Einstellungsdialog in der Sektion *Verfassen* die gewünschte Default-Sprache für das Schreiben von E-Mails auszuwählen und die von einer Textverarbeitung gewohnten Funktionen zur Rechtschreibprüfung stehen auch in Thunderbird zur Verfügung.

7.1.2 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.

7.1.3 Gesicherte Verbindungen zum Mail-Server

Die Grafik im Bild 7.2 zeigt den Weg einer E-Mail vom Sender zum Empfänger.

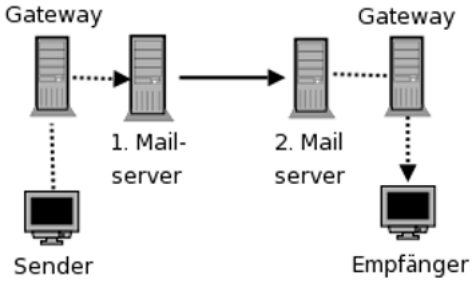


Abbildung 7.2: Der Weg einer E-Mail durch das Web

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 abruft. 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 Möglichkeit des weltweiten Zugriffs auf seine Mails erkauft der Nutzer sich jedoch mit einer Einschränkung des Datenschutzes. (siehe http://blog.kairaven.de/archives/1060-Unsichere-und-geschuetzte-E-Mail-Sphaeren.html).

Die im Bild 7.2 gestrichelten 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.

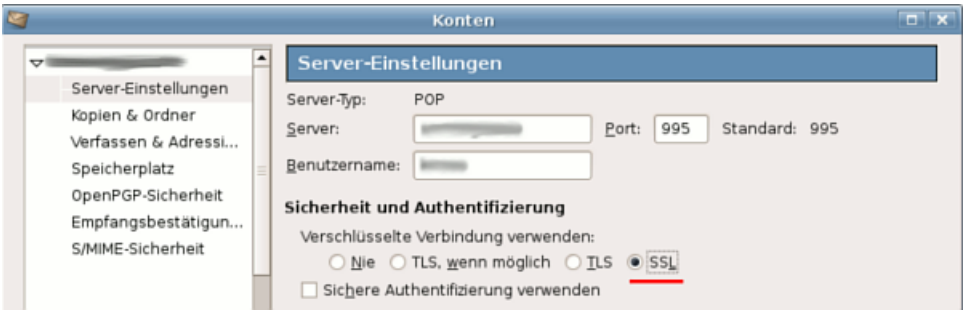


Abbildung 7.3: Konfiguration für das Abrufen von Nachrichten

Wie einfach es ist, ungesicherte Verbindungen zu belauschen, die Passwörter zu extrahieren und das Mail-Konto zu kompromittieren, wurde auf der re:publica 2008 demonstriert.

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. (http://www.heise.de/security/news/meldung/116073) 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.

Fast alle Mail-Server bieten Optionen zur verschlüsselten Kommunikation mit dem E-Mail Client. Diese Option ist in Thunderbird nach der Einrichtung eines neuen Kontos zu aktivieren. Die Einstellungen des POP3-Servers findet man in dem Dialog *Konten...* im Unterpunkt *Server-Einstellungen* des Kontos (Bild 7.3). In der Regel unterstützen POP3-Server die SSL-Verschlüsselung.

Ebenfalls im Dialog *Konten...* findet man die Einstellungen für die SMTP-Server (ganz untern). In der Liste der Server ist der zu modifizierende Server auszuwählen und auf den Button *Bearbeiten* zu klicken. In dem sich öffnenden

Dialog kann eine Option zur verschlüsselten Versendung gewählt werden.

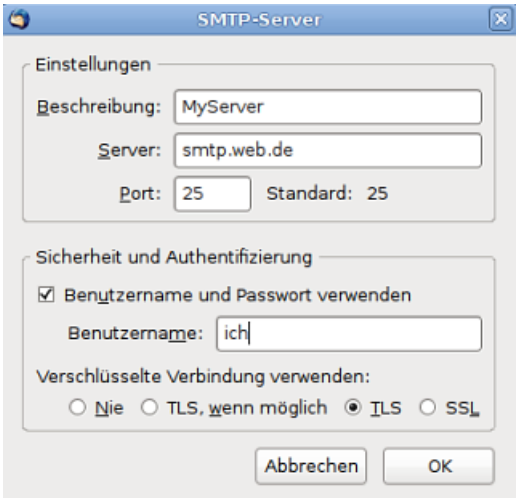


Abbildung 7.4: Konfiguration für den SMTP-Server

Viele SMTP-Server bieten neben TLS-Verschlüsselung für Port 25 auch auf den Ports 587 (submission, TLS) oder 465 (SMTP-SSL) verschlüsselte Verbindungen für das Senden von E-Mails. Diese Ports muss man bei der Verwendung von Anonymisierungsdiensten wie Tor oder JonDonym nutzen, da diese Dienste den Port 25 aus Gründen des Spam-Schutzes in der Regel sperren.

7.1.4 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 Bestarium 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.

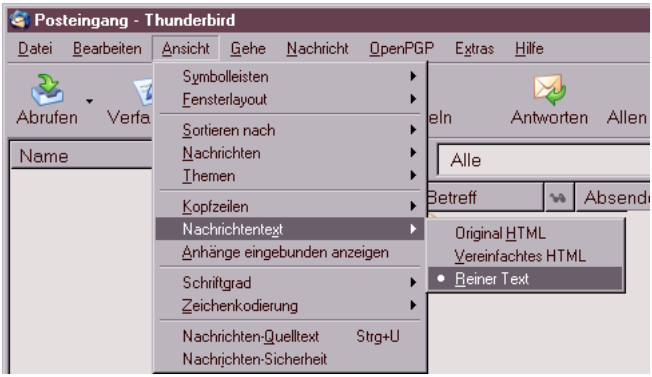


Abbildung 7.5: Ansichten als reien Text darstellen

Die Option findet man im Menüpunkt *Ansicht -> Nachrichtentext* (siehe Bild 7.5). Wer auf grafischen Schnick nicht ganz verzichten will, wählt die Option *Vereinfachtes HTML*. In diesem Fall werden nur HTML Tags für das Layout interpretiert, beispielsweise Fettdruck oder Tabellen.

- Die Option *Anhänge eingebunden anzeigen* im Menü *Ansicht* sollte man ebenfalls deaktivieren, um das gefährlicher Anhänge nicht schon beim Lesen einer E-Mail automatisch zu öffnen.

- Das Laden externer Grafiken ist zu blockieren. Häufig wird dieses Feature von Spammern zu Beobachtung des Nutzers eingesetzt. Die Option findet man im Dialog *Einstellungen* in der Sektion *Datenschutz* auf dem Reiter *Allgemein*.

- Gespeicherte Passwörter für den Zugriff auf SMTP-, POP- oder IMAP-Server sollten mit einem Masterpasswort vor Unbefugten geschützt werden (siehe Bild 7.6).

7.1.5 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.

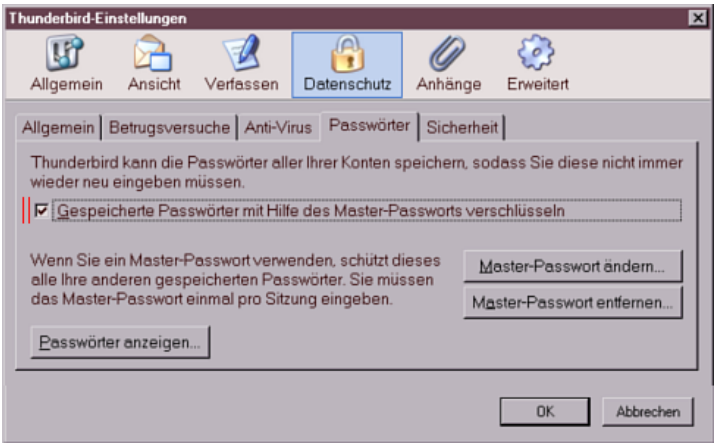


Abbildung 7.6: Masterpasswort festlegen

- 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 7.7). Bei jedem Start prüft Thunderbird, ob die Ordner komprimiert werden können.
- Regelmäßig sollten Backups des gesamten Profils von Thunderbird angelegt werden. Unter WINDOWS sichert man *C:/Dokumente und Einstellungen/<NAME>/Anwendungsdaten/Thunderbird*, unter Linux ist *$HOME/.thunderbird* zu sichern.

7.1.6 X-Mailer Kennung modifizieren

Wir haben gelesen, dass es kriminelle Elemente gibt, die via Internet ihre Software auf fremden Rechnern installieren möchten. In diesem Zusammenhang

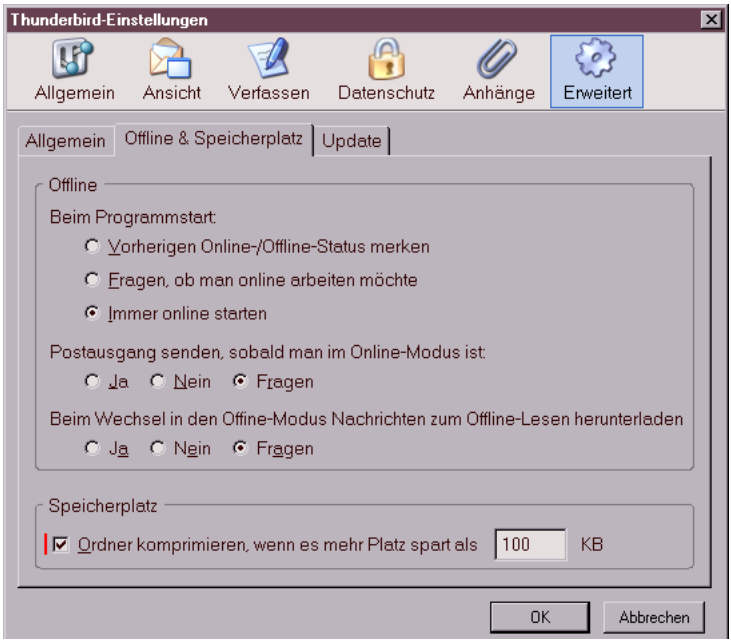


Abbildung 7.7: Ordner automatisch komprimieren

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.

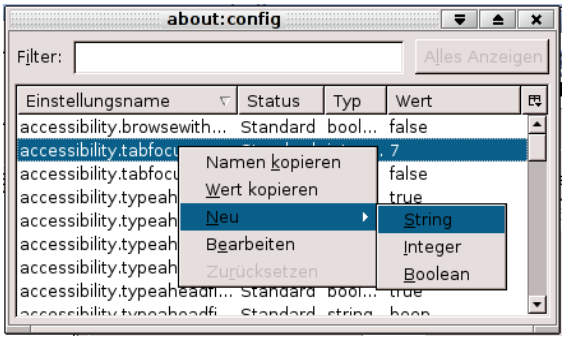


Abbildung 7.8: Neue Config-Variable anlegen

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.

Man kann auf eine beachtliche Auswahl an Kennungen für die Variable *general.useragent.override* zurückgreifen. Da jeder E-Mail Client einen typischen Aufbau des Headers verwendet, sollte man für einen plausiblen Fake nur Kennungen von Thunderbird Versionen verwenden. (Da auch Spam-Scanner diese Informationen analysieren, bleibt eine Mail mit einem Outlook-Fake eher im Junk hängen.)

```
Thunderbird 2.0.0.24 (Windows/20100228)

Mozilla-Thunderbird 2.0.0.24 (X11/20100329)

Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.1.8)
Gecko/20100227 Thunderbird/3.0.3
```

```
Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.1.9)
Gecko/20100330 Shredder/3.0.4

Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.1.15)
Gecko/20101027 Lightning/1.0b1 Thunderbird/3.0.10

Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.2.15)
Gecko/20110303 Thunderbird/3.1.9

Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.14)
Gecko/20110223 Thunderbird/3.1.8

Mozilla/5.0 (X11; U; Linux i686; de; rv:1.9.2.15) G
ecko/20110303 Lightning/1.0b2 Thunderbird/3.1.9

Mozilla/5.0 (Windows; U; Windows NT 6.0; de; rv:1.9.2.15)
Gecko/20110303 Lightning/1.0b2 Thunderbird/3.1.9
```

Wer die Erweiterung Enigmail für die Verschlüsselung nutzt, sollte dieser Erweiterung die Geschwätzigkeit abgewöhnen und die Ausgabe von Versionen im Header deaktivieren. Die Variable *extensions.enigmail.addHeaders* ist in den erweiterten Optionen auf *false* zu setzen!

Außerdem sind in den Einstellungen von Enigmail für GunPG folgende zusätzliche Optionen einzutragen, welche die Ausgabe der GnuPG-Version unterbinden:

```
--no-emit-version
```

Anderenfalls sieht ein Schnüffler an einer signierten oder verschlüsselten E-Mail, dass nicht MacOS genutzt wird, sondern evtl. Linux oder WINDOWS.

7.1.7 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"*.

10min Mail-Adresse

Unter www.10minutemail.com kann man mit einem Klick eine E-Mail Adresse anlegen, die für 10min gültig ist. Das reicht, um sich in einem Forum anzumelden. Bei Bedarf kann die Verfügbarkeit der E-Mail Adresse in Schritten von 10min verlängert werden.

Um eine 10minuten Adresse zu nutzen, öffnet man als erstes die Webseite *www.10minutemail.com* im Browser. Cookies und Javascript sind für diese Website freizugeben. Danach öffnet man in einem neuen Browser Tab die Seite für die Anmeldung im Forum oder Blog. Hier überträgt man mit Copy&Paste die 10minuten Mail Adresse und sendet das Formular ab. Dann wechselt man zurück in den Browser Tab von *www.10minutemail.com* und wartet auf die eingehende Bestätigungsmail. In der Regel einhält diese Mail einen Link zur Verifikation. Auf den Link klicken - fertig.

AnonBox des CCC

Die AnonBox (https://anonbox.net) ist ein ähnliches Projekt wie 10minutemail. Auf der Webseite 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 Nachrichte werden nach dem Abrufe gelöscht. Sie können nur 1x gelesen werden!

Die AnonBox bietet als einziges Projekt HTTPS-Verschlüsselung.

6-12h Mail-Adressen

Einige Anbieter von Wegwerf-E-Mail-Adressen bieten einen sehr einfach nutzbaren Service, der keinerlei Anmeldung efordert. E-Mail Adressen der Form *pittiplatsch@trash-mail.com* oder *pittiplatsch@emaildienst.de* kann man

überall und ohne Vorbereitung angeben.

Liste einiger Anbieter (unvollständig):

- http://www.sofort-mail.de
- http://www.trash-mail.com
- http://dodgit.com
- http://www.mailinator.com/

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 und löschen.

Alle eingegangenen Nachrichten werden nach 6-12h 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 Addon Bloody Vikings

Das Firefox Addon Bloody Vikings vereinfacht die Nutzung von Wegwerfadressen. Nach der Installation von der Webseite kann ein bevorzugter Dienst für die Wegwerfadressen gewählt werden.
https://addons.mozilla.org/de/firefox/addon/261959/
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.

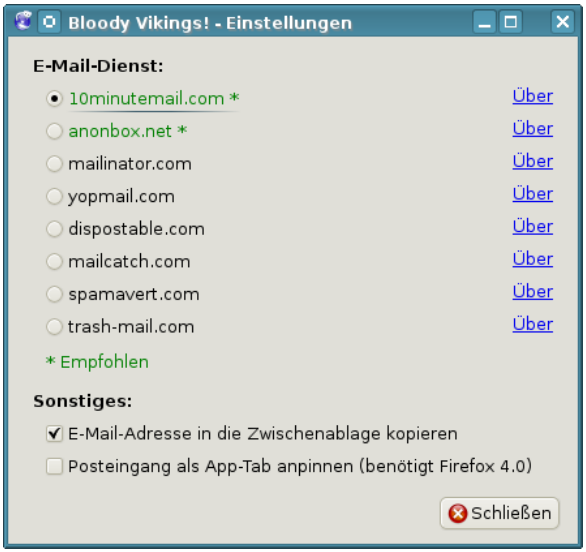


Abbildung 7.9: Bloody Vikings konfigurieren

8 E-Mails verschlüsseln

Der Einsatz kryptographischer Methoden ist insbesondere für die Kommunikation via E-Mail sinnvoll. Das europäische Verbraucheramt in Kiel, das BSI sowie der Bundesdatenschutzbeauftragte empfehlen die breite Nutzung folgender Methoden:

- **Signieren** von E-Mails: Eine vom Absender erstellte Signatur ermöglicht es dem Empfänger, die Identität des Absenders zu prüfen und gewährleistet, dass die E-Mail nicht verändert wurde.
- **Verschlüsseln** von E-Mails: Es wird die Vertraulichkeit der Kommunikation gewährleistet. Eine Nachricht kann nur vom Empfänger geöffnet und gelesen werden.

Mit OpenPGP und S/MIME haben sich zwei Standards für diese Aufgaben 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.

Beide Standards nutzen **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 Kommunikationpartner 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.

8.1 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:

8.1.1 Installation von GnuPG

WINDOWS-User finden Binärpakete mit grafischer Installationsroutine auf der Website http://gnupg.org/download/index.en.html weiter unten im Abschnitt *Binaries*. Das Setup-Archiv ist nach dem Download mit den Rechten des Administrators zu starten.

Wir empfehlen das Paket **GnuPG-Pack**, welches einige zusätzliche Tools enthält wie WinPT Tray, GPGrelay, Enigmail und GPGSX. Mit GPGol soll auch Outlook die Verschlüsselung nutzen können. Das Paket steht unter http://home.arcor.de/rose-indorf/ zum Download bereit.

Nach dem Download ist das ZIP-Archiv zu entpacken. Das Setup-Programm (EXE-Datei) ist zu starten und den Anweisungen zu folgen. Nach Bestätigung der Lizenzbedingungen usw. kann man die zu installierenden Komponenten auswählen (Bild 8.1).

Ob man WinPT für die Verschlüsselung via Zwischenablage benötigt, kann man selbst entscheiden. Für Thunderbird benötigt man das Enigmail Add-on. Außerdem sollte man die Erweiterung für den Explorer GPGSX mit installieren. Das vereinfacht die Ver- und Entschlüsselung von Dateien mit einem Klick im Explorer.

In einem weiteren Schritt werden verschiedene Zusatzfeatures angeboten. Statt der vorgeschlagenen Verschlüsselung der GPG-Schlüsselringe mit dem Windows Encrypt Filesystem empfehlen wir die komplette Verschlüsselung der Festplatte. Damit kann diese Option deaktiviert werden.

8.1.2 Installation der Enigmail-Erweiterung

Enigmail ist eine Erweiterung für Thunderbird, welche den Einsatz von GnuPG im täglichen E-Mail-Chaos vereinfacht. Die aktuelle deutsche Version steht unter https://addons.mozilla.org/de/thunderbird/addon/71 zum Download zur Verfügung:

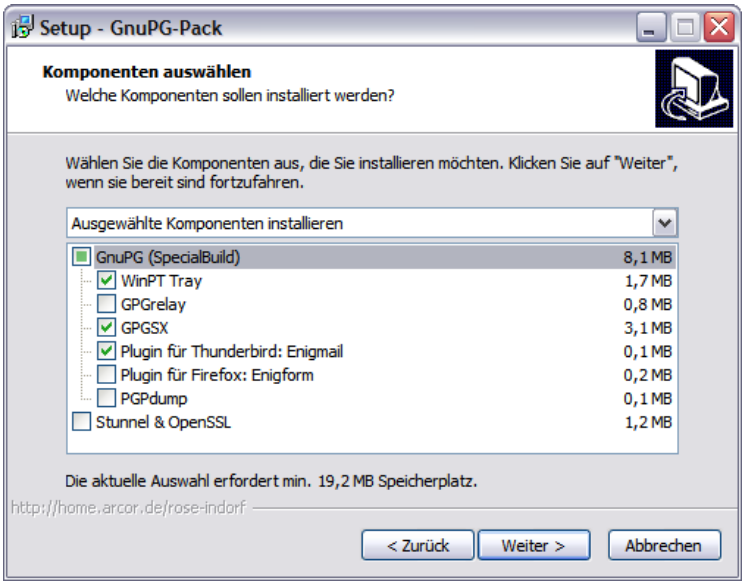


Abbildung 8.1: Komponenten des GnuPG-Pack zur Installation auswählen

Nutzer der Mozilla-Browser sollten nicht mit der linken Maustaste auf den Download-Link klicken. Statt dessen ist mit der rechten Maustaste auf den Downloadlink zu klicken und im Kontextmenü der Punkt *Ziel speichern unter* zu wählen.

Nach dem Download ist Thunderbird zu starten und der Dialog zur Verwaltung der Erweiterungen über den Menüpunkt *Extras / Erweiterungen* zu öffnen. Hier wählt man den Button *Installieren* und in dem sich öffnenden Dateidialog das gespeicherte Plug-In (.xpi).

Nach Installation von Enigmail muss Thunderbird neu gestartet werden. Es wird der **Assistent** zur Einrichtung von Enigmail ausgeführt, der folgende Schritte durchläuft:

1. Abfrage, für welche Konten die Funktionen zur Verschlüsselung aktiviert werden sollen (in der Regel alle).

2. Abfrage, ob gesendete E-Mails standardmäßig signiert und verschlüsselt werden sollen. Um unbedarfte Anwender nicht zu verwirren, kann man

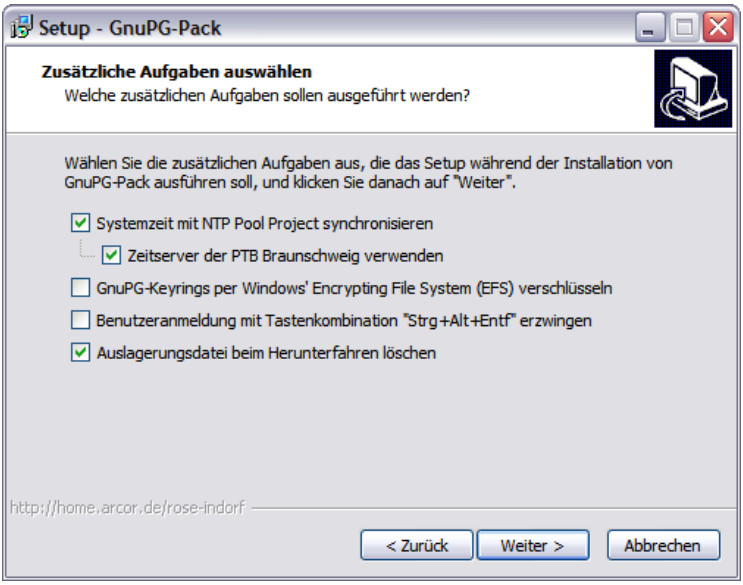


Abbildung 8.2: Weitere Features vom GnuPG-Pack

das Signieren deaktivieren.

3. Optimierung der Einstellungen für GnuPG. Die Vorgaben sind sinnvoll und sollten übernommen werden.

4. Generieren der Schlüsselpaare für alle im Schritt 1 ausgewählten 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.

   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

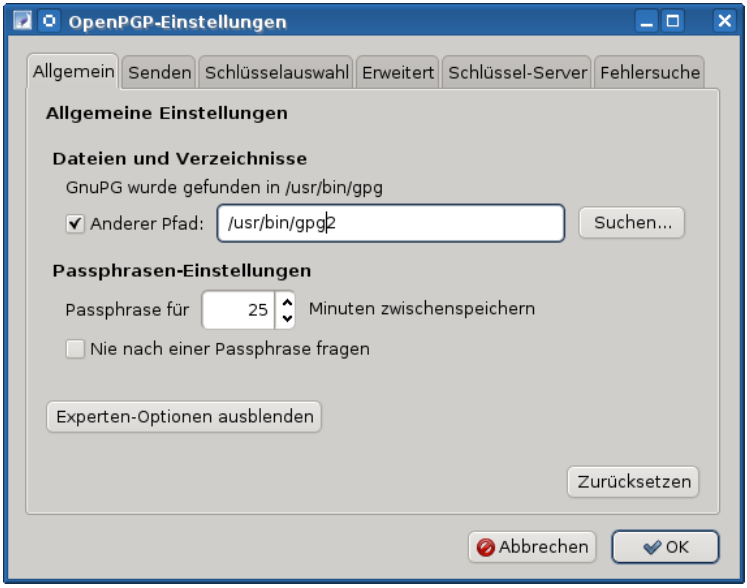


Abbildung 8.3: Einstellungen von EnigMail

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 (Bild 8.3).

8.1.3 Schlüsselverwaltung

Die Schlüsselverwaltung findet man in Thunderbird unter dem Menüpunkt *OpenPGP / Schüssel verwalten*. Ist die Liste noch leer, wählt man zuerst den

Menüpunkt *Erzeugen / Neues Schlüsselpaar*. Diesen Schritt übernimmt jedoch der Assistent zur Einrichtung von EnigMail.

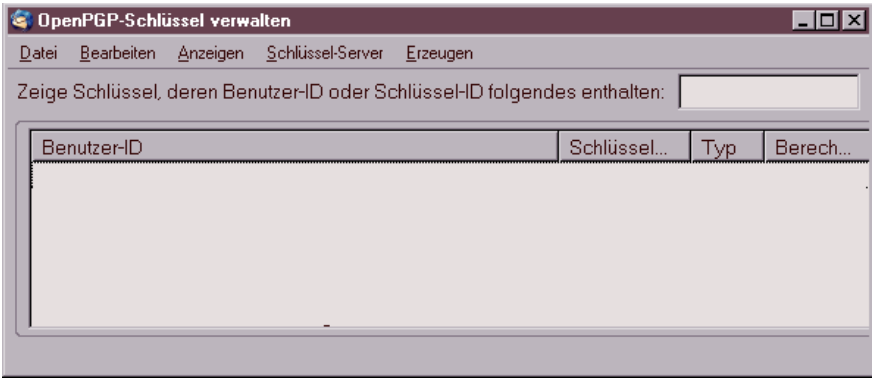


Abbildung 8.4: Schlüsselverwaltung von EnigMail

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 in eine Datei exportieren und diese Datei anschließend als E-Mail-Attachment versenden oder auf einem Webserver ablegen. Den Menüpunkt für den Export in eine Datei findet man unter *Datei / Schlüssel exportieren* in der Schlüsselverwaltung.

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 Schlüsselserver zu importieren.

- Zum Importieren des Schlüssel eines Partners aus einer Datei, die man als Attachement oder per Download erhalten hat, wählt man den Menüpunkt *Datei / Importieren*

- Auch ohne eine signierte E-Mail erhalten zu haben, kann man die Schlüsselserver 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 die Suchanfrage 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 die Auswahl mit OK.

8.1.4 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 8.5) zeigt nach der Installation des Enigmail-PlugIns einen neuen Button *OpenPGP*. Klickt man auf diesen Button, öffnet sich der im Bild 8.5 gezeigte Dialog, der es 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

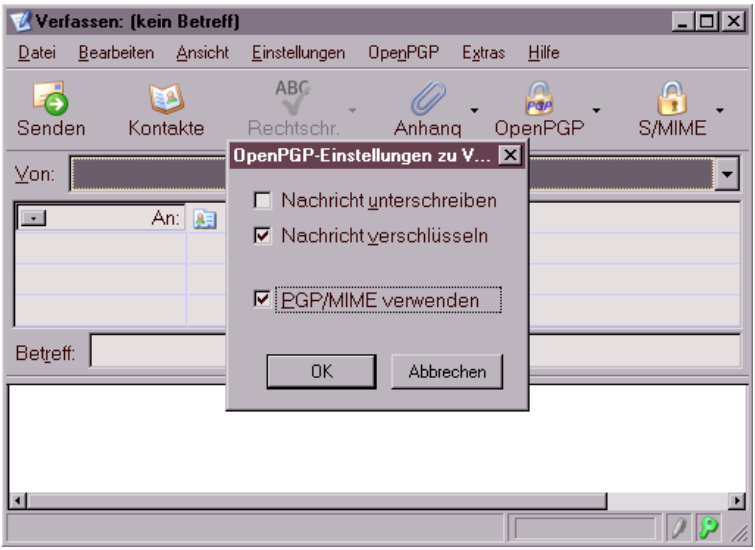


Abbildung 8.5: Signieren und Verschlüsseln einer E-Mail

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.

8.1.5 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 GUIs für GnuPG (z.B. 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 in

umgekehrter Reihenfolge.

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** (http://gpg4usb.cpunk.de) 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 ApplikationPortable PGP http://ppgp.sourceforge.net ist eine Java-Anwendung (plattformunabhängig), die ebenfalls Texte und Dateien ver- und entschlüsseln kann. Eine einfach Schlüsselverwaltung ist ebenfalls enthalten. Zusätzlich zu Portable PGP benötigt man eine Java Laufzeitumgebung. Eine portable Version der Sun-JRE gibt es bei portableapps.com.

Ein Plug-In für Firefox

Für Firefox und Iceweasel gibt es das Plug-In **FireGPG**. Es ver- und entschlüsselt Text in Webformularen mit GnuPG. Die Installation erfolgt wie üblich mit einem einfachen Klick auf den Download Button. (Man muss der Website die Installation des Plug-In explizit erlauben, da es nicht die Mozilla Website ist.) Projektseite: https://addons.mozilla.org/de/firefox/addon/4645

Nach einem Neustart des Browsers findet man im Kontextmenü (rechter Mausklick) einer Textbox einen zusätzlichen Punkt *FireGPG* mit den üblichen Untermenüs: verschlüsseln, signieren, entschlüsseln...

Verschlüsseln und Signieren: Es ist der gesamte Text in der Eingabebox zu markieren (<Strg>-A) und anschließen der entsprechende Menüpunkt aus dem FireGPG Menü zu wählen. Schwupp - es steht der verschlüsselte oder signierte Text in der Box.

Entschlüsseln: Der zu entschlüsselnde Text ist zu markieren (meist reicht ein <Strg>-A) und das dem FireGPG-Untermenü der Punkt *entschlüsseln* zu wählen. Im integrierten Editor wird der entschlüsselte Text angezeigt und kann bei Bedarf auch als Datei gespeichert werden.

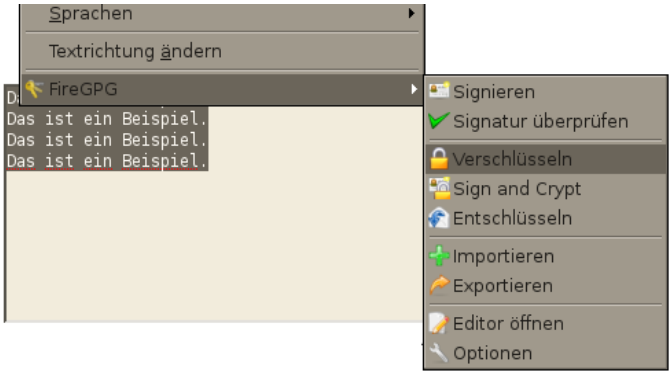


Abbildung 8.6: FireGPG Menü

Leider wird FireGPG nicht mehr weiterentwickelt und wird nicht für Firefox 4.0 zur Verfügung stehen.

8.1.6 GnuPG SmartCard nutzen

Die Sicherheit asymmetrischer Verschlüsselung hängt in hohem Maße von der sicheren Aufbewahrung des privaten Keys ab. Nutzt man GnuPG auf mehreren Rechnen, 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* 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.

CryptoStick: Da das Handling mit CardReader und SmartCard unter Um-

ständen etwas umständlich sein kann, wird in der GPF 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. Projektseite: http://wiki.privacyfoundation.de/GPFCryptoStick

Abbildung 8.7: CryptoStick der GPF

Hardware-Treiber installieren

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

- 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 der GPF gibt es den PC Twin USB PC/SC Treiber. Download Links: https://www.awxcnx.de/handbuch_32r.htm

- 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 libpcsclite1 libccid
  ```

Für den CryptoStick v1.2 benötigt man keine Treiber, sondern nur eine UDEV-Regel. Für Debian/Ubuntu steht das Paket *cryptostick-1.0_all.deb* in unserem Repository bereit. Für alle anderen Distributionen ist die Datei *40-cryptostick.rules* nach dem Download in */etc/udev/rules.d* zu speichern. Download Links: https://www.awxcnx.de/handbuch_32r.htm

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

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 ...: D27600xxxxxxxxxxxxxx
Version ..........: 2.0
Manufacturer .....: unknown
....
```

SmartCards und CryptoStick mit Enigmail nutzen

Enigmail ist ab der Version 1.0.1 voll kompatibel mit der SmartCard und dem CryptoSick. Aktuelle Linux-Versionen enthalten in der Regel eine ältere Version in den Repositories. Wer diese Pakete installiert hat, sollte sie wieder entfernen und eine aktuelle Enigmal Version von der Mozilla Addon Website installieren. Für Thunderbird 2.0.x kann auch Enigmail 0.96 genutzt werden. Evtl. muss man die SmartCard oder CryptoStick auf der Kommandozeile administrieren (siehe unten).

Das Plug-In bietet eine grafische Oberfläche, um die SmartCard zu verwalten. Diese Funktionen öffnet man über den Menüpunkt *OpenPGP - Smartcard verwalten*.

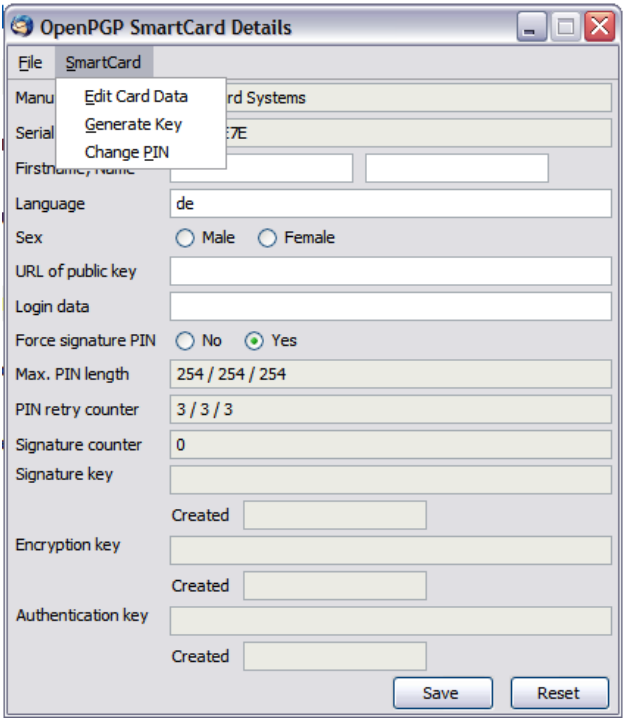


Abbildung 8.8: SmartCard verwalten

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 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.

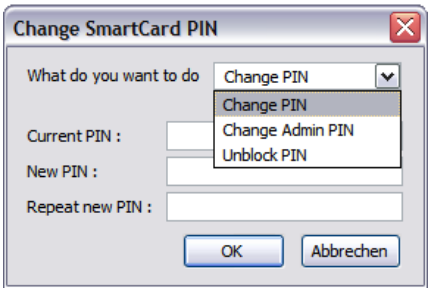


Abbildung 8.9: SmartCard-PINs ändern

3. Als letzten Schritt vor der Nutzung der SmartCard im täglichen Krypto-Chaos sind die Keys auf der SmartCard zu generieren. Der entsprechende Dialog bietet die Auswahl eines Mail-Account an, für den die SmartCard genutzt werden soll. Für diesen Account darf kein(!) OpenPGP-Key vorhanden sein. Anderenfalls bricht der Vorgang mit einer wenig verständlichen Fehlermeldung ab.

   Es sollte unbedingt bei der Erzeugung des Schlüssels ein Backup der Card-Keys angelegt und mit einem Passwort gesichert werden. Später ist kein Zugriff auf diese Schlüssel mehr möglich. Bei Beschädigung der SmartCard kann der gesicherte Card-Key in eine neue SmartCard importiert werden. Das Backup wird im GnuPG-Verzeichnis abgelegt und ist auf einem sicheren Datenträger zu speichern!

   Wurden die Schlüssel erfolgreich generiert, findet man in der *Schlüsselverwaltung* ein neues Paar. Der Public Key dieses Schlüsselpaares kann wie üblich exportiert und den Partnern zur Verfügung gestellt werden. Der Private Key dieses Paares definiert lediglich, dass die kryptografischen Operationen auf einer SmartCard auszuführen sind. Er ist ohne die passende Card unbrauchbar.

Funktionen für Genießer

Die Nutzung von gpg auf der Kommandozeile bietet etwas mehr Möglichkeiten, als bisher im Enigmail-GUI implementiert sind. Natürlich stehen auch die mit dem GUI durchführbaren Funktionen auf der Kommandozeile zur Verfügung.

Einen Überblick über alle SmartCard-Funktionen gibt die Hilfe. Als erstes muss man den Admin Mode aktivieren, dann hat man vollen Zugriff auf alle Funktionen:

```
> gpg --card-edit
Befehl> admin
Befehl> help
```

Neue Schlüssel generiert man auf der SmartCard mit:

```
> gpg --card-edit
Befehl> admin
Befehl> generate
```

Hat man mehrmals den PIN falsch eingegeben kann man ein neuen (alten) PIN (rück-)setzen, wenn man den Admin-PIN kennt:

```
> gpg --card-edit
Befehl> admin
Befehl> passwd
```

Möglicherweise hat man bereits eine OpenPGP Schlüssel mit vielen Signaturen. Den möchte man nicht wegwerfen und im Web of Trust noch einmal von vorn beginnen. Als Ausweg bietet es sich an, einen vorhandenen, starken Schlüssel mit der SmartCard zusätzlich zu schützen. Der Zugriff auf den geheimen Schlüssel ist dann nur mit der SmartCard möglich. Es ist dem vorhanden Schlüssel mit der ID key-id ein Subkey der SmartCard hinzuzufügen. Das geht nur auf der Kommandozeile:

```
> gpg --edit-key key-id
command> addcardkey
```

Dabei wird ein evtl. auf der SmartCard vorhandener Key zertört!

8.1.7 Web des Vertrauens

Im Prinzip kann jeder Anwender einen Schlüssel mit beliebigen E-Mail Adressen generieren. Um Vertrauen zu schaffen, bietet OpenPGP das **Web of**

Trust.

Hat Beatrice die Echtheit des Schlüssels von Anton überprüft, kann sie diesen mit ihrem geheimen Schlüssel signieren und auf die Schlüsselserver 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 8.10 zeigt eine mögliche Variante für den Key von Anton (A).

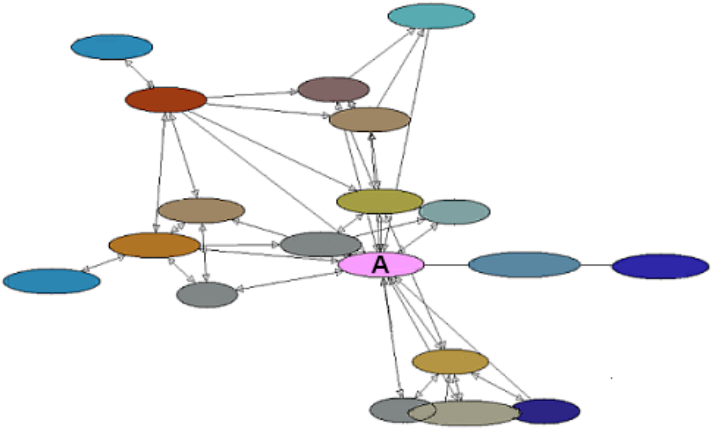


Abbildung 8.10: Beispiel für ein Web of Trust

OpenPGP-Schlüssel signieren

Die Echtheit eines Schlüssels kann anhand des Fingerabdrucks geprüft werden. Zu jedem Schlüssel existiert ein eindeutiger Fingerabdruck. Dieser lässt sich in den Eigenschaften des Schlüssels anzeigen. In der Schlüsselverwaltung ist der zu prüfende Schlüssel auszuwählen und über den Menüpunkt *Anzeigen - Eigenschaften* den im Bild 8.11 dargestellten Dialog zu öffnen.

Der angezeigte Fingerabdruck des Schlüssels kann mit dem Wert verglichen werden, den man vom Eigentümer des Schlüssels erhalten hat. Sind beide identisch, kann das Vertrauen des öffentlichen Schlüssels auf ein hohes

Niveau gesetzt werden. Den Dialog findet man in der Schlüsselverwaltung unter *Bearbeiten - Vertrauenswürdigkeit*.

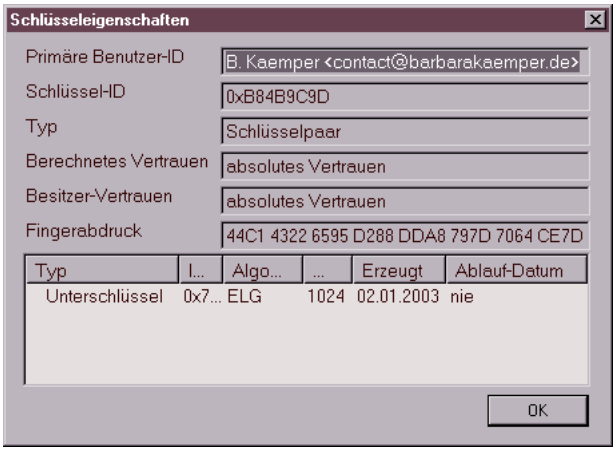


Abbildung 8.11: Schlüssel-Eigenschaften

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 Ergbnisse 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 sgnieren. Alle Partner benötigen lediglich den öffentlichen Schlüssel der CA, um die Echtheit der Schlüssel zu überprüfen.

Beispiele für Certification Authorities sind:

- Krypto-Kampagne der Zeitschrift Ct
- OpenPGP-CA der German Privacy Foundation e.V.
- 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 Beteiligetn 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-Ditributionen 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
```

8.1.8 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 Schlüsselservern 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.

8.2 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.

8.2.1 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.

Im folgenden wird grob der Weg zur Erstellung eines Zertifikates beschrieben:

- Wer häufig CAcert.org nutzt, sollte das Root-Zertifikat dieser CA in den Browser importieren. Man erspart sich damit lästige Nachfragen beim Besuch der Website. Die Root Zertifikate von CAcert.org ist standardmäßig nicht in den häufig genutzten Browsern enthalten. CAcert.org bietet sie auf der Webseite zum Download.

- Es ist notwendig, die Root-Zertifikate von CAcert.org in den E-Mail

Client als vertrauenswürdige CA zu importieren. Nur so kann die Gültigkeit des eigenen Zertifikates überprüft werden.

- Die Anmeldung folgt dem üblichen Schema. Nach Eingabe der Kontaktdaten erhält man eine E-Mail zu Verifizierung und kann sich im Anschluss auf der Website einloggen, um die persönlichen Angaben zu vervollständigen.
- Zur Bestätigung der Identität kann man auf der Website einen Assurer in der Nähe suchen und um ein persönliches Treffen bitten. Zum Treffen ist ein Ausdruck des WOT-Formulars für den Assurer mitzubringen.
- Hat man 50 Punkte durch Bestätigungen von mehreren Assurer erreicht, kann man auf der Webseite ein Zertifikat erstellen. Das Zertifikat und den Privaten Key findet man nach dem Vorgang in der Zertifikatsverwaltung des Browsers unter *Eigene Zertifikate*! Es gibt keinen Downloadlink o.ä.
- Das Zertifikat wird aus der Zertifikatsverwaltung des Browsers als *.P12 Datei exportiert und im E-Mail Client wieder importiert.

8.2.2 Erzeugen eines Zertifikates

Die verschiedenen Certification Authoroties (CAs) bieten ein Webinterface, um nach der Überprüfung der Identität ein signiertes Zertifikat zu erstellen. In der Regel stehen zwei Wege zur Auswahl:

1. Der Anbieter (CA) führt den kompletten Vorgang aus: die Generierung des privaten Key inklusive Sicherung mit einer Passphrase, die Generierung des Certification Request (CSR), die Signierung des CSR und die Erstellung der Zertifikatsdatei mit privatem und öffentlichem Schlüssel.

   CAcert.org hat eine Lösung entwickelt, den privaten Key im Browser des Nutzers zu generieren und nur den CSR (public Key) zur Signatur auf den eigenen Server zu laden. Viele CAs generieren aber beide Schlüssel auf dem eigene Server und haben damit auch 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 Authorithies nicht blind vertrauen.

Die OpenSSL-Bibliothek bietet alles Nötige. Die Tools sind unter Linux installiert. Ein grafisches Interface ist *TinyCA*, erhältlich unter 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.

8.2.3 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 8.12).

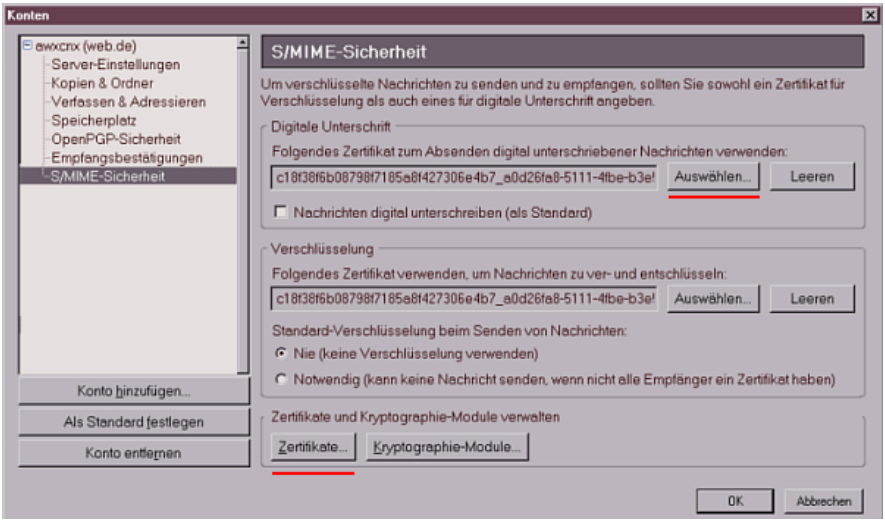


Abbildung 8.12: Kontoeinstellungen zur S/MIME-Sicherheit

Zuerst ist das persönliche Zertifikat zu importieren. Ein Klick auf den Button *Zertifikate* öffnet den Manager für eigene Zertifikate (Bild 8.13). Hier ist der Button *Importieren* zu wählen und das gespeicherte persönliche Zertifikat mit öffentlichem und geheimem Schlüssel zu importieren.

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

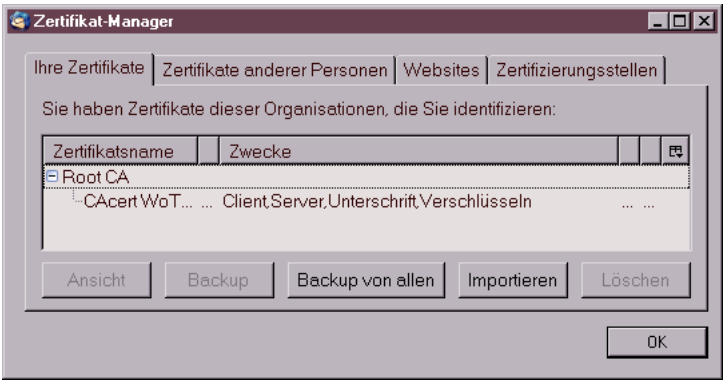


Abbildung 8.13: Zertifikatsmanager für eigene Zertifikate

Entschlüsseln auszuwählen.

Sollen alle ausgehenden Nachrichten standardmäßig signiert werden, kann die entsprechende Option aktiviert werden.

Thunderbird bietet die Möglichkeit, das Online Certifate 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.

8.2.4 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 8.14), um die Verwaltung zu öffnen.

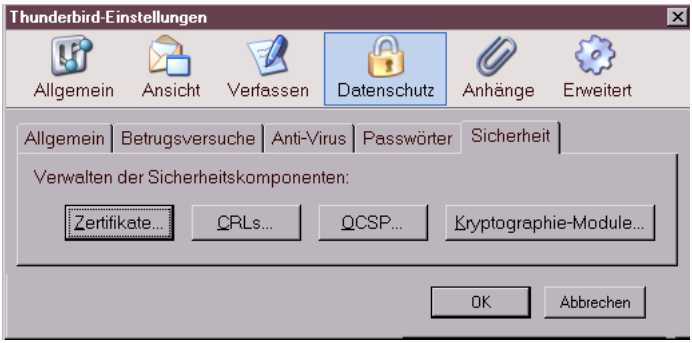


Abbildung 8.14: Dialog Sicherheits-Einstellungen

Im Zertifikatsmanager ist auf dem Reiter *Zertifikate anderer Personen* der Button *Importieren* zu finden, welcher eine Dateiauswahl öffnet, um das erhaltene Zertifikat aus einer lokal gespeicherten Datei zu importieren.

Die Root-Zertifikate weiterer Certification Authorities (CAs) können auf dem Reiter *Zertifizierungsstellen* importiert werden.

8.2.5 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.

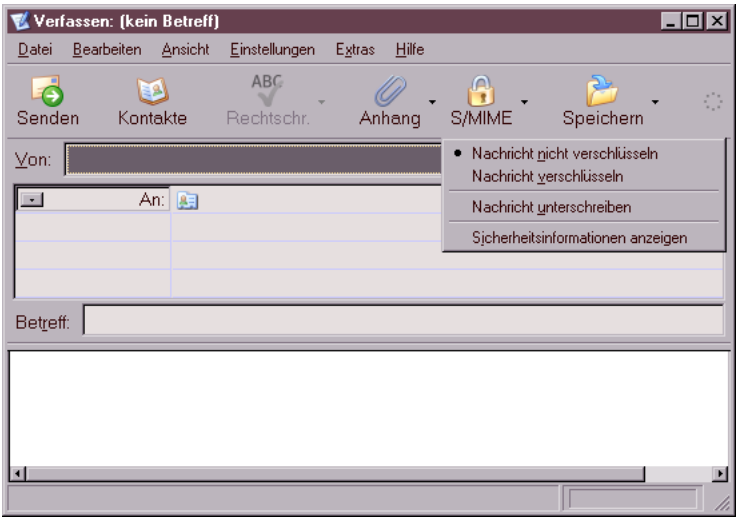


Abbildung 8.15: Verschlüsseln oder Signieren einer E-Mail

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 8.15 dargestellte Menü zum Festlegen der Kryptographie-Optionen für die aktuelle 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 8.16)

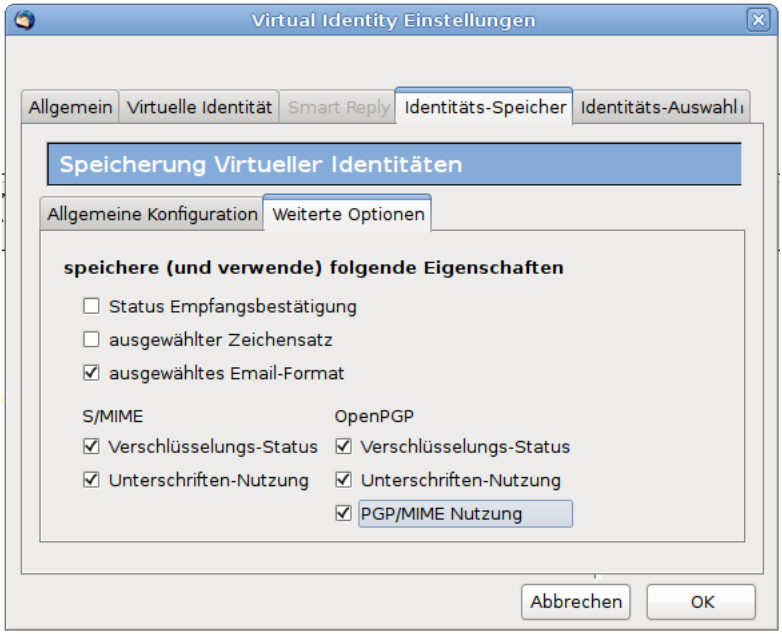


Abbildung 8.16: Einstellungen des Plug-In Virtual Identity

Unter dem Menüpunkt *"Extras - Virtual Identity - Datenspeicher"* findet man die gesammelten Daten und kann sie auch editieren.

8.3 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 Zerti-

fikat vertrauen möchte.

8.3.1 Webbrowser Firefox

Nutzer des Browsers Firefox klicken auf auf das *Root Certificate* und aktivieren in dem sich öffnenden Dialog (Bild 8.17) mindestens den ersten und zweiten Punkt.

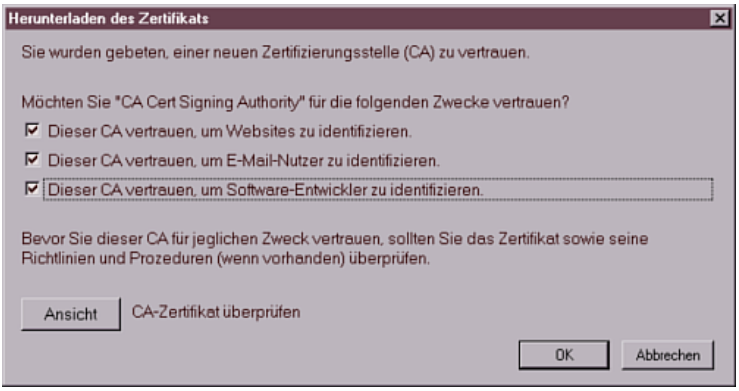


Abbildung 8.17: Herunterladen eines Zertifikates

8.3.2 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 8.18 dargestellten Manager für Zertifikate zu öffnen.

In diesem Dialog ist auf dem Reiter *Zertifizierungsstellen* der Button *Importieren* zu wählen und das zuvor gespeicherte Zertifikat zu importieren.

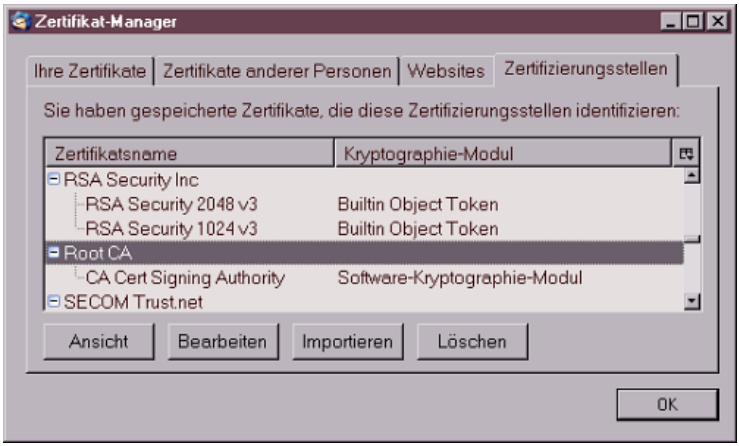


Abbildung 8.18: Zertifikats-Manager von Thunderbird

Im Anschluss sind im folgenden Dialog mindestens die ersten beiden Optionen zu aktivieren (siehe Firefox).

8.4 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.

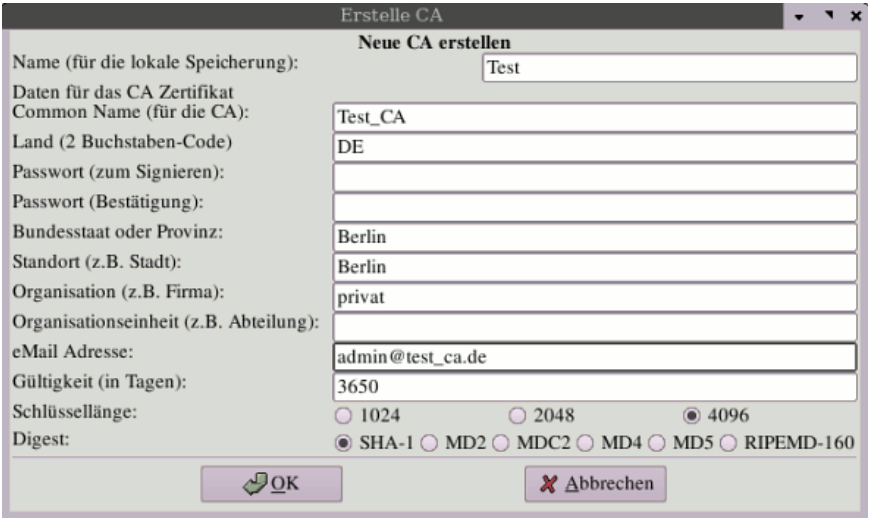


Abbildung 8.19: Anlegen einer neuen CA

Der *Common Name* der CA kann frei gewählt werden. Das Passwort sollte man sich gut überlegen und keinesfalls vergessen. Mit einem Klick auf *Ok* erscheint ein zweiter Dialog mit weiteren Angaben zur CA. Wichtig sind hier die URL der Revocation List für zurückgezogene Zertifikate und die URL der Policy der CA. Die Policy ist ein HTML-Dokument, welches beschreibt, wer ein Zertifikat von dieser CA erhalten kann, also z.B. etwas in der Art: *Nur für persönlich Bekannte!*

Im Anschluss können die E-Mail Zertifikate der Nutzer erstellt werden. Die nötigen Angaben sind selbsterklärend (Bild 8.20. Mit einem Klick auf *Ok* wird das S/MIME-Zertifikat erstellt und mit dem Root-Zertifikat der CA signiert. Dabei wird das Password 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

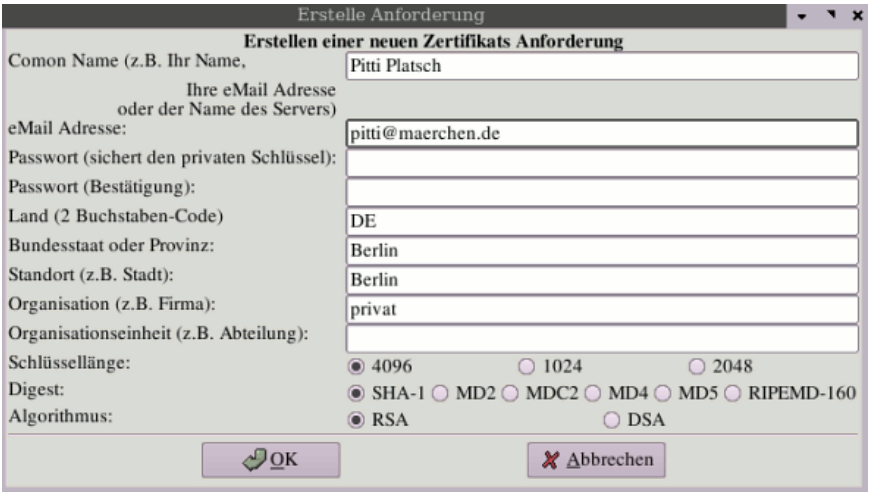


Abbildung 8.20: Erstellen eines E-Mail Zertifikats

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 und ebenfalls zum Download unter der angegebenen URL bereitzustellen. Die Oberfläche bietet für beide Aufgaben einen Button in der Toolbar.

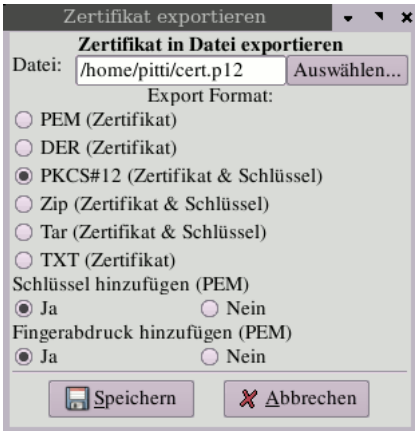


Abbildung 8.21: Zertifikat exportieren

8.5 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 Vertrauenswürdikeit 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 web-basiertes Interface für die Erzeugung und Signatur der Zertifikate. In der Regel werden nach erfolgricher 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 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, das 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 isrealischen 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 Abgordnete 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 stattlichen Stellen).

Projekt De-Mail

Auch das geplante Portale De-Mail für die rechtsverbindliche und sichere deutsche Alternative zur E-Mail soll X.509 Zertifikate für die Gewährleistung der vertraulichen Kommunikation nutzen. Die Anforderungen sehen eine Entschlüsselung der vertraulichen E-Mails durch Betreiber des Dienstes ausdrücklich vor. Als Grund wird die Notwendigkeit des Virescans genannt.

Außerdem wirbt das Projekt damit, den Nutzern einen "Datentresor" für vertrauliche digitale Dokumente zur Verfügung zu stellen. Das Konzept kann jedoch nur als Placebo bezeichnet werden. Sowohl die verschlüsselten Dokumente als auch die Schlüssel für den Zugriff auf die Dokumente sollen beim Anbieter des Dienstes liegen. Die Entschlüsselung der vertraulichen

Daten durch Mitarbeiter ist ebenfalls ausdrücklich vorgesehen.

Das Projekt De-Mail wird in Zusammenarbeit mit dem ePA einen Key-Escrow (Hinterlegung der Schlüssel bei den Behörden) für unbedarfte Anwender vorrantreiben. 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.

8.6 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 Östereich 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.

9 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.

9.1 PrivacyBox der GPF

Die PrivacyBox unter https://privacybox.de ermöglicht es, anonyme Nachrichten zu empfangen. Sie bietet in erster Linie Journalisten, Bloggern u.a. eine vorratsdatenfreie und anonyme Kontaktmöglichkeit für Informanten, steht aber auch anderen Interessenten offen.

Die PrivacyBox nimmt keine E-Mails an! Die Nachrichten müssen auf der Kontaktseite des Empfängers geschrieben werden. Nur so können die Betreiber die Anonymität der Absender garantieren und eine automatische Zuordnung von Absender und Empfänger bei der Erstellung von Kommunikationsprofilen verhindern.

Um eine Kontaktseite zu erstellen, ist ein Account anzulegen und anschließend zu konfigurieren - fertig. Für die Verbreitung der Kontaktinformation ist man selbst verantwortlich. Eingehende Nachrichten können via POP3-SSL abgerufen werden (auch als Tor Hidden POP3 Service) oder

an einen externen E-Mail bzw. I2P-Mail Account weitergeleitet werden. Die Nachrichten werden mit OpenPGP oder S/MIME verschlüsselt, wenn der Empfänger einen Key bereitstellt.

Das Standard-Design der PrivacyBox ist etwas häßlich. Man kann aber ein HTML-Template erstellen und das Aussehen der eigenen Kontaktseite dem privaten Blog oder der eigene Website anpassen. Das Template ist an die Admins der PrivacyBox zu senden. Es wird geprüft und kurzfristig freigeschaltet.

Die PrivacyBox ist eine Einbahnstrasse, es können nur Nachrichten empfangen werden. Sie ist auch als Tor Hidden Service erreichbar unter der Adresse http://c4wcxidkfhvmzhw6.onion oder als eepsite im Invisible Internet unter der Adresse http://privacybox.i2p.

9.2 alt.anonymous.messages

Um die Zuordnung von Absender und Empfänger zu erschwerden, 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 OpnePGP-Schlüssel die E-Mail Adresse des Inhabers. Verwendet man einen solchen Schlüssel ist der Empfänger natürlich deanomynisiert.

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.

9.3 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. Im Unterschied zu den den oben genannten Web-Diensten ist die Einrichtung etwas aufwendiger. Das Invisible Internet Project (I2P) bietet

mit Susimail einen anonymen Mailservice inclusive SMTP- und POP3-Zugang und Gateway ins Web.

9.4 Tor Messaging

Man kann Nachrichten nicht nur per E-Mail austauschen. Eine Alternative ist es, die Nachrichten im Webinterface zu schreiben und zu lesen. Das vereinfacht die Nutzung. Tor Privat Messaging unter http://4eiruntyxxbgfv7o.onion/pm/ ist ein Tor Hidden Service im Onionland, um Textnachrichten unbeobachtet auszutauschen. Wer Probleme mit der Installation von Tor hat oder unterwegs ist, kann unsere Tor-Web-Proxys nutzen: https://privacybox.de/top-proxy.de.html oder https://www.awxcnx.de/tor-i2p-proxy.htm.

9.5 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.

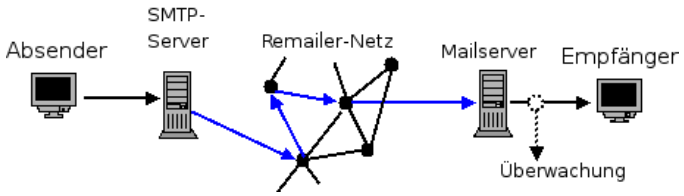


Abbildung 9.1: Konzept einer anonymen E-Mail

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!

9.5.1 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.

10 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 Persönlichkeitsprofiles 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

10.1 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. Standartmäßig wird diese CA nur von wenigen Newsreadern aktzeptiert. 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.

10.2 Thunderbird konfigurieren

1. Anlegen eines neuen SMPT-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.

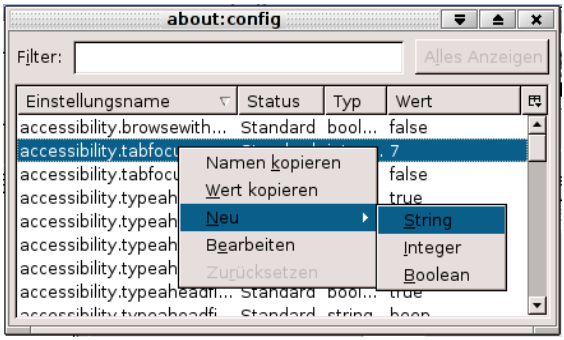


Abbildung 10.1: Neue Config-Variable anlegen

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

mail.identity.id**N**.headers	archive
mail.identity.id**N**.header.archive	X-No-Archive: yes

4. Abbonieren der News-Gruppen.

11 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.

11.1 Warum sollte man diese Dienste nutzen?

Anonymisierungsdienste verstecken die IP-Adresse des Nutzers und verschlüsseln die Kommunikation zwischen Nutzer und den Servern des Dienstes. Außerdem werden spezifischer Merkmale modifiziert, die den Nutzer identifizieren könnten (Browser-Typ, Betriebssystem, TCP-Timestamps, Referer....).

1. **Profilbildung:** Nahezu alle großen Suchmaschinen genenrieren 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 sinnvollen IP-Adresse zur Verfügung steht, können sie den Standort des Nutzers 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 verschlüsselte der Kommunikation mit den Servern des Anonymisierungsdienstes verhindert ein Mitlesen des Datenverkehrs durch Dritte in unsicheren Netzen. (Internet Cafes, WLANs am Flughafen oder im Hotel, TKÜV...)
4. **Rastern:** Obwohl IP-Adressen die Identifizierung von Nutzern ermöglichen, sind sie rechtlich in vielen Ländern ungenügend geschützt. In den USA können sie ohne richterliche Prüfung abgefragt werden. Die TK-Anbieter genießen Straffreiheit, wenn sie die nicht vorhandenen Grenzen übertreten. Wenig verwunderlich, dass man IP-Adressen zur täglichen Rasterfahndung nutzt. Facebook gibt täglich 10-20 IP-Adressen an US-Behörden, AOL übergibt 1000 Adressen pro Monat...
5. **Vorratsdatenspeicherung:** Ein Schreiben des Bundesdatenschutzbeauftragen 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 Auskunftsersuchen 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.
6. **Zensur:** Der Datenverkehr kann vom Provider oder einer restriktiven Firewall nicht manipuliert oder blockiert werden. Anonymisierungsdienste ermöglichen einen unzensierten Zugang zum Internet. Sie können sowohl die "Great Firewall" von China und Mauretanien durchtunneln sowie die in westeuropäischen Ländern verbreitet Zensur durch Kompromittierung des DNS-System.

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 Dissidenden zu beobachten

8. **Leimruten:** Einige Websites werden immer wieder als Honeypot genutzt. Ein Beispiel ist die Website des BKA. Surfer werden hier identifiziert und machen 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 Anonymisierungsienste auch gegen Beobachtung durch die Betreiber des Dienstes selbst. Die mehrfache Verschlüsselung des Datenverkehrs und die Nutzung einer Kette von Servern verhindert, dass einzelne Betreiber des Dienstes die genutzten Webdienste einem Nutzer zuordnen können.

11.2 Tor, I2P, Freenet und JonDonym

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

- **Tor Onion Router** ist ein weltweit verteiltes Anonymisierungs-Netzwerk. Die Projektwebsite bietet unter der Adresse https://www.torproject.org umfangreiche Informationen.

- **JonDonym** steht in einer limitierten kostenfreien Variante zur Verfügung sowie in einer kostenpflichtigen, kommerziellen Variante, die eine höhere Anonymität und Geschwindigkeit bietet.

- Das **Invisible Internet Project** hat das primäre Ziel, Anonymität sowohl für Konsumenten als auch für Anbieter von Angeboten zu bietet. Dieses

Ziel läßt sich nur in einem geschlossenen Netz verwirklichen. Es bietet aber auch die Möglichkeit, anonym auf herkömmliche Websites zuzugreifen.

Tor Onion Router

Tor nutzt ein weltweit verteiltes Netz von 2400 aktiven Nodes. Aus diesem Pool werden jeweils 3 Nodes für eine Route ausgewählt. Die Route wechselt regelmäßig in kurzen Zeitabständen. Die zwiebelartige Verschlüsselung sichert die Anonymität der Kommunikation. Selbst wenn zwei Nodes einer Route kompromittiert wurden, ist eine Beobachtung durch mitlesende Dritte nicht möglich.

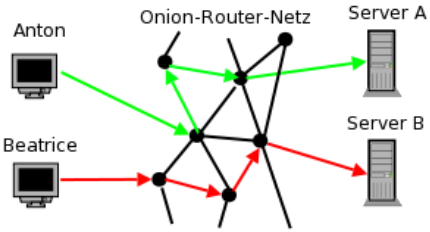


Abbildung 11.1: Prinzip von Tor

Da die Route ständig wechselt, müsste ein großer Teil des Netztes kompromittiert worden sein, um einen Zusammenhang von Surfer und angefragter 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 schnüfflenden 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. Innerhalb von 24h konnten mit einen Tor Exit Node folgende Accounts erschnüffelt werden: 114x Yahoo, 50x GMail, 9x Paypal, 9x Linkedin, 3x Facebook.
- 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

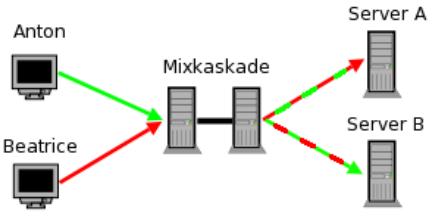


Abbildung 11.2: Prinzip von JonDonym

Premium-Accounts erfolgt über die Bezahlinstanz der JonDos GmbH.

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 Kaskade einen richterlichen Beschluss in ihrem Land erhalten. In Deutschland ist eine Gerichtsbeschluss nach §100a StPO nötig. Im Gegensatz zu Tor und I2P ist eine Verfolgung schwerer Verbrechen möglich. Die internationale Verteilung der Kaskaden verhindert eine pauschale Überwachung durch einen Staat.

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 verschlüssellt 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.

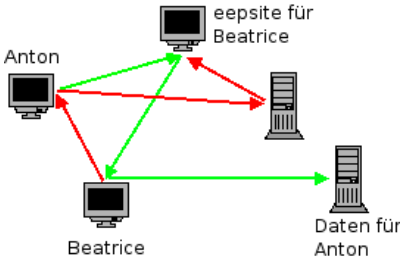


Abbildung 11.3: Prinzip von I2P

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.

11.2.1 Finanzierung der Anonymisierungsdienste

Wie wird die Entwicklung der Software und die Infrastruktur des Dienstes finanziert und welche Abhängigkeiten ergeben sich möglicherweise daraus?

Tor Onion Router

Die Softwareentwicklung wird durch Spenden finanziert. TorProject.org benötigt pro Jahr ca. 1 Mio. Dollar für die Weiterentwicklung der Software und den Betrieb weniger Kernkomponenten des Dienstes. Die Grafik 11.4 zeigt die Zusammensetzung der Spender für 2009 (Quelle Tor Financial Report 2009).

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 "Gouvernments" (72% der Einnahmen) kommt in erster Linie von der US-Regierungsorganisationen. Diese Spenden werden nicht detailierter aufgelistet.

Der Hauptteil der Infrastruktur wird von Enthusiasten finanziert und technisch in der Freizeit betreut. Die Kosten von 600-800 Euro pro Power-Server

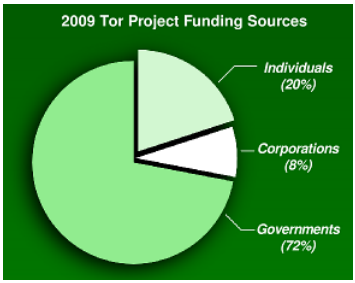


Abbildung 11.4: Anteil der Finanzierung von TorProject.org

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 dieser Angebote ist eine volumenabhängige Gebühr im Voraus zu bezahlen. Die Einnahmen sollen die Kosten für die Weiterentwicklung der Software, die Betreuung des Projektes und die Infrastruktur der Premium-Dienste decken. Diese 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.

11.3 JonDo installieren

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 plattform-unabhängig. Es gibt auch eine Version ohne grafisches Interface: JonDoConsole.

1. 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 (5MB) 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.)

2. 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.

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

3. 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

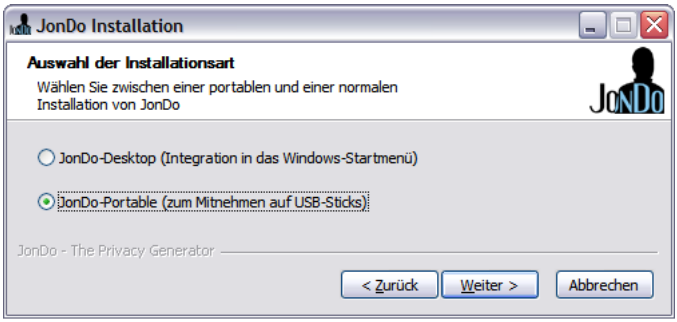


Abbildung 11.5: Installation von JonDo

verwendete Ditribution zu ersetzen (lenny, sid, intrepid, jaunty oder karmic):

```
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 http://anonymous-proxy-servers.net/downloads/JonDos_GmbH.asc zum Download bereit liegt. 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 Bowserprofil *JonDoFox* für Firefox/Iceweasel gleich mit installiert, findet man auch einen fertig konfigurierten Browser in der Menügruppe *Internet*.

4. 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
```

Startet man JonDo, öffnet sich das im Bild 11.6 gezeigte Hauptfenster des Programms. Hier kann man eine Kaskade auswählen und mit Klick auf die Option *Anonymität Ein* die Verbindung herstellen.

Hinweis: Aufgrund der dauerhaften Überlastung der kostenfreien Mix-Kaskaden kann es mehrere Minuten dauern, ehe ein Platz frei wird und eine Verbindung zum Anonymisierungsdienst hergestellt werden kann. Der JonDo Client probiert im ständigen Wechsel die verfügbaren Kaskaden durch. Sie müssen warten. Mit Premium-Diensten treten diese Probleme nicht auf und man wird sofort verbunden.

11.3.1 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:

Abbildung 11.6: Hauptfenster von JonDo

- 20x höhere Geschwindigkeit (siehe: Status der Mix-Server)
- Alle Internet-Protokolle nutzbar (kostenfreie Kaskaden nur für Surfen)
- SOCKS5 Support für Anwendungen, die keinen HTTP-Proxy unterstützen
- Hohe Verfügbarkeit (kostenfreie Kaskaden sind häufig überlastet)
- In der Regel wird der Datenverkehr durch 3 Länder geleitet.

JonDonym bietet mehrere Volumen-Tarife, die im voraus zu bezahlen sind. Als Bezahlmethoden stehen Paysafecard, Paypal, Überweisung und Briefsendung zur Auswahl. Die Einrichtung eines Premium-Account erfolgt im JonDo Client. Wählen sie in *Einstellungen* den Punkt *Bezahlung* (Bild 11.7).

Ein Klick auf den Button *Konto erzeugen* startet den Wizzard, 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

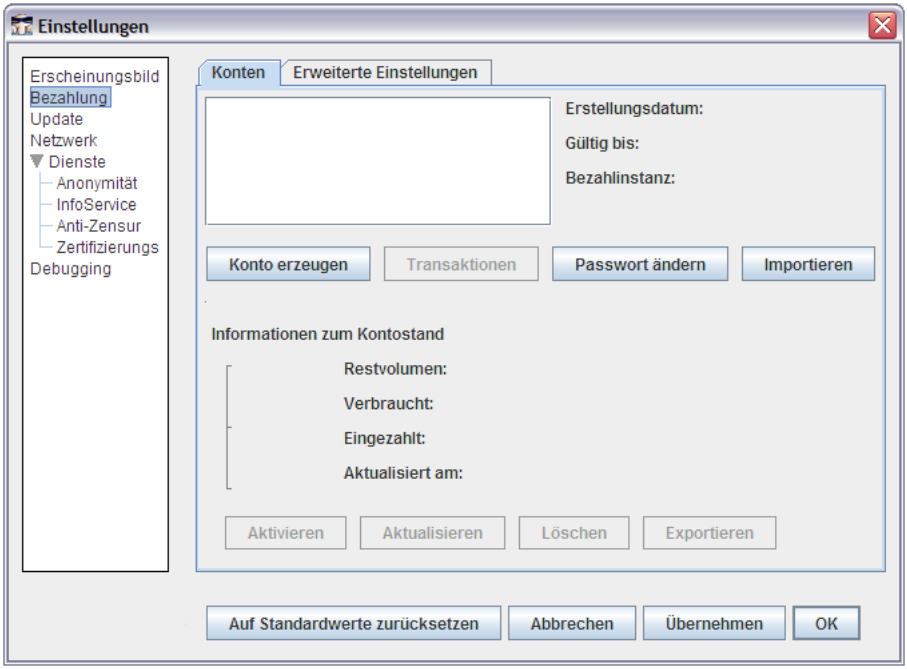
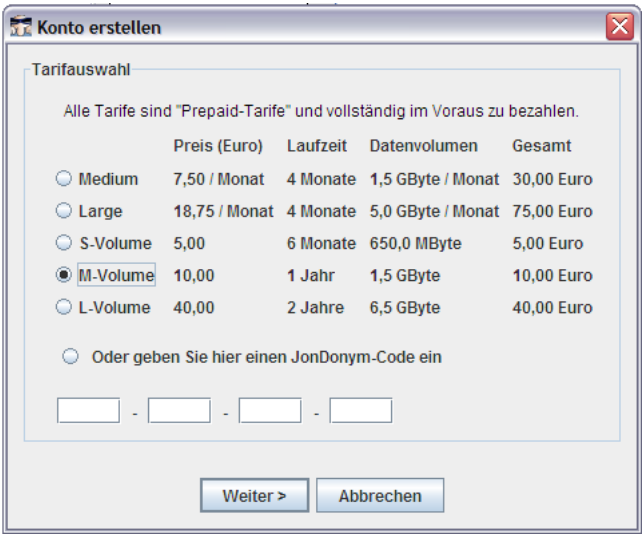
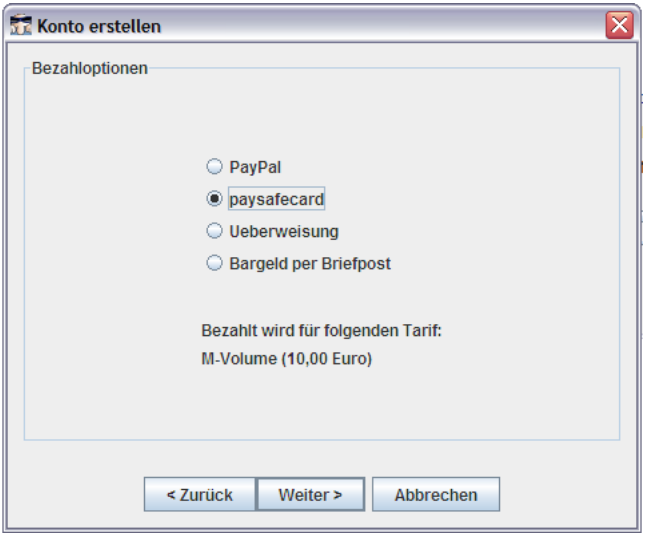


Abbildung 11.7: Verwaltung der Premium-Accounts

4 Monaten zur Verfügung oder einfache Volumentarife mit einer längeren Laufzeit.



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



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.

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

11.4 Tor Onion Router installieren

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 und durch Spenden finanziert.

Das Tor Onion Router Netzwerk besteht gegenwärtig aus ca. 2000 Servern (Nodes), die weltweit verteilt sind. Etwa 60% der Nodes sind aktiv.

11.4.1 Tor mal ausprobieren

Wer Tor schnell mal ausprobieren möchte oder unterwegs in einem Internetcafe keinen Tor Client installieren kann, findet auf folgenden Webseiten

Web-Proxys für das Tor-Netzwerk. Einfach auf der Website die gewünschte URL eingeben und ab gehts.

- https://privacybox.de
- https://www.awxcnx.de

Verglichen mit der lokalen Installation des Tor Clients ist dies die zweitbeste Möglichkeit, anonym zu surfen. Die Betreiber des Proxy könnte den Datenverkehr mitlesen. (Sie tun es aber nicht!)

11.4.2 Tor für WINDOWS

TorProject.org bietet für WINDOWS zwei Bundles:

1. **TorBrowser** ist eine portable Firefox-Version incl. Tor, Vidalia und auf Wunsch auch mit dem Instant-Messanger Pidgin. Das Archiv ist nach dem Download zu entpacken, keine Installation ist nötig. Es kann auch auf dem USB-Stick mitgenommen werden. Wird der TorBrowser vom USB-Stick gestartet hinterläßt er keine Spuren auf dem Rechner.
   https://www.torproject.org/torbrowser/index.html.de
2. Das Installationspaket **Vidalia-Bundle** von der Downloadseite enthält Tor, Polipo und das grafische Tool Vidalia. Es ist für die feste Installation auf dem Windows-Rechner gedacht. Firefox muss zusätzlich installiert werden (oder ist bereits vorhanden).
   https://www.torproject.org/easy-download.html.de

   Nach dem Download können das selbstentpackende EXE-Archiv gestartet werden, um die nötigen Komponenten zu installieren.

   Es ist nicht nötig, für das Programm *Tor* Shortcuts im Programmmenü anzulegen und einen Autostart beim Anmelden vorzusehen. Tor kann vollständig über das Control-Panel Vidalia gesteuert werden. Es ist zweckmäßig, Vidalia bei der Anmeldung automatisch zu starten.

   Nach der Auswahl eines Verzeichnisses, in welchem der aktuelle Nutzer Schreibrechte hat, werden die ausgewählten Komponenten installiert. Es ist nicht notwendig, die Installation als Administrator durchzuführen.

   Das Control-Panel Vidalia bietet die Möglichkeit, Tor zu konfigurieren, zu starten und zu beenden. Ein Klick auf das Zwiebel-Icon im Systray

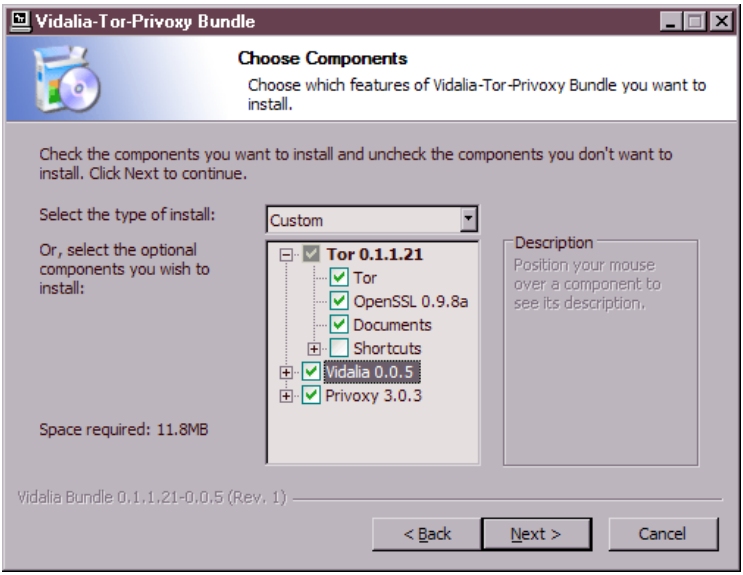


Abbildung 11.8: Installation des Bundles

öffnet das Vidalia-Menü, welches Einträge für das Starten und Beenden von Tor bietet. Vidalia kann mit der Anmeldung automatisch gestartet werden. Dieser Autostart wird bei der Installation eingerichtet.

11.4.3 Tor für Linux

Es stehen eine Reihe von Paketen für diverse UNIX Distributionen auf der Downloadseite des Projektes zur Verfügung.

TorBrowserBundle

Das Bundle aus Tor, Firefox und Vidalia steht auf der englischen Downloadseite auch für Linux zur Verfügung. Download des passenden Archives, entpacken und starten. Eine Installation ist nicht nötig, das TorBrowserBundle kann auch auf dem USB-Stick mitgenommen werden.

```
> tar -xzf tor-browser-gnu-linux-1.0.5-dev-de.tar.gz
> cd or
> start-tor-browser
```

Debian und Ubuntu

Debian und Ubuntu enthalten das Paket *tor*. Es kann mit der Paketverwaltung installiert werden. Dabei handelt es sich jedoch um eine selten aktualisierte und veraltete Version.

Torproject.org stellt aktuelle Pakete zur Verfügung. Das APT-Repository kann mit folgender Zeile ist der Datei */etc/apt/sources.list* genutzt werden. Grafische Frontends wie Synaptic u.ä. unterstützen auch das Hinzufügen von Repositories.

```
deb   http://deb.torproject.org/torproject.org   DISTRI   main
```

DISTRI ist dabei durch *etch*, *lenny*, *hardy*, *intrepid*, *jaunty* oder *karmic* zu ersetzen, wenn die entsprechende Distribution verwendet werden. Die Integrität der Pakete kann mit dem PGP-Signaturschlüssel verifiziert werden. Der Schlüssel ist in den Apt-Keyring einzufügen:

```
> gpg --keyserver subkeys.pgp.net --recv 886DDD89
> gpg --fingerprint 886DDD89
   Schl.-Fingerabdruck = A3C4 F0F9 79CA A22C DBA8
      F512 EE8C BC9E 886D DD89
> gpg --export 0x886DDD89 | sudo apt-key add -
```

Im Anschluss installiert man *tor* wie üblich mit:

```
# apt-get update
# aptitude install tor vidalia
```

In der Menügruppe Internet findet man nach der Installation *Vidalia (Tor GUI)*. Über dieses Interface kann Tor bei Bedarf gestartet und gestoppt werden.

Sourcen

Die Sourcen stehen auf der Downloadseite zur Verfügung.
https://www.torproject.org/download-unix.html.de

Tor benötigt zum Compilieren die Paket **libssl-dev** und **libevent-dev**, welche mit den Tools der jeweiligen Distribution zu installieren sind. Nach dem Download ist das Archiv zu entpacken, in das Verzeichnis mit dem Quellcode zu wechseln und der übliche Dreisatz als User root aufzurufen:

```
# ./configure && make && sudo make install
```

Die Administrator-Privilegien sind nur für den letzten Schritt nötig. Hat man keine Möglichkeit, diese Privilegien zu erlangen, kann auf "make installäuch verzichtet werden. Das ausführbare Programm "torßteht dann im Unterverzeichnis ßrc/or/ßum Start bereit und kann auch in ein beliebiges anderes Verzeichnis kopiert werden.

11.4.4 Polipo oder Privoxy

Mit Ausnahme von Mozilla Firefox benötigen alle anderen Webrowser einen HTTP-Proxy, der den Datenverkehr an Tor weiter zu leiten. Tor bietet nur einen SOCKS-Proxy. Der Browser sendet seine Anfragen an den HTTP-Proxy und dieser leiten sie an den Tor Client weiter. Unter Linux hat man die Wahl zwischen Polipo und Privoxy als HTTP-Proxy mit SOCKS-Support. Beide sind nach der Installation zu konfigurieren. Das WINDOWS-Paket von torproject.org enthält Polipo und ist bereits vorkonfiguriert.

- **Polipo:** Wird von TorProject.org empfohlen. Da der Proxy den Datenverkehr sofort an den Browser weiterleitet, ist der gefühlte Seitenaufbau etwas schneller. Leider kommt es häufiger zu Timeouts beim Aufruf einer Website, vor allem bei Tor Hidden Services.

  Um den Datenverkehr an Tor weiter zu leiten, ist in der Datei */etc/polipo/config* ein Parent-Proxy zu konfigurieren:

  ```
  socksParentProxy = "localhost:9050"
  socksProxyType = socks5
  ```

  Danach ist Polipo neu zu starten:

  ```
  > sudo invoke-rc.d polipo restart
  ```

  Im Browser gibt man folgende Proxy-Adresse an, um die Daten durch Polipo und Tor zu jagen:

  ```
  Host:   localhost
  Port:   8123
  ```

- Wir empfehlen den Content-Filter **Privoxy**. Durch mehrfache Versuche beim Aufruf einer Website entfallen die lästigen Timeouts. Da Privoxy die Website zuerst komplett lädt und filtert, bevor sie an den Browser

weitergeben wird, ist der gefühlte Seitenaufbau etwas langsamer.

Privoxy kann mit dem Paketmanager der jeweiligen Linux-Distribution installiert werden, für Debian und Ubuntu wie üblich mit:

```
> sudo aptitude install privoxy
```

Die Konfiguration von Privoxy erfolgt vollständig ebenfalls über Textdateien. Man findet diese in der Regel im Verzeichnis */etc/privoxy* (SuSE Linux: */var/lib/privoxy/etc*).

In der Datei *config.txt* der Privoxy Konfiguration sind folgende Anpassungen nötig:

1. Für die Weiterleitung des Datenverkehrs an Tor ist folgende Zeile einzufügen oder die ensprechende Kommentarzeichen zu entfernen. (Nicht den Punkt am Ende der Zeile vergessen!):

   ```
   forward-socks4a  /  localhost:9050 .
   ```

2. Da über Socks4a-Verbindungen gelegentlich einige Verbindungen verloren gehen, sollte Privoxy mehrfach versuchen, eine Verbindung herzustellen (1-3x):

   ```
   forwarded-connect-retries 3
   ```

3. Um zu vermeiden, das alle abgerufenen Webseiten im Logfile protokolliert werden, sind nur die folgenden Debug-Ausgaben zulässig:

   ```
   debug   4096
   debug   8192
   ```

Anschließend ist der Content-Filter neu zu starten. Unter Linux kann man diverse GUIs für die Steuerung der Daemons verwenden oder auf der Kommandozeile mit:

```
> sudo invoke-rc.d privoxy restart
```

Im Browser gibt man folgende Proxy-Adresse an:

```
Host:   localhost
Port:   8118
```

11.5 Anonym Surfen

Anonymes Surfen ist die Hauptanwendung für Tor und JonDonym. Beide Projekte empfehlen, den Webbrowser Firefox zu nutzen und bieten für diesen Browser mit dem Add-on **TorButton** und dem Profil **JonDoFox** besondere Unterstützung. Neben dem anonymen Zugriff auf herkömmliche Websites bietet Tor zensurresitente Hidden Services, das Onionland.

11.5.1 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 Hilfmittel enthalten, um sich anonym im Web zu bewegen. Es wird der HTML-Header gefakt, Cookies und Javascript werden kontrolliert, SSL-Zertifikate werden besser überprüft und Werbung wird blockiert.
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 vorraus, dass Firefox bereits vorhanden ist. Bei der USB-Version wird ein Portable 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*.
http://anonymous-proxy-servers.net/de/help/firststeps2.html

- Für andere Linux 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 bestehede Firefox Konfiguration. Firefox oder Iceweasel sollten zuvor mit dem Paketmanager installiert worden sein.

```
> 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 11.9). Damit wird der Nutzer auch gezwungen, den Browser zu schließen, bevor er zum anonymen Surfen wechselt.

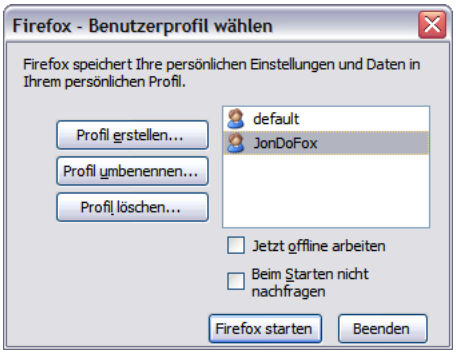


Abbildung 11.9: Profil beim Start von Firefox wählen

Als Erstes sollte man nach dem Start des JonDoFox die Add-ons aktualisieren (Menüpunkt: *Extras -> Add-ons*) und den Anonymitätstest von JonDos besuchen, um sicher zu gehen, dass alles richtig funktioniert. Ein Lesezeichen ist vorbereitet. https://what-is-my-ip-address.anonymous-proxy-servers.net/

JonDoFox setzt einige Restriktionen, um eine hohe Anonymität beim Surfen zu garantieren. Gelegentlich kommt es dabei auch zu Einschränkungen der Funktion einiger Websites.

Cookies und Javascript

Viele Webseiten nutzen Cookies und Javascript. Neben der Sammlung von Informationen über den Surfer können diese Techniken auch sinnvoll eingesetzt werden. Um grundsätzlich die Anonymität zu wahren, sind im JonDoFox die Annahme von Cookies und die Ausführung von Javascript

deaktiviert.

Zwei kleine Symbole in der Statuszeile unten rechts ermöglichen es, diese Techniken für einzelne, vertrauenwürdige Webseiten gezielt freizugeben. Ähnlich wie Cookies kann auch Javascript für einzelne Domains freigegeben werden.

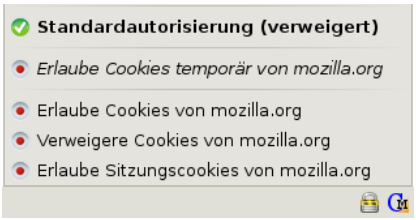


Abbildung 11.10: Cookies für eine Websites freigeben

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.

Ähnlich wie Cookies kann auch **Javascript** für einzelne Domains bei Bedarf freigegeben werden. 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.

Das JonDoFox Profil bring eine Vielzahl von **Suchmaschinen** mit. Leider wird meist nicht die HTTPS-Version verwendet. Wir empfehlen, die Liste der Suchmaschinen erst einmal aufzuräumen und dann die HTTPS-verschlüsselten Versionen von Ixquick, Startingpage, Wikipeadia, Scroogle

und DuckDuckGo zu installieren. Die Addons für diese Suchmaschinen gibt es unter http://mycroft.mozdev.org.

Anonymisierungsdienst wechseln

onDoFox ist nicht nur für anonymes Surfen mit JonDonym konzipiert. Es ist auch eine gutes Profil, um Tor zu nutzen. Mit einem Klick auf das Add-on in der Statusleiste kann den Anonymisierungsdienst einfach wechseln.

11.5.2 Anwenungen für anonymes Surfen

Eine kleine Auswahl von Beispielen soll zeigen, was mit einem anonymisiertem Browser möglich ist und was man beachten sollte, um die Anonymität zu wahren.

Anonyme E-Mails ohne Account

Um einzelne E-Mails unkompliziert und ohne Einrichten eines Kontos zu empfangen, kann man temporäre Wegwerf-Adressen nutzen:

- www.10minutemail.com
- http://www.sofort-mail.de
- http://www.trash-mail.com
- http://dodgit.com

Anonymes Senden von E-Mails kann via Remailer Webinterface erfolgen:

- https://www.awxcnx.de/anon-email.htm (unterstützt Dateianhänge)
- https://www.bananasplit.info/cgi-bin/anon.cgi
- https://www.cotse.net/cgi-bin/mixmail.cgi

Als passwort-geschützte Alternative kann man die *anonbox* des CCC nutzen. (https://anonbox.net) Sie bietet ein Postfach, welches nach der Anmeldung bis 24 Uhr des Folgetages verfügbar ist und anschließend gelöscht wird.

Videos im Web

Videos werden in der Regel als Flash-Filme auf Webseiten bereitsgestellt und von einem Flash-Player im Browser angezeigt. Aus Sicherheitsgründen werden Flash-Applikationen im JonDoFox nicht ausgeführt. Man sollte die Videos auf der Festplatte speichern und einen lokalen Medien-Player zum Abspielen nutzen.

- Das Plug-In *DownloadHelper* zeigt durch drei rotierende Kugeln in der Toolbar an, das Medien gefunden wurden, die gespeichert werden können. Dabei können die Flash-Filme in ein gebräuchlicheres Format konvertiert werden. (Bild 11.11)

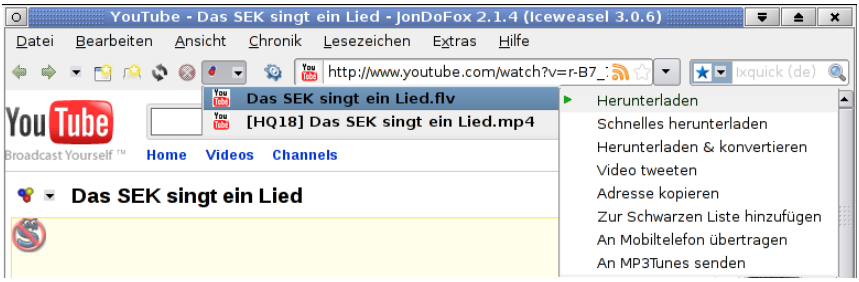


Abbildung 11.11: Flash-Videos von Youtube lokal speichern

- Es gibt auch Webdienste, die Flash-Videos aus dem Web konvertieren und für den Download bereitstellen, bspw. www.share-tube.de.

Dateien anonym tauschen und verteilen

Um anonym größere Dateien zu tauschen, empfehlen die Entwickler die Nutzung von *1-Click-Hostern*. Die folgenden Webdienste verlangen keine Benutzerdaten und setzen keine Freigabe von Cookies oder Javascript voraus:

- http://www.turboupload.com/
- http://www.filefactory.com/
- http://www.share-now.net/

- http://files.ww.com/

Man ruft die Webseite des Dienstes auf und lädt die zu tauschende oder anonym zu verteilende Datei auf den Server des Dienstes. Ist der Upload abgeschlossen, erhält man eine Link, den man an die Tauschpartner sendet oder anonym veröffentlicht. Interessierte können sich die Datei unter dem Link herunter laden.

Bei anonym verteilten Dateien sollte man sicherstellen, dass die Datei keine Meta-Inforamtionen enthält, die den Absender verraten. Insbesondere Dokumente von Office-Suiten (MS-Office, OpenOffice.org) sind nicht anonym verteilbar. Sie enthalten umfangreiche Angaben über den Bearbeiter. Diese Dokumente anonymisiert man zuverlässig, indem sie ausgedruckt und wieder eingescannt werden. Die resultierende Bilddateien sind dann gesäubert.

11.5.3 Anonym Surfen mit Tor

Die Entwickler von Tor empfehlen ausdrücklich, das Add-on TorButton zu nutzen. Es bietet neben der Umschaltung des Proxy weitere Funktionen für hohe Anonymität. Man kann z.B auf Cookies, die via Tor empfangen wurden, im normalen Modus nicht zugreifen. Das verhindert eine ungewollte Deanonymisierung. Der HTML-Header wird gefakt, um Browserkennung und andere Merkmale zu vereinheitlichen, gefährliche Javascript-Hooks werden blockiert usw.

Firefox Profil anlegen

Um eine hohe Anonymität zu sichern, empfehlen wir, für jeden Anon-Dienst ein eigenes Profil zu nutzen. Damit werden alle Daten konsequent getrennt.

Das Add-on *ProfileSwitcher* vereinfacht die Arbeit mit mehreren Profilen. Es steht unter https://nic-nac-project.org/ kaosmos/profileswitcher-en.html zur Installation bereit, ist als erstes zu installieren und Firefox neu zu starten. Den Profilmanager von Firefox öffnet man mit dem Menüpunkt *Datei - Profilmanager öffnen* oder man nutzt das Symbol in der Statusleiste (rechte Maustaste!). Ohne das Plug-In startet man den Profilmanager auf der Kommandozeile mit:

```
> firefox -P
```

Nach dem Anlegen mehrerer Profile fragt Firefox bei jedem Start, welche Konfiguration genutzt werden soll. Die Umschaltung zwischen verschiedenen Konfigurationen erfolgt über den Menüpunkt *Datei - Anderes Profil laden* oder man nutzt das Symbol in der Statusleiste .

Abbildung 11.12: Profilmanager für Firefox

Profil TorBrowser konfigurieren

Die Basics für anonymes Surfen werden vom **TorButton** eingerichtet. Das Add-on steht unter https://www.torproject.org/torbutton zum Download bereit und wird mit einem Klick auf den Link *Installation* integriert. Nach der Installation ist Firefox neu zu starten. Torbutton vereinfachen durch sinnvolle Standardwerte die Konfiguration.

Um lästige Timeouts (vor allem beim Zugriff auf Hidden Services) zu reduzieren, empfehlen wir den Content-Filter Privoxy. Privoxy hat eine bessere SOCKS-Unterstützung als Firefox und kann es im Hintergrund mehrfach versuchen, eine Website aufzurufen. Der Screenshot 11.13 zeigt, wie die Proxy-Einstellungen im TorButton zu setzen sind. Wer es einfacher haben möchte, benutzt die empfohlen Proxy-Einstellungen.

TorButton ist ein komplexes Tool mit vielen Konfigurationsmöglichkeiten. Auf einige Möglichkeiten wollen wir kurz hinweisen. Wenn für anonymes Surfen mit Tor ein eigenes Profil verwendet wird, sollte beim Start auch stets Tor aktiviert sein, damit man sich nicht versehentlich deanonymisiert. Unter *Sicherheitseinstellungen - Start-up* kann man dieses Verhalten konfigurieren (Bild 11.14).

Auf dem Reiter *Überschriften* kann sollte man die Fakes für den HTML Header aktivieren. Die Blockade des Referer kann zu Problemen auf Websiten

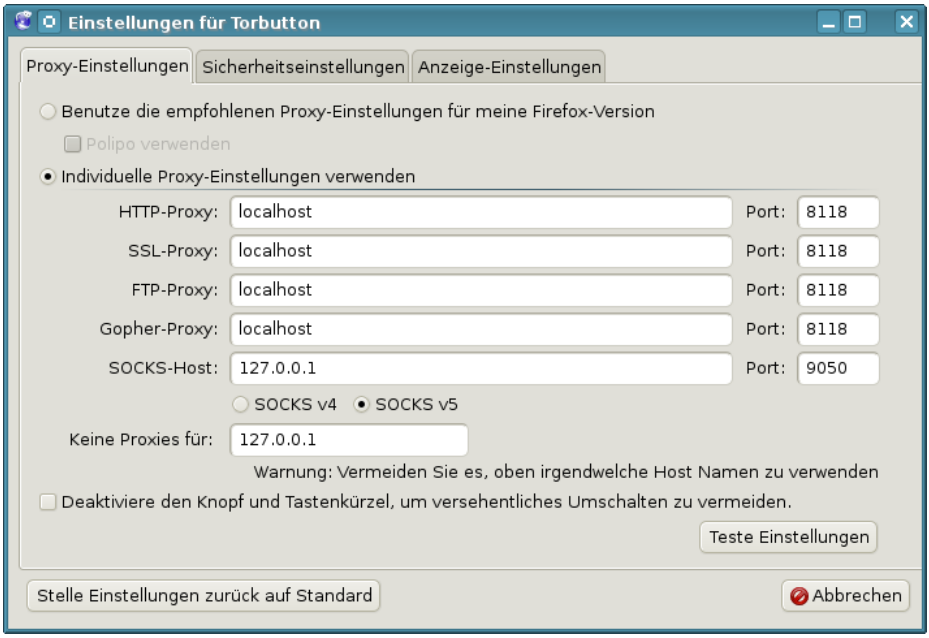


Abbildung 11.13: Proxy-Einstellungen für TorButton

führen. Diese Option sollte man deaktivieren und das empfohlene Add-on **RefControl** installieren, um den Referer nur bei einem Wechsel der Domain zu blockieren.

Anschließend installiert man einige weitere Add-ons, die das anonyme Surfen bequemer und sicherer machen:

- **NoScript:** Javascript sollte generell blockiert werden. Auf vertrauenswürdigen(!) Seiten kann man Javascript aktivieren, wenn es nötig ist.
- **CookieMonster** blockiert unerwünschte Cookies. Die Identifizierung durch Cookies sollte natürlich blockiert werden.
- **RefControl** bietet ein feiner einstellbares Management für die Schleimspur im Internet (Referer). TorButton kann den Referer nur komplett deaktivieren, was einige Websites unbenutzbar macht.

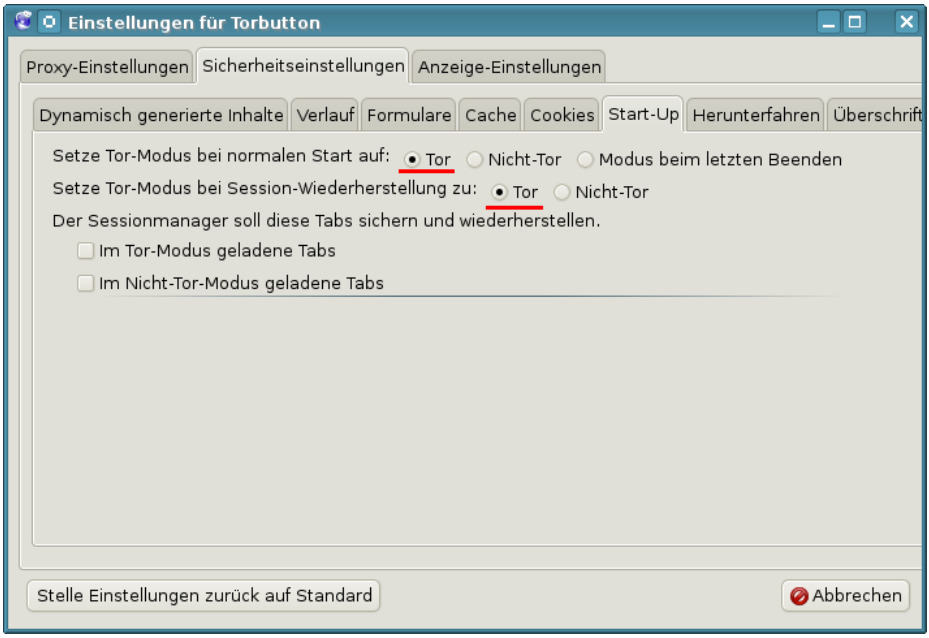


Abbildung 11.14: Sicherheitseinstellungen von TorButton

- **AdBlock Plus:** Das Blockieren von Webung rediziert nicht nur die Belästigung. Da das Tor-Netz langsam ist, wird auch der Seitenaufbau beschleunigt, wenn überflüssige Daten nicht geladen werden.
- Da sich im Tor Netzwerk nicht nur die good guys tummeln, sollte man den Abschnitt "HTTPS-Security" im Kapitel "Spurenarm Surfen" beachten. Das Add-on **Certificates Patrol** wird dringend empfohlen.
- Datensparsame Suchmaschinen wie Ixquick-SSL, Scroogle, Startingpage-SSL, DuckDuckGo-SSL, Wikipedia-SSL usw. installiert man von mycroft.mozdev.org.

Je nach Nutzung können einige weitere Add-ons sinnvoll sein: SSL Blacklist, PwdHash, oder für anonyme Downloads von Flash-ideos den DownloadHelper bzw. UnPlug.

Es gibt einige Add-ons, die ähnliche Aufgaben wie TorButton übernehmen wollen und damit den Einstellungen von TorButton in die Quere kommen.

Nicht immer ist dabei klar, welches Plug-In zuerst abgearbeitet wird. Um diese Konflikte zu verweiden sollte auf das Add-on UserAgentSwitcher in jedem Fall verzichtet werden. TorButton setzt beim anonymen Surfen eine einheitliche User-Agent Kennung.

Anonymitätstest

Nachdem die Software installiert und der Browser konfiguriert ist, möchte man wissen, ob es auch funktioniert und der Datenverkehr jetzt anonym über den Onion Router läuft.

- TorButton bietet im Einstellungsdialog auf dem Reiter *Proxy-Einstellungen* ein Knöpfchen für den Test.
- Torproject.org bietet unter https://check.torproject.org eine Testseite. Wenn eine grüne Zwiebel angezeigt wird: Herzlichen Glückwunsch.
- Umfangreicher testet der Anonymitätstest von JonDonym. Hier wird auch geprüft, ob man durch FTP-Links, Flash-Applets oder Java-Applets deanonymisierbar ist. http://what-is-my-ip-address.anonymous-proxy-servers.net/

11.5.4 Tor Hidden Services

Das Tor Netzwerk ermöglicht nicht nur den anonymen Zugriff auf herkömmlich Angebote im Web sondern auch die Bereitstellung anonymer, zensurresitenter und schwer lokalisierbarer Angebote auf den Tor-Nodes. Der Zugriff auf die Tor Hidden Services ist nur über das Tor Netzwerk möglich. Wer Probleme mit der Installation von Tor hat oder unterwegs ist, kann usere Web-Proxys für den Zugriff auf Tor Hidden Services nutzen:

- https://www.awxcnx.de/tor-i2p-proxy.htm
- https://privacybox.de/tor-proxy.en.html

Die kryptische Adresse mit der Endung .onion dient gleichzeitig als Hashwert für ein System von Schlüsseln, welches sicherstellt, das der Nutzer auch wirklich mit dem gewünschten Dienst verbunden wird.

Hidden Wiki und Linklisten

Sie dienen als erste Anlaufstelle für die Suche nach weiteren Hidden Services.

- http://kpvz7ki2v5agwt35.onion/wiki (Hidden Wiki)
- http://dppmfxaacucguzpc.onion (Tor Directory)

Suchmaschinen

Die derzeit einzige Suchmaschine für Tor Hidden Services ist Torgle http://oqznfi3tdo6nwg3f.onion

Wikileaks.org Submission

Um die Whistleblower zu schützen, bietet Wikileaks.org einen Tor Hidden Service für Submission von Dokumenten unter http://suw74isz7wqzpmgu.onion.

Foren und Blogs

Das Onion-Forum http://l6nvqsqivhrunqvs.onion bietet Diskussionen zu vielen Themen. Die deutsche Sektion ist allerdings im Moment von SPAM dominiert.

Torando unter http://xqz3u5drneuzhaeo.onion/users/a1cerulean ist eine Hidden Community (im Aufbau).

Tor Messaging

Tor Privat Messaging unter http://4eiruntyxxbgfv7o.onion/pm/ bietet die Möglichkeit, Text-Nachrichten ohne Attachements unbeobachtet auszutauschen. Der Dienst erfordert das Anlegen eines Accounts. Das Schreiben und Lesen der Nachrichten erfolgt im Webinterface.

Usenet Server

Noauth bietet unter http://fehw2z6yc3exfmgk.onion/news/ ein Webinterface für einige alt.* Newsgruppen. Schreiben von anonymen Artikeln ist möglich und in diesen Newsgruppen expliziet erlaubt.

Jabber-Server

Server die ein anonymes Konto für Instant-Messaging via XMPP ermöglichen, stehen unter den folgenden Adressen bereit:

- ww7pd547vjnlhdmg.onion
- 3khgsei3bkgqvmqw.onion

torchat Adressen

torchat ist ein Instant Messenger, der ohne zentralen Server auskommt und die Verbindung abhörsicher und VDS-frei von Tor-Client zu Tor-Client routet. Die Userkennungen entsprechen den kryptischen Onion-Adressen. Eine Liste mit einigen Adressen findet man unter http://eqt5g4fuenphqinx.onion/page/33.

Hidden Hosting

Bei Freedom Hosting unter http://xqz3u5drneuzhaeo.onion kann man eine eigene Website im Onionland veröffentlichen, wenn man keinen TOR-Node hat, der ständig im Netz erreichbar ist.

Remailer-Webinterface

Unter der Adresse http://a5ec6f6zcxtudtch.onion/anon-email.htm ist es möglich, eine E-Mail oder ein Newsposting anonym und ohne Hinweise auf den Absender zu versenden.

Vertrauenfrage

Für die Hidden Services gibt es (noch) kein Vertrauens- und Reputationsmodell. Unter dem Deckmantel der Anonymität tummeln sich aber nicht nur Gutmenschen. Anonym bereitgestellten Dateien sollte man immer ein gesundes Misstrauen entgegen bringen. In Diskussionen wird aus dem Deckmantel der Anonymität heraus alles mögliche behauptet.

11.6 Anonyme E-Mails mit Thunderbird

Nicht nur beim Surfen, sondern auch bei jedem Versenden und Abrufen von E-Mails werden IP-Adresse 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 Anonymiserungsdienst (JonDonym, Tor) zu nutzen. Sollte die Angabe einer bereits vorhandene E-Mail Adresse nötig sein, kann man Wegwerf-Adressen nutzen. Einige Vorschläge für E-Mail Provider:

- https://www.fastmail.fm
- https://www.secure-mail.biz/
- http://www.aktivix.org
- https://rosposta.com
- https://www.hushmail.com

Wenn der neue E-Mail Provider die Angabe einer bereits vorhandenen E-Mail Adresse verlangt, können Wegwerf-Adressen genutzt werden. Auch zum Lesen der eingehenden Nachrichten beim Anbieter der temporären Wegwerf-Adresse ist ein Anonymisierungsdienst zu nutzen.

Thunderbird-Profil erstellen

Wir empfehlen, für anonyme E-Mail Accounts ein eigenes Profil in Thunderbird zu erstellen. Das gewährleistet eine konsequente Trennung von anonymer und nicht-anonymer E-Mail Kommunikation. Anderenfalls kommt man bei mehreren Konten schnell einmal durcheinander und gefährdet durch eine hektisch versendete Mail die Anonymität des geschützten Postfaches.

Auch für Thunderbird kann man das Add-on *ProfilSwitcher* verwenden. Ohne das Plug-In startet man den Profil-Manager von Thunderbird in der Konsole mit der Option -P:

```
> thunderbird -P
```

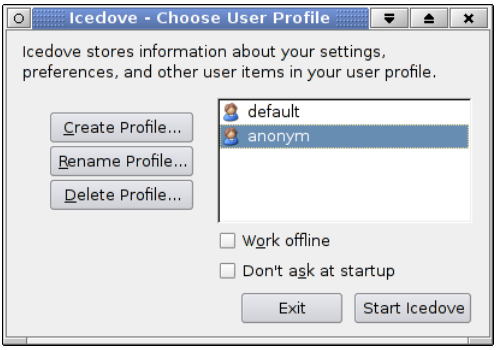


Abbildung 11.15: Profilmanager für Thunderbird

Es öffnet sich der Dialog Bild 11.15 zur Verwaltung verschiedener Profile.

Es ist ein neues Profil zu erstellen und die Option *Dont ask at startup* zu deaktivieren. In Zukunft wird Thunderbird genau wie Firefox bei jedem Start fragen, welches Profil genutzt werden soll.

Thunderbird-Profil konfigurieren

Beim ersten Start des neuen Profil *anonym* wird auch der Assistent für das Anlegen eines E-Mail Kontos automatisch gestartet. Achtung: der Assistent baut zum Test der Mail-Server eine Verbindung zum Provider auf. Da noch kein anonymiserender Proxy konfiguriert wurde, ist der Assistent erst einmal zu beenden. Er kann später wieder gestartet werden.

1. **Tor:** Um im Profil *anonym* den Datenverkehr durch zu jagen, sind die Proxy-Einstellungen wie im Bild 11.16 zu konfigurieren.

   ```
   Host: localhost
   Port: 9050
         SOCKS v5
   ```

2. **Jon>Donym:** Statt Tor kann man auch die Premium-Dienste von JonDonym nutzen. Die Kaskaden mit dem notwendigen SOCKS-Support sind mit einem roten, geschwungenen S gekennzeichnet. JonDonym hat

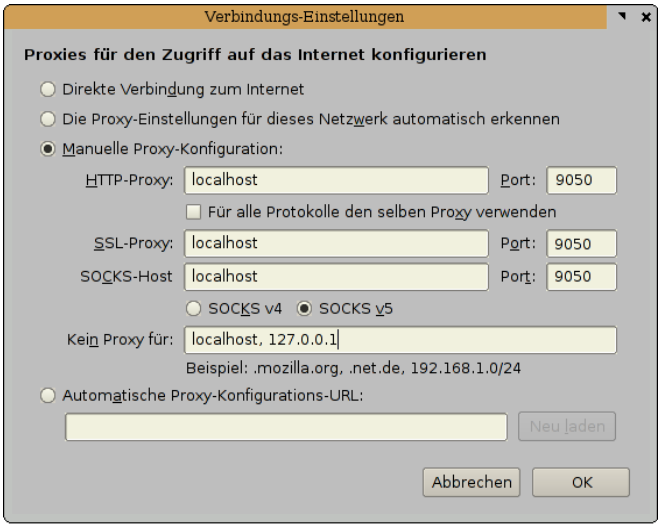


Abbildung 11.16: Proxy-Einstellungen in Thunderbird

im Gegensatz zu Tor keine Probleme mit DNSBL (siehe untern). Auch das Senden von Mails via SMTP ist auf Anhieb problemlos möglich. Es sind folgende Einstellungen für HTTP-, HTTPS- und SOCKS-Proxy zu wählen:

```
Host: localhost
Port: 4001
      SOCKS v5
```

Außerdem ist für beide Varianten (Tor, JonDonym) die Variable **network.proxy.socks_remote_dns** in den erweiterten Einstellungen auf **true** zu setzen, um DNS-Leaks zu vermeiden. Die erweiterten Einstellungen findet man im Dialog *Einstellungen* in der Sektion *Erweitert* auf dem Reiter *Allgemein*.

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. Die GPF beteibt einen sauberen Tor Exit Node *gpfTOR3*, bei dem wir dafür sorgen, dass er nicht in den Spamlisten auftaucht. Über diesen Exit-Node ist das anonyme Senden von E-Mails in der Regel problemlos möglich.

Die Konfiguration erfolgt mit der Option *MapAddress* in der Config-Datei *torrc* (alles in eine Zeile schreiben!). Der Traffic zu dem angegebenen SMTP-Host wird über Exit-Node mit dem Fingerprint $.... geleitet.

```
MapAddress smtp.privatdemail.net
smtp.privatdemail.net.$6D3EE5088279027AD8F64FF61A079DC44E29E3DF.exit
```

Möchte man die E-Mails von einem Tor Hidden Service abrufen, erhält man in der Regel 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.

11.7 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 und das OTR-Plugin für das Jabber-Protokoll ermöglicht eine starke Verschlüsselung.

Das Bild 11.17 zeigt die Konfiguration für einen anonymen Account in Pidgin. Als Proxy-Einstellungen sind folgende Werte zu setzen:

Abbildung 11.17: Proxy-Einstellungen in Pidgin

	Tor Onion Router	JonDonym Premium
Type	SOCKS5	HTTP
Host	localhost	localhost
Port	9050	4001

11.8 Anonymes Peer-2-Peer 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 an anonymen Varianten für 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 deanonymiseren. 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.
https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea

Die *privacy attacks for bittorrent over tor* gelten auch für alle anderen Anon-Dienste.

Anonymes Peer-2-Peer Filesharing

Es gibt einige Projekte, die Möglichkeiten für anonymes Filesharing entwickeln.

- **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 veteilen.
  - http://www.turboupload.com/
  - http://www.filefactory.com/
  - http://www.share-now.net/
  - http://files.ww.com/
- **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 zensur-resistentes Filesharing ohne zentrale Server. Alle Teilnehmer leiten Daten für andere Teilnehmer weiter und stellen selbst Dateien bereit. Da weitergeleitet 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/.
- **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 Anonmos-Tracker bekannt sein müssen. Download und Informationen auf der Projektwebsite http://anomos.info.

11.9 Nicht-proxyfähige Internetanwendungen

Mit Hilfe von proxifier-Tools können auch Applicationen anonymisoert werden, die keine Unterstützung für Proxies bieten. Unter Windows kann man Widecap nutzen (http://widecap.com). Linux/UNIX Distributionen enthalten das nette Tool *proxychains*.

proxychains für Linux/UNIX

Nachdem man *proxychains* mit dem Paketmanager der Distribution installiert hat, ist die Standardkonfiguration bereits für Tor Onion Router vorbereitet. Sollen statt Tor die Premium-Dienste von JonDonym genutzt werden, ist eine Konfigurationsdatei in *$(HOME)/.proxychains/proxychains.conf* zu erstellen:

```
strict_chain
proxy_dns
[ProxyList]
http 127.0.0.1 4001
```

Um den Traffic beliebiger Anwendungen zu anonymisieren, startet man die Anwendung unter Kontrolle von *proxychains*. Unbeobachtete Administration eines Servers mittels SSH ist möglich mit:

```
proxychains ssh user@server.tld
```

Den Instant Messenger Kopete (KDE/Linux) kann man anonymisieren:

```
proxychains kopete
```

11.10 Tor Bad Exit Nodes

Ein sogenannter *Bad-Exit-Node* im Tor-Netz versucht den Traffic zu beschnüffeln oder zusätzliche Inhalte in eine (nicht SSL-gesicherte) Website einzuschmuggeln. Bedingt durch das Prinzip des Onion Routings holt der letzte Node einer Kette die gewünschten Inhalte. Diese Inhalte liegen dem Node im Klartext vor, wenn sie nicht SSL- oder TLS-verschlüsselt wurden.

Durch einfaches Beschnüffeln wird die Anonymität des Nutzers nicht zwangsläufig kompromittiert, es werden meist Inhalte mitgelesen, die im Web schon verfügbar sind. Erst wenn Login-Daten unverschlüsselt übertragen werden oder man-in-the-middle Angriffe erfolgreich sind, können die Bad Exit Nodes an persönliche Informationen gelangen. Persönliche Daten, bspw.

Login Daten für einen Mail- oder Bank-Account, sollten nur über SSL- oder TLS-gesicherte Verbindungen übertragen werden. Bei SSL-Fehlern sollte die Verbindung abgebrochen werden. Das gilt für anonymes Surfen via Tor genauso, wie im normalen Web.

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	$3163a22dc3849042f2416a785eaeebfeea10cc48
tortila	$acc9d3a6f5ffcda67ff96efc579a001339422687
whistlersmother	$e413c4ed688de25a4b69edf9be743f88a2d083be
BlueMoon	$d51cf2e4e65fd58f2381c53ce3df67795df86fca
TRHCourtney1..10	$F7D6E31D8AF52FA0E7BB330BB5BBA15F30BC8D48
	$AA254D3E276178DB8D955AD93602097AD802B986
	$F650611B117B575E0CF55B5EFBB065B170CBE0F1
	$ECA7112A29A0880392689A4A1B890E8692890E62
	$47AB3A1C3A262C3FE8D745BBF95E79D1C7C6DE77
	$0F07C4FFE25673EF6C94C1B11E88F138793FEA56
	$0FE669B59C602C37D874CF74AFEA42E3AA8B62C6
	$E0C518A71F4ED5AEE92E980256CD2FAB4D9EEC59
	$77DF35BBCDC2CD7DB17026FB60724A83A5D05827
	$BC75DFAC9E807FE9B0A43B8D11F46DB97964AC11
Unnamed	$05842ce44d5d12cc9d9598f5583b12537dd7158a
	$f36a9830dcf35944b8abb235da29a9bbded541bc
	$9ee320d0844b6563bef4ae7f715fe633f5ffdba5
	$c59538ea8a4c053b82746a3920aa4f1916865756
	$0326d8412f874256536730e15f9bbda54c93738d
	$86b73eef87f3bf6e02193c6f502d68db7cd58128

   Die genannten Nodes sind nicht mehr online, die Liste ist nur ein Beispiel.

2. Die folgenden Nodes wuden 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 ermitteln. 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 modifizieren.

Beide Tor Nodes gingen kurz nach ihrer Entdeckung offline. Inzwischen können die Geheimdienste durch Zusammenarbeit mit kompromittierten Certification Authorithies gültige SSL-Zertifikate fälschen. Diese man-in-the-middle Angriffe sind sehr schwer erkennbar.

3. Das 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. Die Nodes aus dem IP-Adressbereich 149.9.0.1/16 stehen in dem Verdacht, für US-Dienste zu schnüffeln:

`myrnaloy`	`$8FF73B8FBFBF2CCB52A8E46A515418F97A69C812`
`nixnix`	`$43BE706E24143AB6B3B86DBF7CD4FDE1E0C4CAF1`
`jalopy`	`$35BDC6486420EFD442C985D8D3C074988BFE544B`
`croeso`	`$CE6747CFAE6F260B3EF6965AD5DE0F1E1BEF240E`
`bettyboop`	`$D7F821F181CC1B811758E2FEE3EF1E9AD856D06D`

Es gibt für das Schnüffeln dieser Nodes nur Anhaltspunkte, keine Beweise.

- Sie laufen alle bei einem Betreiber, der bisher nicht durch Privacy-Aktivitäten aufgefallen ist. Kosten aber sicher einiges an Geld.
- Sie nutzten lange Zeit eine sehr veraltete, evtl. modifizierte Version von Tor.
- Sie verwenden eine Exit-Policity, die diese These unterstützt. (accept *:80, accept *:110, accept *:5222...) Die Nodes sind nur an unverschlüsseltem Traffic interessiert, evtl. um Daten auszuspähen.
- Eine Kontaktadresse des Betreibers ist nicht angegeben. Trotz Bemühungen der Community konnten Betreiber nicht ermittelt werden.

Ein passiv schnüffelnder Tor-Node ist nicht erkennbar. Neben den hier gelisteten Nodes gibt es sicher weitere Nodes, die mit unterschiedlichen Interessen den Datenverkehr beobachten. Es wäre eine mühselige Sysiphos-Arbeit, jedem Verdacht und jeder Verschwörungstheorie nachzugehen und einzelen Nodes zu sperren. Effektiver ist es, nur vertrauenswürdige Nodes als Exit zu nutzen.

11.11 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...). Wir gehen davon aus, dass es verschiedene Organisationen gibt, die mit unterschiedlichen Interessen im Tor Netz nach Informationen phishen. Auch SSL-verschlüsselte Verbindungen sind nicht 100% geschützt. C. Soghoian und S. Stamm haben in einer wiss. Arbeit gezeigt, dass Geheimdienste wahrscheinlich in der Lage sind, gültige SSL-Zertifikate zu faken.

Als Verteidigung können Nutzer in der Tor-Konfiguration Exit Nodes angeben, denen sie vertrauen und ausschließlich diese Nodes als Exit-Nodes nutzen. Welche Nodes vertrauenswürdig sind, muss jeder Nutzer selbst entscheiden, wir können nur eine kurze Liste als Anregung zum Nachdenken liefern.

- Die von der GPF/SPF betriebenen Server sammlen keine Informationen. Eine Liste unserer Server ist online unter https://www.privacyfoundation.de/service/serveruebersicht
- Der CCC betreibt nach eigenen Aussagen die 4 Tor Nodes: chaoscomputerclub42, chaoscomputerclub23 (wird ergänzt, sobald verifiziert)
- Der Node FoeBud3 wird wirklich vom FoeBud betrieben.
- ...wird fortgesetzt.

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 angeggeben 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.

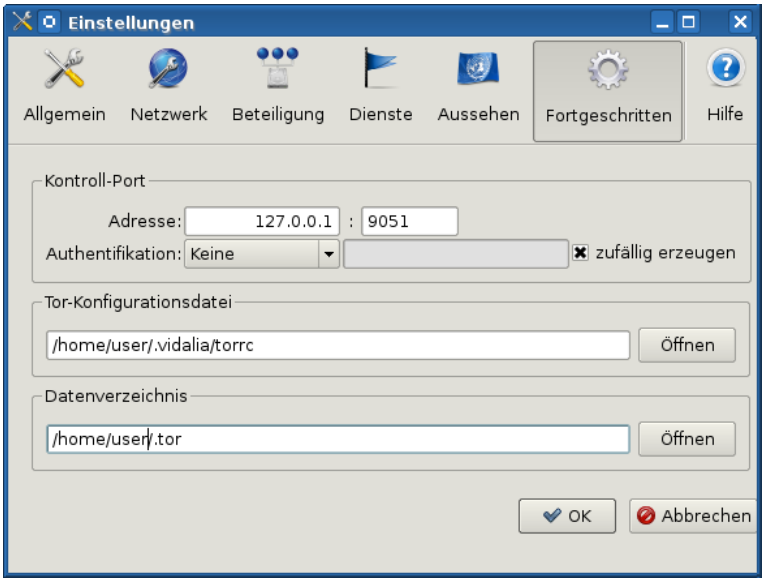


Abbildung 11.18: torrc in Vidalia auswählen

11.12 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 verschlüssellt 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.

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

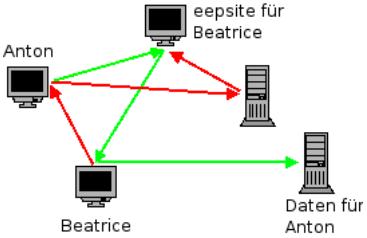


Abbildung 11.19: Prinzip von I2P

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.

11.12.1 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.

I: 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. Aktuelle Distributionen enthalten die freie Implementierung *openjdk-6-jre* oder das Original *sun-java6-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 11.20: 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.

- **Debian** und **Ubuntu:** für diese Distributionen bieten wir fertige DEB-Pakete zur Installation in unserem Repository. Die Install-Routine installiert die Software, richtet einen System-User ein sowie die Start- und Stopscripte für den Reboot ds Rechners. https://www.awxcnx.de/wabbel.htm

- **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
```

  Das Datei *i2pinstall-0.x.y.exe* ist im HOME-Verzeichnis des eingeschränkter User 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 su 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, im sich im Invisible Internet zu orientieren. Zum Warmlaufen sollte man ihm 30min Zeit lasen. Wenn es danch noch immer nicht so richtig funktioniert, sind die Netzwerkeinstellungen zu prüfen. Die Startseite der Router-Console gibt einige Hinweise.

11.12.2 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 forgeschrittene Internetnutzer)

- Evtl. ist auf einem Gateway/Router ein Port Forwarding für den UDP Port zu konfigurieren.
- Außerdem braucht man einen DNS-Namen oder 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 *configuation* (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 abbonieren. Die Einstellungen für SusiDNS findet man in der Router Konsole. Subscriptions kann man unter der Adresse http://localhost:7657/susidns/subscriptions.jsp einfügen. (Bild 11.21)

Abbildung 11.21: 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
```

11.12.3 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 Internet zu surfen.

Firefox konfigurieren

Wir empfehlen, für das Surfen im Invisible Internet ein seperates Firefox-Profil zu erstellen. Dann ist es für spionierenden Websites gänzlich unmöglich, im Cache oder 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 11.22) 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 11.22: Firefox Profil-Manager

Anschließend kann das Profil *I2P-Fox* gestartet werden und die Proxy-Einstellungen sind wie im Bild 11.23 gezeigt zu konfigurieren. Die allgemeinen Hinweise zu Cookies, Javascript, Plug-Ins, HTTPS-Security usw. im Abschnitt Spurenarmen Surfen gelten auch für I2P. Das Profil *I2P-Fox* ist entsprechend zu konfigurieren.

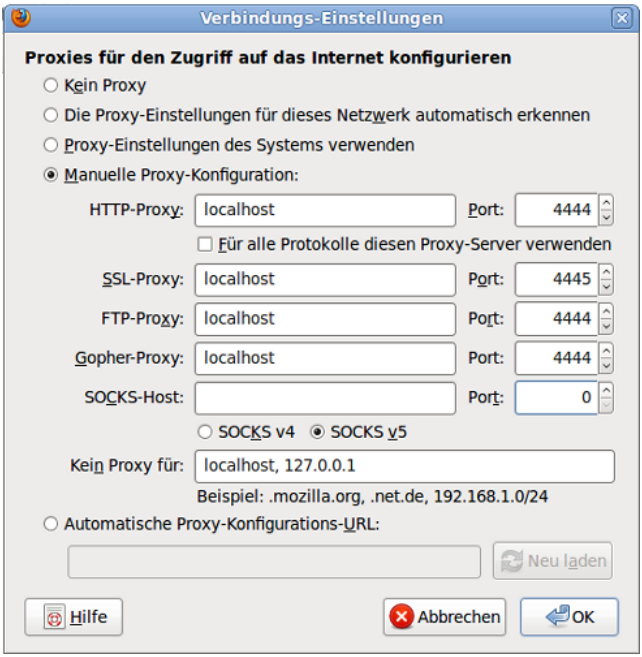


Abbildung 11.23: Firefox Proxy-Einstellungen für I2P

Wer den Aufwand des ständigen Profil-Wechsel vermeiden möchte, kann ein Proxy-Switcher als Plug-In installieren. Es gibt mehrere Plug-Ins für Firefox, die eine einfache Umschaltung zwischen verschiedenen Proxyeinstellungen erlauben:

- QuickProxy: https://addons.mozilla.org/de/firefox/addon/1557
- SwitchProxy: https://addons.mozilla.org/de/firefox/addon/125

11.12.4 I2P Mail 1 (Susimail)

Die Anwendung Susimail ist integraler Bestandteil von I2P und ermöglicht den unbeobachteten Austauch 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 Emfängern 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.

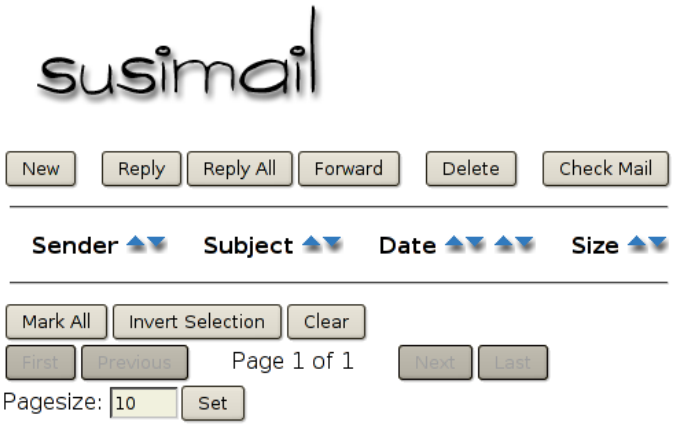


Abbildung 11.24: Webinterface von Susimail

Es bietet eine simple Möglichkeit, Mails abzurufen und zu versenden. Kom-

fortabler 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.

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+Privoxy als Proxy nutzt. Sollte der E-Mail Client ständig den Fehler TIMEOUT liefert, 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, folgene 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 dem Server viele tote Mail-Accounts, wo noch immer Mails eingehene (Spam und Mailinglisten) und die viel Speicherplatz verbrauchen.

5. Bitte verwendet den Dienst nicht, um anonym Beleidigungen oder Drohungen zu schreiben bzw. anderweitig strafrechtlich relevant. Das bringt den Betreibern Ärger und gefährdet den reibungslosen Betrieb.

Englischer Orginaltext bei HQ Postman: http://hq.postman.i2p/?p=63

11.12.5 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 ohne Anhänge.
- 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 11.25).

Abbildung 11.25: Installation des Plug-in I2P Bote

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:

```
http://tjgidoycrw6s3guetge3kvrvynppqjmvqsosmtbmgqasa6vmsf6a.b32.i2p/i2
```

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"*.

Abbildung 11.26: Neue Identät 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 11.27 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.

Abbildung 11.27: Neue E-Mail in I2P Bote schreiben

Eingehende Mails findet man im Ordner *Posteingang* und weitere Fragen beantworten bestimmt die FAQ von I2P Bote unter http://i2pbote.net/faq.html.

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 Häckchen in der Spalte **Bek**.

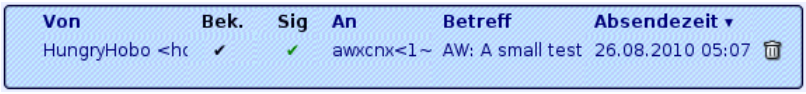


Abbildung 11.28: Inbox mit verifiziertem Absender

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 zb. OpenPGP zu nutzen, um die Vertraulichkeit der Nachricht zu gewährleisten.

11.12.6 I2P BitTorrent

Der I2P-Router bietet auch eine angepasste Implementierung des BitTorent Protokolls für anonymes Peer-2-Peer Filesharing. Im Gegensatz zum Nutzung von normalem BitTorrent über Tor ist die Implementierung des Invisble Internet Project anonym und die Nutzung ausdrücklich erwünscht. Der Dienst bietet Optimierungen mit speziellen Clients.

Die I2P-Router-Konsole bietet einen einfachen BitTorrent Client als Webinterface unter *Torrents* (http://localhost:7657/i2psnark).

Die zum Tausch bereitgestellten oder heruntergeladenen Dateien findet man im Unterverzeichnis *i2psnark* der I2P-Installation. Dieses Verzeichnis sollte Lese- und Schreibrechte für alle lokalen User haben, die I2PSnark nutzen

Abbildung 11.29: I2PSnark BitTorrent-Client im Webinterface

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 herunter geladenen Dateien auch anderen Teilnehmern zur Verfügung. Bei BitTorrent im normalen Netz gilt es als freundlich, wenn man heruntergeladenen Dateien mindestens für 2 Tage zum Upload anbietet oder bis die Datenmenge des Upload das 2,5fache des Down-

loads beträgt. Da die Geschwindigkeit im I2P-Netz wesentlich geringer ist, sollte man herunter geladenen Dateien mindestens für 1 Woche zum Upload anbieten.

11.13 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.

11.13.1 CyberGhost VPN

Die VPN-Technologie wurde nicht für den Anonymisierung entwickelt. Sie dient dem Datenaustausch zwischen zwei vertrauenswürdigen Endpunkten über unsichere Netze. Um Kosten zu sparen, definieren sich einige Anbieter von Anonymisierungslösungen selbst als 100% vertrauenswürdig und nutzen die VPN-Technik.

Besonders CyberGhost VPN fällt durch aggressive Vermarktung in Deutschland auf. Wir haben vier Werbebotschaften von CyberGhost etwas näher betrachtet.

100% anonym im Internet, TÜV geprüft (2008)

> *Mit Hilfe von Cyberghost soll jeder - völlig kostenfrei - 100 % anonym im Internet surfen, Files downloaden oder Dateien austauschen können.*

Im Gegensatz zum großen Bruder Bild ist die ComputerBild geradezu subversiv. So hieß das Titelthema des Heftes 24/2008 *Anonym Surfen*. Anbei eine CD mit einem Programm des Anonymisierungsdienstes CyberGhost inklusive eines Jahresaccounts, der sonst 70,- Euro kostet. Die Stimme des Volkes sollte sich nun auch im Internet frei artikulieren können.

CyberGhost leitet den Datenverkehr über einen einzelnen schnellen Proxy und verschleiert so die IP-Adresse ohne dass dies allzu viel Zeit kostet. Die Server stehen überwiegend in Deutschland. ComputerBild Leser sollen ihre Anonymität ohne Komforteinbußen genießen können.

Geht das tatsächlich? Ja, das sagt sogar der TÜV. Die ComputerBild ließ den Dienst vom Tochterunternehmen LGA testen:

> *Das Ergebnis: Mit der Premium-Version von CyberGhost VPN bleiben ihre Wege im Internet verborgen. Eine Garantie, die bisher einmalig ist.*

Damit stand dem Erfolg nichts mehr im Wege. Das Siegel einer Behörde hat für den Deutschen den gleichen Wert wie für einen Italiener der Segen des Papstes. Die Leute rissen den Händlern die Hefte aus den Händen, manche kauften sogar mehrere.

Fachleute hätten allerdings vorher die Frage gestellt, inwiefern der TÜV überhaupt 100prozentige Sicherheit garantieren kann. Indizien sprechen gegen seine Kompetenz. Wäre der TÜV-Prüfer in der Lage gewesen, einen Browser zu bedienen, hätte er vielleicht einen Beitrag im CyberGhost-Forum gefunden: http://www.sad-forum.de/board/index.php?page=Thread&threadID=398.

Dort fragt ein Kunde, ob es möglich wäre, die Verbindung zu unterbrechen, wenn der Kontakt zum CG-Proxy abreißt. Sie haben richtig gelesen! Schon ein halbes Jahr vor der TÜV-Prüfung stellte ein Nutzer fest, das der CyberGhost Client einfach die reale IP-Adresse sendet, wenn CG nicht erreichbar ist, was alle paar Stunden mal vorkommt.

Wie soll man anonym ein regierungskritisches Blog betreiben, wenn man bei jedem dritten Einloggen die eigene IP-Adresse in den Logs hinterlässt?

In der aktuellen Version sollen diese Probleme behoben sein. Beim kostenfreien Basic-Account ist der Abbruch der Verbindung ohne automatische Neuverbindung kein Bug, sondern ein fest eingebautes Feature. Es ist kein Bug, wenn man als nicht-zahlender Kunde rausgeworfen wird.

100%-Anonymität trotz Vorratsdatenspeicherung (2009)

Eine weiteres unseriöses Werbemärchen ist die garantierte 100%-Anonymität trotz Vorratsdatenspeicherung im Jahr 2009. Auszug aus einem Rundschreiben an alle Nutzer:

> *Die gute Nachricht zuerst: Mit CyberGhost VPN surfen Sie auch in 2009 100% anonym.*
>
> *Da wir zur Datenvorratspeicherung verpflichtet sind, speichern wir ab dem 01.01.2009 für sechs Monate bei jeder Verbindung mit einem CyberGhost-Server (Premium oder Basic) folgende Verkehrsdaten:*

Die Kennung (User-ID und Einwahl-IP-Adresse) und die IP-Adresse des zugewiesenen CyberGhost-Servers und den Zeitpunkt (Datum und Uhrzeit) des Logins auf den Server sowie den Zeitpunkt (Datum und Uhrzeit) des Logouts vom Server.

Die versprochene 100%-Anonymität ergibt sich laut Erklärung der Betreiber einzig aus dem Fakt, dass zu einem beliebigen Zeitpunkt mehrere Surfer einen CyberGhost-Server nutzen und die Deanonymisierung mittels IP-Adresse damit mehrdeutig wäre. Der Serverstatus von CyberGhost zeigt im Moment (März 2011) 46 aktive Server mit insgesamt ca. 1.000 User an. Im Mittel nutzen also nur 22 User die gleiche IP-Adresse.

CyberGhost verschweigt, das mit wenigen Log-Einträgen zu unterschiedlichen Zeitpunkten durch einfache Schnittmengenbildung ein Nutzer mit hoher Wahrscheinlichkeit deanonymisiert werden kann. Man braucht nur die VDS-Daten von 3-4 Zeitpunkten, als der Nutzer online war und den Dienst nutzte. Diese Zeitpunkte kann man mit Leimruten, Zeitstempeln von Blog-Kommentaren oder -veröffentlichungen... relativ einfach einsammeln. Ein Beispiel:

1. Das BKA launcht eine neue Honeypot-Website zu einem Thema, bei sie mit ihren Ermittlungen nicht weiterkommen. Dieser Ansatz wurde schon mehrfach praktiziert: Die Leimruten des BKA.
2. Da dem BKA die Speicherung und Auswertung der IP-Adressen der Besucher 2009 untersagt wurde, springt das BSI ein, wenn ein Richter dieser Fahndungsmethode zugestimmt hat.
3. Ein Journalist, der intensiv zu dem Thema recherchiert, besucht an einigen Tagen 2-3x die Website, um sich über aktuelle Entwicklungen zu informieren. Da er über die Leimruten informiert ist, verwendet er Cyberghost und meint, er wäre damit hinreichend anonym.
4. Das BKA erhält vom BSI die Adressen der Besucher und fragt bei Cyberghost nach den passenden VDS-Daten.
5. Wenn der Jounalist Pech hatte, fast den ganzen Tag online war oder sein Zugangsprovider die IP-Adresse zwischen mehreren Aufrufen des Honeypot nicht wechselte, bringt die Schnittmenge der verschiedenen Zeitpunkte ein eindeutiges Ergebnis.

Mit dem vorläufigen Ende der VDS bewies CyberGhost echte Marketing Qualitäten: **Wir löschen als Erste!** (Richtige Anonymisierungsdienste haben nie gespeichert.)

Hohe Anonymität bei der Nutzung von BitTorrent

Als drittes Werbemärchen ist die in den FAQ von Cyberghost beworbene hohe Anonymität bei der Nutzung von BitTorrent zu nennen. Der hohe Traffic bei P2P-Filesharing spült natürlich Geld in Kassen von Cyberghost. Die von TorProject.org erstellten *privacy attacks for bittorrent over tor* gelten aber auch für alle anderen Anonymisierungsdienste. (Inzwischen wurde die Werbung für BitTorrent aus den FAQ entfernt.)

Trotz der bestehenden Mängel und der schwachen Anonymität wurde Cyberghost von der ComputerBild 2009 zum Sieger im Vergleich der Anonymisierungsdienste gekürt (mit Vorratsdatenspeicherung!) und wird auch 2010 weiter gepusht. https://www.privacyfoundation.de/blog/category/cyberghost

Gegendarstellung von CyberGhost

CyberGost VPN wurde auf unsere bissigen Kommentare aufmerksam und möchte die Schieflage in unserer Darstellung etwas korrigieren. Die folgende Gegendarstellung haben wir unkomentiert übernommen.

> Zunächst einmal etwas Grundsätzliches: Es ist verständlich, dass ein kommerziell ausgerichtetes Unternehmen im Bereich Internet-Sicherheit prinzipiell misstrauisch beäugt wird. Wir leben in einer Welt, in der Wirtschaft und Staat nachweislich ihrer Verantwortung oftmals nicht (mehr?) nachkommen, siehe Tepco, siehe BP, siehe die gesamte europäische Lobbykratie. Gelder werden hin und her geschaufelt (meistens leider nur in einer Richtung) und die Anhäufung von Profit gilt als oberste Maxime, der alles untergeordnet wird. Diese Erfahrung haben wir alle gemacht und übertragen auf einen kommerziellen Anonymisierungsdienst nährt dies verständliche und gerechtfertigte Ängste. Man geht automatisch davon aus, dass bei einem Konflikt zwischen Anliegen und Geschäft der Gewinner von vornherein fest steht. Dieses Misstrauen können wir euch nicht nehmen und wollen es auch gar nicht. Das Prinzip der Anonymisierung ist zu wichtig, zumal in einigen Ländern sogar Menschenleben davon abhängen, als dass man es einer Marketing-Aktion unterordnet und mit lächerlichen Beruhigungssprüchen ernste Einwände wegbügelt. Womit ihr ins Spiel kommt, denn wir sehen euch als ebenso wichtig. Für uns und für andere, weil ihr euch stellvertretend mit diesen Themen auseinandersetzt und dafür sorgt, dass eine öffentliche Kontrolle

stattfindet und Menschen nicht für schnelles Geld verkauft werden.

Nichtsdestotrotz müssen wir ein paar Äußerungen auf diesem Blog korrigieren, weil sie unserer Meinung nach auf falschen Schlussfolgerungen und Annahmen beruhen und auch dem aktuellen Stand der Dinge bei uns nicht mehr entsprechen.

1. Der Bezug auf die Vorratsdatenspeicherung ist nicht mehr gegeben, wie im Beitrag vom 11.November 2009 beschrieben, und wird es so auch nicht mehr. Damals waren wir gezwungen, die VDS umzusetzen, da der Gesetzgeber einen VPN-Anbieter wie uns kurzerhand zu einem Provider umdefinierte. Die VDS wurde zwischenzeitlich vom Verfassungsgericht gekippt, wobei um eine Nachfolgeregelung nach wie vor auf politischer Ebene gerungen wird, aktuell als Mindestdatenspeicherung. Wird diese neue Regelung unseren Dienst kompromittieren, werden wir dagegen vorgehen, sehr wahrscheinlich werden wir aber bereits vorher Deutschland als Standort verlassen haben. Die Tatsache, dass verschiedentlich Provider wie die Telekom sehr langsam beim sofortigen Löschen der Verbindungsdaten vorgehen und auch schon mal ein paar Tage dafür brauchen, heißt ja nicht, dass wir dazu gehören. Wir gehören nicht dazu!

2. Die im Zusammenhang mit der VDS kommunizierte Schnittmengenbildung als Sicherheitsrisiko lässt außer Acht, dass diese von der Anzahl gleichzeitiger User und der User-Fluktuation auf den Servern abhängig ist. Sowie sich mehrere User auf dem CyberGhost-Server eingeloggt haben, ohne zwangsläufig auch ins Internet zu gehen (wie es bei uns der Fall ist, da wir beim Systemstart automatisch verbunden werden), ist die Schnittmengenbildung bereits ausgehebelt. Zu allen in dem Blog-Eintrag als Beispiel aufgeführten Zeitpunkten kämen zig User in Betracht. Davon abgesehen ist die VDS aber sowieso kein Thema mehr für uns (siehe oben).

3. Ihr sprecht immer noch von einem Sicherheits-Loch beim Verbindungsabbruch. Hierzu ist zu sagen, dass dies tatsächlich vor langer Zeit ein Problem war. Hey, wir sind nicht perfekt, haben aber schnell gelernt. CyberGhost wird stetig weiterentwickelt und mittlerweile wird die Internetverbindung bei einem Verbindungsabbruch komplett gesperrt, um eine De-Anonymisierung zu vermeiden. Und das nicht erst seit gestern.

4. Gekürzt, da *Datensafe* von uns nicht mehr genannt ist.

5. Zu guter Letzt: Wenn ihr Interesse habt, laden wir euch gerne zu uns ein. Ihr könnt Einblick in den Quellcode nehmen und euch mit unseren Programmierern austauschen. Wir wollen gerne wissen, welche Gefahren ihr seht, welche Befürchtungen ihr habt und wie wir unseren Dienst verbessern können. Und wir reden ausdrücklich nicht über Vertrauen, weil wir wollen, dass ihr misstrauisch bleibt und uns und den anderen Anbietern auch weiter auf die Finger klopft, wenn ihr meint, es läuft da etwas schief.

11.13.2 Free Hide IP

Free Hide IP wird gleichfalls von der Computerbild als Anonymisierungsdienst angepriesen.

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

Der Anoynymitätstest von JonDonym zeigt, dass der Dienst nicht einmal einfachste Anforderungen erfüllt. Nutzer können in mehreren Varianten deanonymisiert werden. Der Dienst schützt nicht einmal gegen die Deanonymisierung 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.

11.13.3 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?

11.13.4 CTunnel.com

Web-Proxys sind ein probates Mittel, um Zensur im Internet zu umgehen. Sie sind aber meist als Anonymisierungsdienste unbrauchbar. Mit einfachen Javascripten ist es möglich, die meisten Web-Proxys zu umgehen und die reale IP-Adresse ds Nutzers zu ermitteln.

CTunnel.com ist ein ganz besonderer Web-Proxy. Man verspricht zwar eine anonyme Nutzung des Internet. Die Entwickler haben sich große Mühe gegeben, die Nutzung des Dienstes mit deaktiviertem Javascript unmöglich zu machen. Der gesamte Inhalt der Website ist base64 encoded und wird von einer Javascript-Funktion geschrieben.

Die IP-Adressen der Nutzer werden bei aktiviertem Javascript gleich an drei Datensammler verschickt. Neben *Google Analytics* erhalten auch

xtendmedia.com und *yieldmanager.com* diese Information. Google Analytics ist bekannt, die beiden anderen Datensammler sind ebenfalls Anbieter von Werbung.

Die Website enthält keinen Hinweis auf die Datenweitergabe. Zumindest im Fall von Google Analytics besteht jedoch eine Informationspflicht.

Die Ereignisse rund um den Sahra-Palin-Hack zeigen, dass auch der Dienst selbst Informationen über die Nutzer speichert. Die Kommunikationsdaten werden selbst bei kleinen Vergehen an Behörden weitergegeben. Eine seltsame Auffassung von Anonymität.

11.13.5 Tor BlackBelt Privacy, Cloakfish unnd AdvTor

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 Modifaktionen 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 Betriebssystem aussreichen 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 verschieden 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.

Advanced Onion Router (AdvOR) soll eine verbesserte Version von Tor sein. Leider sind die Verbesserungen nur unzureichend dokumentiert. Da der Code von AdvOR aus verschiedenen Tor Versionen zusammengestückelt und damit schwer zu prüfen ist und außerdem nach Ansicht von Nick M. Sicherheitslücken enthält, raten die Tor Entwickler von der Benutzung ab (siehe OR-Talk: http://archives.seul.org/or/talk/Oct-2010/msg00026.html).

11.13.6 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 Proxylisten sind alles andere als anonym. So wurde beispielsweise im Mai 2007 in der Newsgruppe *alt.privacy.anon-server* eine Liste gepostet, die mit verschiedenen DNS-Namen für Proxies gut gefüllt war. Eine Überprüfung der Liste ergab, dass hinter allen die gleiche IP-Adresse und somit derselbe Server steckt. Der Betreiber des Servers erhält eine website-übergreifende Zusammenfassung des Surfverhaltens der Nutzer!

12 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.

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) und von einem sauberen USB-Stick booten.

5. Zur **Herausgabe von Schlüsseln** im Fall einer Beschlagnahme des Rechners oder verschlüsselten Datenträgers gibt es immer wieder Missverständnisse. In Deutschland gelten folgende gesetzlichen Reglungen:
    - 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.

12.1 Quick and Dirty mit GnuPG

Eine Möglichkeit ist die Verschüsselung einzelner Dateien mit GnuPG oder PGP. Einfach im bevorzugten Dateimanager mit der rechten Maustaste auf eine Datei klicken und den Menüpunk *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 Orginal 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 Orginal wieder auf der Platte.

12.1.1 GnuPG für WINDOWS

Diese simple Verschlüsselung klappt unter WINDOWS nicht auf Anhieb. Es ist die nötige Software zu installieren. Folgende Varianten können wir empfehlen:

1. Das Programmpaket **GnuPG-Pack** enthält neben einer aktuellen Version von GnuPG auch einige grafische Tools, welche die Arbeit vereinfachen. GPGSX ist eine Erweiterung für den Explorer, die Verschlüsseln, Entschlüsseln sowie sicheres Löschen (*Wipe...*) von Dateien und Ordnern mit wenigen Mausklicks ermöglicht. Mit einem Klick der rechten Maustaste auf eine Datei erhält man das in Bild **??** dargestellte Kontextmenü. Das Paket steht unter http://home.arcor.de/rose-indorf/ zum Download bereit.

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.

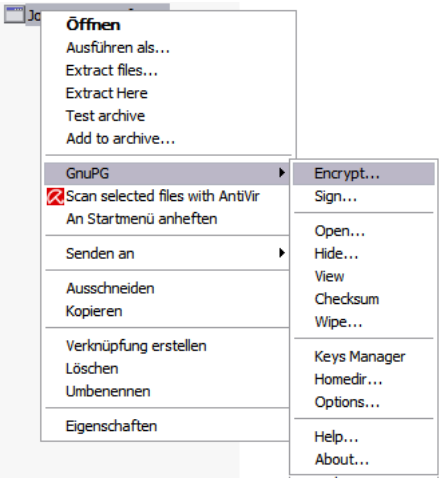


Abbildung 12.1: Kontextmenü einer Datei im Explorer

3. Die Programme **GnuPG** und **GPGShell**: GPGshell ist ein 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.

Startet man diese Tools nach der Installation, erscheint ein Assistent. Er bietet die Möglichkeiten, ein vorhandenes Schlüsselpaar zu importieren oder ein neues Schlüsselpaar zu generieren. Das Schlüsselpaar besteht aus einem öffentlichen Schlüssel für die Verschlüsselung und einem geheimen Schlüssel für die Entschlüsselung. Dann kann es losgehen.

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(!) Orginaldateien in den Reißwolf zu werfen.

12.1.2 GnuPG für KDE

Unter Linux sind alle benötigten Komponenten in der Regel installiert. Es ist ausreichend KGPG oder Kleopatra einmal zu starten. Ein Assistent führt

durch die die Schritte zur Generierung des Schlüsselpaares und installiert auf Wunsch auch einen Reißwolf auf dem Desktop.

Der Dateimanage *Konqueror* bietet im Kontextmenü einer Datei den Punkt *Aktionen / Datei verschlüsseln* und im Kontextmenü eines Verzeichnisses den Punkt *Aktionen / Ordner komprimieren und verschlüsseln*. Der sich öffnende Dialog bietet die Möglichkeit, alle nötigen Optionen auszuwählen.

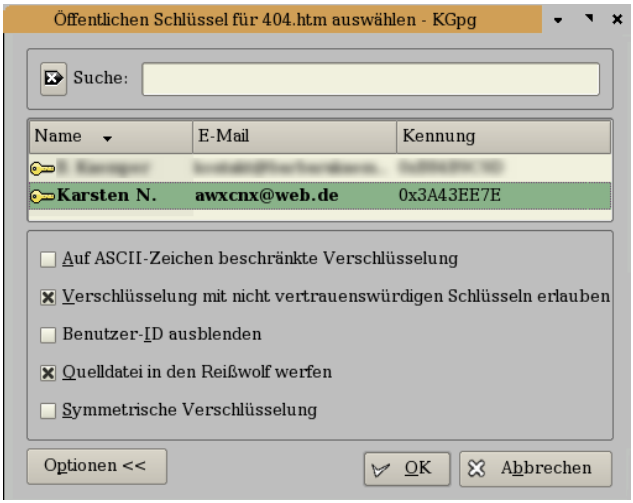


Abbildung 12.2: Verschlüsselungseinstellungen von KGPG

Soll die Datei für mehrere Empfänger verschlüsselt werden, ist bei der Auswahl der Schlüssel in der Liste die Taste <Strg> gedrückt zu halten.

Die Option *"Auf ASCII-Zeichen beschränkte Verschlüsselung"* bläht die verschlüsselte Datei unnötig auf, da nur 7 Bit eines Bytes genutzt werden. Diese Option kann für Backups in der Regel deaktiviert werden.

Die Option *"Quelldatei in den Reißwolf werfen"* bezieht sich auf die Datei, welche verschlüsselt werden soll. Wurde ein Verzeichnis komprimiert, bezieht diese Option sich auf das komprimierte temporäre Archiv. Die Orginaldateien des Verzeichnisses werden nicht vernichtet.

Wird die Option *"Symmetrische Verschlüsselung"* aktiviert, erfolgt die Ver-

schlüsselung nicht mit einem Public PGP-Schlüssel. Es wird statt dessen eine Passphrase verwendet. Die Entschlüsselung erfordert dann ebenfalls nur die Angabe dieser Passphrase und keinen Key.

12.1.3 Kleopatra für KDE 4.x

KDE 4.x enthält neben KGPG auch das Tool Kleopatra. Es kann neben OpenPGP-Schlüsseln auch S/MIME-Zertifikate für die Verschlüsselung nutzen. Wie bei KGPG findet man die Menüpunkte im Kontextmenü einer Datei oder eines Verzeichnisses unter *Aktionen*. Bei Auswahl der Ver- oder Entschlüsselung mit Kleopatra öffnet sich ein Assistent, der schrittweise durch den Prozess führt.

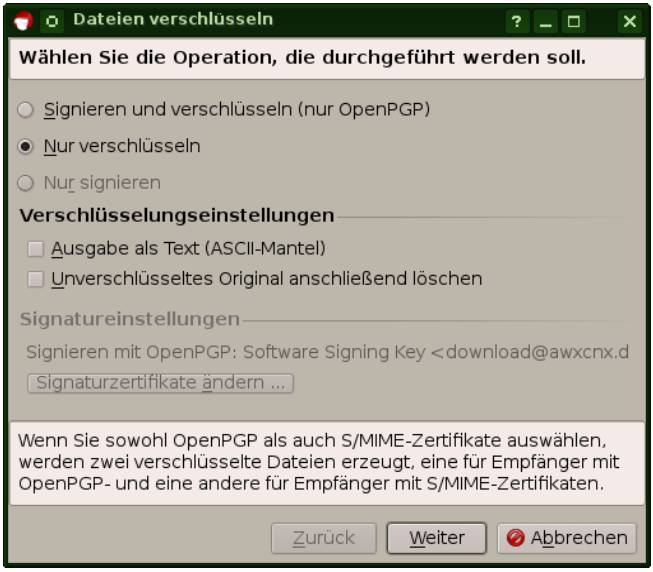


Abbildung 12.3: Assistent von Kleopatra

Bei der Schlüsselauswahl werden sowohl OpenPGP-Keys als auch S/MIME-Zertifikate angezeigt. Es ist darauf zu achten, dass man den richtigen Key auswählt. Sollen mehrere Personen die Datei entschlüsseln können, ist bei der Auswahl mit der Maus wie üblich die <STRG>-Taste gedrückt zu halten.

Werden sowohl OpenPGP-KEys und S/MIME-Zertifikate für die Verschlüsselung ausgewählt, erhält man als Ergbnis zwei verschlüsselte Dateien, eine mit OpenPGP verschlüsselt und eine mit den Zertifikaten verschlüsselte Datei. Man sollte darauf auchten, beide Dateien nicht zu verwechseln.

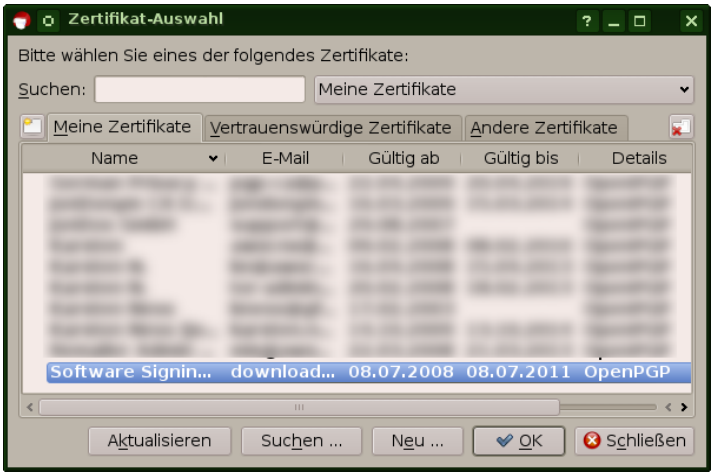


Abbildung 12.4: Schlüsselauswahl von Kleopatra

12.2 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 göffneten 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 Existens des versteckten Volumes nachzuweisen. Also Vorsicht bei Nutzung dieses Features.

12.2.1 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.

12.2.2 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 belästigt.

12.2.3 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 komlett verschlüsseln.

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

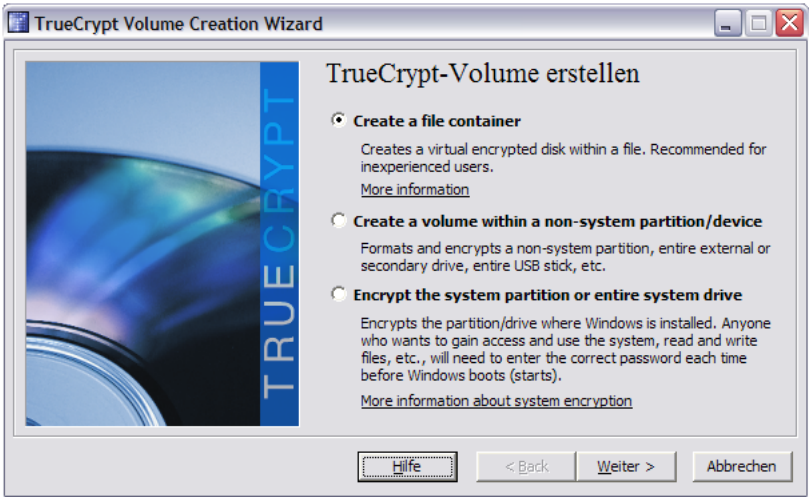


Abbildung 12.5: Assistent zur Erstellung eines Containers

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 Keyfiles (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.

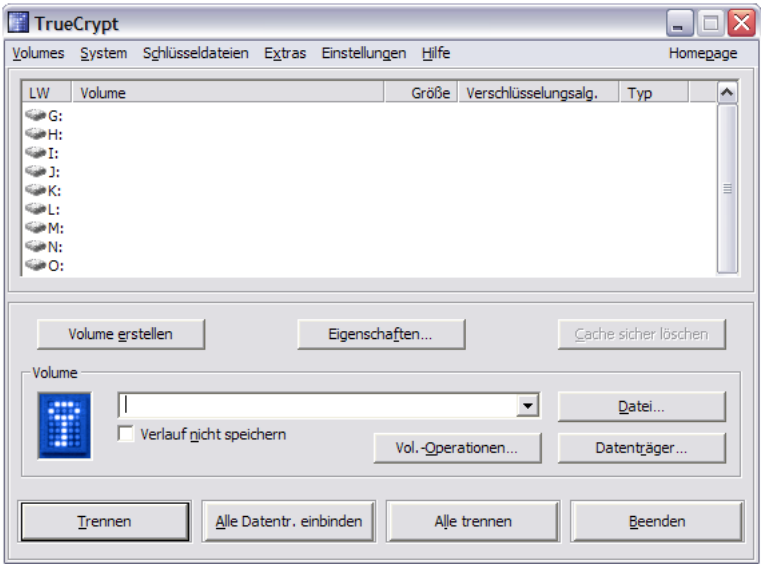


Abbildung 12.6: Hauptfenster von Truecrypt

12.2.4 Verschlüsselten Container öffnen

Truecrypt-Container werden beim Öffnen grundsätzlich als neue Laufwerke eingehängt. Das in Bild 12.6 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.

Anschließend ist der Button *Einbinden* zu wählen. Das in Bild 12.7 dargestellte Fenster zur Eingabe der Schlüssel erscheint. Hier ist der Schlüssel für das Öffnen des Containers einzugeben (die Passphrase oder/und das Keyfile).

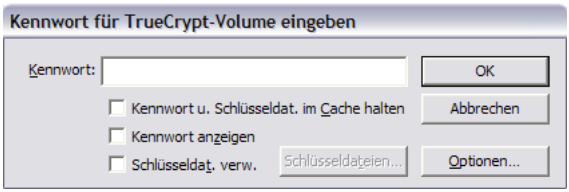


Abbildung 12.7: Eingabe des Schlüssels

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 Schlüsseleingabe. Der Vorgang kann einige Zeit dauern.

12.2.5 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.

12.2.6 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: Vorrausetzung 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.

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 12.9).

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

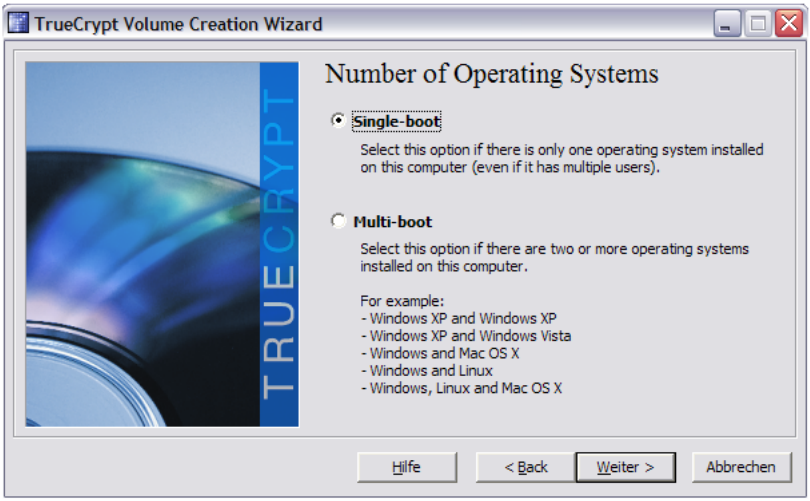


Abbildung 12.8: Assistent für die System-Verschlüsselung

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.

Abbildung 12.9: Erstellung der Rescue-Disk

12.2.7 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.

12.3 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 Packet *cryptsetup*, SuSE-Linux im Packet *util-linux-crypto*.

  Einige Distributionen installieren das Tool unter dem Namen *cryptsetup-luks*. Die im Folgenden beschrieben 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 Packet **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 des 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 Abhängigheit 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 ladenen Module eingefügt werden. In der Datei */etc/modules* ist die Zeile *dm_crypt* anzuhängen.

12.3.1 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 Paswort für den Container geändert werden. Sie werden nicht automatisch synchronisiert.

12.3.2 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
   ```

12.3.3 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 is7. 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
```

12.3.4 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 12.10 warten - fertig.

Abbildung 12.10: 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 Scripte, 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 Komando:

```
> 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 Komadozeile 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.

12.3.5 Debian GNU/Linux komplett verschlüsseln

In einem komplett verschlüsselten Sytem 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 verschlüssltes 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 Verzeichnis */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.

12.3.6 HOME-Verzeichnis verschlüsseln

Die Verschlüsselung der persönlichen Daten im $HOME-Verzeichnis bieten alle Linux-Distributionen bei der Installation an. Wer keine Komplettverschlüsselung nutzen möchte, sollte zumindest diese Option aktivieren. Der Container mit den verschlüsselten Daten wird beim Login automatisch geöffnet. Die Nutzung ist vollständig transparent. Bei Verlust des Laptops sind die Daten jedoch geschützt.

12.3.7 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, das 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 funtionieren 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*-Partionion 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
```

12.4 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 genutzen Distribution und evtl. einer zweiten CD für Download-Stuff schnell beisammen. Für WINDOWS wächst in kurzer Zeit eine umfangreiche Sammlung von Software und Aktivierungs-Keys.

Für das Backup der persönlichen Daten haben wir 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.

12.4.1 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 http://truerandom.com/homepage/projects/usbsticks/small.html

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. Viele USB-Sticks mit Verschlüsselung verwenden zwar starke Algorithmen (in der Regel AES256), legen aber einen zweiten Schlüssel zur Sicherheit auf dem Stick ab, der mit geeigneten Tools ausgelesen werden kann und Zugriff auf die Daten ermöglicht. Selbst eine Zertifizierung des NIST ist keine Garantie für eine saubere Implementierung, wie ein Artikel bei Heise.de zeigt. http/www.heise.de/newsticker/meldung/NIST-zertifizierte-USB-Sticks-mit-Hardware-Verschluesselung-geknackt-894962.html.

Unison-GTK

Für die Synchronisation der Daten steht z.B. Unison-GTK auf der Website http://www.cis.upenn.edu/ bcpierce/unison/ für verschiedene Betriebssysteme (auch WINDOWS) zur Verfügung und bietet ein GUI für die Synchronisation. Die Installation ist einfach: Download, Entpacken und Binary starten. Für Debian/Ubuntu funktioniert auch "*apt-get install unison-gtk*".

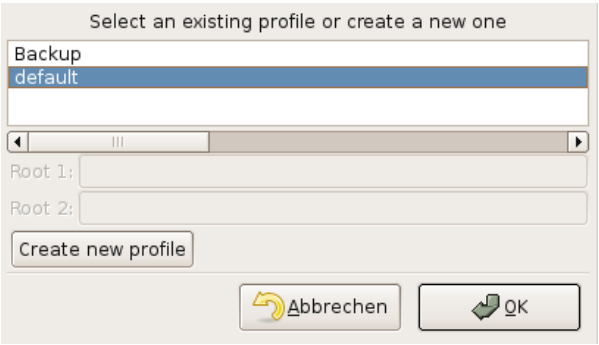


Abbildung 12.11: Profil nach dem Start von Unison-GTK auswählen

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 12.11).

Nach Auswahl des Profiles analysiert Unison die Differenzen und zeigt im Haupfenster an, welche Aktionen das Programm ausführen würde. Ein Klick auf *Go* startet die Synchronisation.

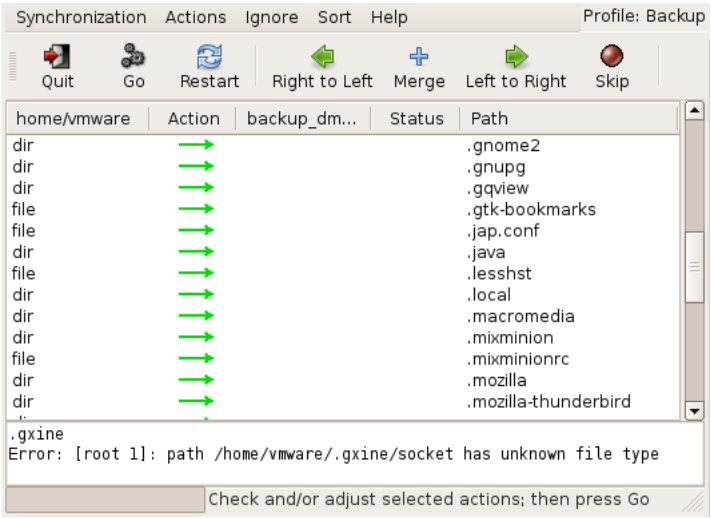


Abbildung 12.12: Hauptfenster von Unison

Achtung: Unison synchronisiert in beide Richtungen und eignet sich damit auch zum Synchronisieren zweier Rechner. Verwendet man einen neuen (leeren) Stick, muss auch ein neues Profil angelegt werden! Es werden sonst alle Daten in den Quellverzeichnissen gelöscht, die im Backup nicht mehr vorhanden sind.

Neben der Möglichkeit, lokale Verzeichnisse zu synchronisieren, kann Unison auch ein Backup auf einem anderen Rechner via FTP oder SSH synchronisieren.

rsync

Das Tool *rsync* ist in allen Linux-Distributionen enthalten und insbesondere für 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 Orginal 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 -includeängegeben 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 sowei die rsync-Parameter zugeordnet. Ein Klick auf die kleine Rakete oben rechts startet die Synchronisation (Bild 12.13).

12.4.2 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.

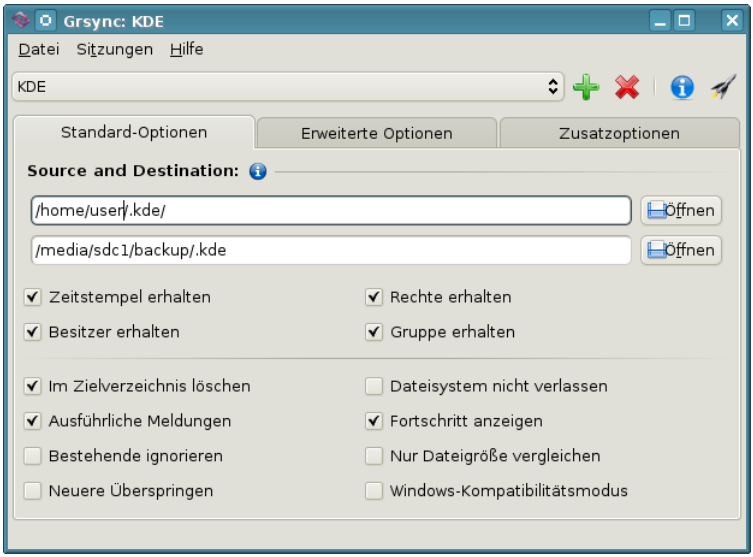


Abbildung 12.13: Hauptfenster von Grsync

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, ergänzt die folgenden Optionen:

```
> tar -cj datadir | aespipe -C 10 -e aes256 > data.tar.bz2.enc
```

Die Option *-C 10* bewirkt, das 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 Password wird dabei mit dem Programm *gpg* verschlüsselt:

```
> tar -cj data_dir | aespipe -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 folgender Kommandozeile:

```
> aespipe -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 | aespipe -T > %f.enc"
Name=Datei verschlüsseln (aespipe)
Icon=encrypted
```

Zukünftig findet man im Kontextmenü einer Datei unter *Aktionen* den Menüpunkt *Datei verschlüsseln (aespipe)* (Bild 12.14). 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.

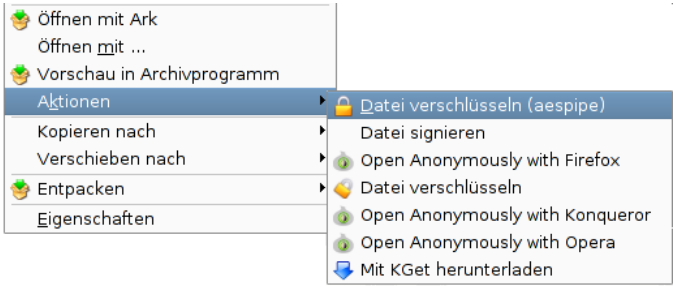


Abbildung 12.14: Neue Aktion im Servicemenü von Konqueror

Verzeichnisse sind zuerst zu komprimieren. Einträge sind bereits vorhanden.

12.4.3 Verschlüsselte Backups mit dar

Der Disk Archiver *dar* steht auf der Website http://dar.linux.free.fr zum Download bereit und ist auch in fast allen Linux Distributionen enthalten. Mit KDar steht unter http://kdar.sourceforge.net/ ein grafisches GUI für KDE zur Verfügung.

Wir wollen hier nicht das 30-seitige Manual-Page von *dar* wiedergeben, das Programm bietet viele Möglichkeiten. Wir beschränken uns 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
```

Nach dem Durchlauf des Programms findet man im Verzeichnis $HOME/backup die Dateien *projekt.1.dar*, *projekt.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.

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 Blowfisch 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.

12.4.4 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". (http://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t) 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 muss verschlüsselt werden, um die Vertraulichkeit zu gewährleisten.
- Es sollen 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.

Dublicity und Déjà Du 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. Mit *Déjà Du* steht auch ein grafisches Interface zur Verfügung.

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 deja-du
```

Duplicity ist ein Kommandozeilen Tool. Ein verschlüsseltes Backup schiebt man mit folgendem Kommando auf den Server:

```
> duplicity Verz BackupAddresse
```

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 automatiiseren, kann man ein kleines Shellscript schreiben:

```
#!/bin/sh
PASSPHRASE="gutes_passwort"
duplicity Verz BackupAddresse
```

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" Verz BackupAddresse
```

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 bei rsync ist 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 BackupAddresse /home/user/restore
```

Weitere Informationen findet man in der manual page von dublicity.

13 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, Datein vom Datenträger zu entfernen. Über die Arbeit der einzelnen Varianten sollte Klarheit bestehen, anderenfalls erlebt man evtl. eine böse Überraschung.

1. Dateien in den Papierkorb werfen

Unter WIN wird diese Variante als *Datei(en) löschen* bezeichnet, was etaws 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.

2. Papierkorb leeren

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 Tools wie Sleuthkit unterstützen Ermittler dabei. Sie bieten Werkzeuge, die den gesamten, als frei gekennzeichneten Bereich, eines Datenträgers nach Mustern durchsuchen können.

3. Dateien sicher löschen

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 GnuPG-Pack (WINDOWS) bietet nach Installation der Erweiterung GPGSX die Möglichkeit, Dateien und Verzeichnise 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 integriert 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 alle Dateien in allen Unterverzeichnissen 34x und löscht anschließend das gesamte Verzeichnis.

  ```
  > wipe -rcf verzeichnis
  ```

Auch bei diesen Varianten bleiben möglicherweise Spuren im Dateisystem zurück. Aktuelle Betriebssysteme verwenden ein Journaling Filesystem. Metadaten und evtl. auch Dateiinhalte 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 Dateiinhalte werden aber sicher gelöscht.

4. Gesamten Datenträger säubern

Bevor ein Laptop oder Computer entsorgt oder weitergeben wird, sollte man die Festplatte gründlich putzen. Am einfachsten erledigt man diesen Job mit einer Linux Live-CD. Nach dem Booten des Live Systems öffnet man ein Terminal 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 mehrfach mit NULL und Zufallszahlen zu überschreiben, kann man folgende Kommandos nutzen:

```
> dd if=/dev/zero of=/dev/hda
> dd if=/dev/urandom of=/dev/hda
```

5. Zerstören des Datenträgers

In einem Degausser kann man Informationen auf einem magnetischen Datenträger bei hohen Temperaturen und unter Einwirkung eines starken Magnetfeldes vollständig zerstören. Für Privatpersonen ist diese Variante in der Regl zu teuer.

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 Online, 2008, wieder einmal viel heiße Luft.)

Wie funktioniert diese Technik, über die Zeit Online bereits 1996 berichtete und können Nicht-Terroristen das auch nutzen?

Ein Beispiel

Statt Bits und Bytes werden in diesem Beispiel Buchstaben genutzt, um das Prinzip der Steganografie zu erläutern. Nehmen wir mal an, Terrorist A möchte an Terrorist B die folgende kurze Botschaft senden:

```
Morgen!
```

Statt die Nachricht zu verschlüsseln, was auffällig sein könnte, versteckt er sie in dem folgenden, harmlos aussehenden Satz:

```
Mein olles radio geht einfach nicht!
```

Wenn der Empfänger weiss, dass die eigentliche Botschaft in den Anfangsbuchstaben der Wörter kodiert ist, wäre es ganz gut, aber nicht optimal.

Ein Beobachter könnte auf den Gedanken kommen: *"Was - wieso Radio? Der zahlt doch keine GEZ!"* Er wird aufmerksam und mit ein wenig Probieren kann der die Botschaft extrahieren. Also wird Terrorist A die Nachricht zusätzlich

verschlüsseln, nehmen wir mal eine einfache Caesar-Verschlüselung mit dem Codewort KAWUM, es entsteht:

```
Ilpcmg!
```

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* (http://steghide.sourceforge.net/) und *outguess* (http://niels.xtdnet.nl/) 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 Selbsverteidigung (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.)

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 Downloadsite unter http://steghide.sourceforge.net/ 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.

Konqueror und Nautilus

Linuxer, welche die Dateimanager Konqueror (KDE) oder Nautilus (Gnome) nutzen, können das Verstecken und Extrahieren auch mit wenigen Mausklicks erledigen:

- Das Konqueror/Dolphin Servicemenü für steghide gibt es bei KDE-apps.org. Nach dem Download ist das Archiv zu entpacken. Die .desktop-Datei kopiert man nach *$HOME/.kde/share/apps/konqueror/servicemenus/* und das Shell-Script nach */usr/local/bin*. Download: http://kde-look.org/content/show.php?content=105172

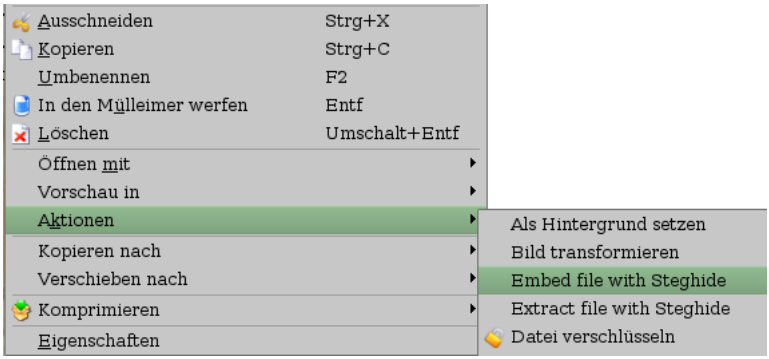


Abbildung 14.1: Steghide Menü im Konqueror

In Zukunft findet man bei einem Rechtsklick auf die Cover-Datei (JPEG, WAV, AU) im Untermenü *Aktionen* die Menüpunkte für das Einfügen und Extrahieren von Dateien mit *steghide*. (Bild 14.1). Für das Verstecken (embed) wählt man noch eine zweite Datei, die dann nach Abfrage des Passworts in der Cover-Datei versteckt wird.

- Das Nautilus Action Script ist ebenfalls zu entpacken und in $HOME/gnome2/nautilus-scripts zu speichern.

  Dann mit der rechten Maustaste auf eine JPEG-Datei klicken, den Menüpunkt “Scripte - steghide_jpg” wählen und den Anweisungen folgen.

14.2 stegdetect

Auch die Gegenseite ist nicht wehrlos. Manipulationen von steghide, F5, outguess, jphide usw. können z.B. mit *stegdetect* erkannt werden. (http://www.outguess.org/download.php) Ein GUI steht mit *xsteg* zur Verfügung, die Verschlüsselung der Nutzdaten kann mit *stegbreak* angegriffen werden. Beide Zusatzprogramme sind im Paket enthalten.

Der Name *stegdetect* ist eine Kurzform von *Steganografie Erkennung*. Das Programm ist nicht nur für den Nachweis der Nutzung von *steghide* geeignet, sondern erkennt anhand statistischer Analysen auch andere Tools.

Auch *stegdetect* ist ein Tool für die Kommandozeile. Neben der zu untersuchenden Datei kann mit einem Parameter -s die Sensitivität eingestellt werden. Standardmäßig arbeitet stegdetect mit einer Empfindlichkeit von 1.0 ziemlich oberflächlich. Sinnvolle Werte liegen bei 2.0...5.0.

```
> stegdetect -s 2.0 bild.jpg
F5(***)
```

Im Beispiel wird eine steganografische Manipulation erkannt und vermutet, dass diese mit dem dem Tool F5 eingebracht wurde (was nicht ganz richtig ist da *steghide* verwendet wurde).

Frage: Was kann man tun, wenn auf der Festplatte eines mutmaßlichen Terroristen 40.000 Bilder rumliegen? Muss man jedes Bild einzeln prüfen?

Antwort: Ja - und das geht so:

1. Der professionelle Forensiker erstellt zuerst eine 1:1-Kopie der zu untersuchenden Festplatte und speichert das Image z.B. in *terroristen_hda.img*
2. Mit einem kurzen Dreizeiler scannt er alle 40.000 Bilder in dem Image:

   ```
   > losetup -o $((63*512)) /dev/loop0 terroristen_hda.img
   > mount -o ro,noatime,noexec /dev/loop0 /mnt
   > find /mnt -iname "*.jpg" -print0 |
      xargs -0 stegdetect -s 2.0 >> ergebnis.txt
   ```

   (Für Computer-Laien und WINDOWS-Nutzer sieht das vielleicht nach Voodoo aus, für einen Forensiker sind das jedoch Standardtools, deren Nutzung er aus dem Ärmel schüttelt.)
3. Nach einiger Zeit wirft man eine Blick in die Datei *ergebnis.txt* und weiß, ob es etwas interessantes auf der Festplatte des Terroristen gibt.

Überwachung

Bitte angepasst und unauffällig verhalten!

„Die Durchsetzung der Disziplin erfordert die Einrichtung des zwingenden Blicks: eine Anlage, in der die Technicken des Sehens Machteffekte herbeiführen und in der umgekehrt die Zwangsmittel die Gezwungenen deutlich sichtbar machen“
(M. Foucault: Überwachen und Strafen, S. 221).

www.pm-buendnis.de

bpm
bündnis für politik- und meinungsfreiheit