Privacy-Handbuch

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

23. Dezember 2020

Inhaltsverzeichnis

Kapitel 1

Scroogled

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

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

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

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

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

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

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

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

“Möchten Sie mir was über Juni 1998 erzählen?”

Greg blickte vom Abflugplan hoch. “Pardon?”

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

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

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

“Womit?”

“Mit Raketenmodellen.”

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

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

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

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

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

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

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

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

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

“Und Sie sind verkleidet als . . . ?”

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

“N-nein. Doch, ja sicher, Yahoo war schon dabei. Aber das war nicht der Grund

für Google mitzumachen. Du weißt doch, die Republikaner hassen Google. Wir sind größtenteils als Demokraten registriert, also tun wir unser Bestes, mit ihnen Frieden zu schließen, bevor sie anfangen, sich auf uns 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.

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

Kapitel 2

Angriffe auf die Privatsphäre

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

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

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

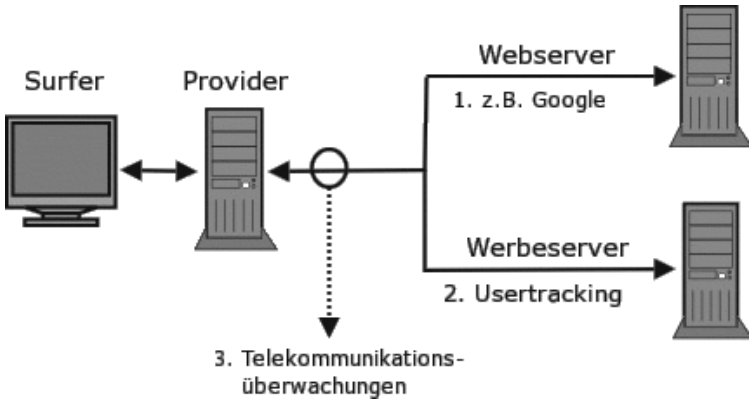


Abbildung 2.1: Möglichkeiten zur Überwachung im WWW

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

2.1 Big Data - Kunde ist der, der bezahlt

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

2.1.1 Google

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

Wirtschaftliche Zahlen

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

Google Web Search

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

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

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

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

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

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

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

   Die entwickelten Bewertungsverfahren werden zur Beobachtung der Trends im Web eingesetzt. Der Primus unter den Suchmaschinen ist damit in der Lage, erfolgversprechende Ideen und Angebote schneller als andere Mitbewerber zu erkennen und

darauf zu reagieren. Die Ideen werden nicht mehr selbst entwickelt, sondern aufgekauft und in das Imperium integriert. Seit 2004 wurden 60 Firmen übernommen, welche zuvor die Basis für die meisten aktuellen Angebote von Google entwickelt hatten: Youtube, Google Docs, Google Maps, Google Earth, Google Analytics, Picasa, SketchUp, die Blogger-Plattformen...

Das weitere Wachstum des Imperiums scheint langfristig gesichert.

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

Adsense, DoubleClick, Analytics & Co.

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

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

97% der TOP100 Websites und ca. 80% der deutschsprachigen Webangebote sind mit verschiedenen Elementen von Google für die Einblendung kontextsensitiver Werbung und Traffic-Analyse infiziert! (Reppesgaard: Das Google Imperium, 2008) Jeder Aufruf einer derart präparierten Website wird bei Google registriert, ausgewertet und einem Surfer zugeordnet. Neben kommerziellen Verkaufs-Websites, Informationsangeboten professioneller Journalisten und Online-Redaktionen gehören die Websites politischer Parteien genauso dazu, wie unabhängige Blogger auf den Plattformen *blogger.com* und *blogspot.com* sowie private Websites, die sich über ein paar Groschen aus dem Adsense-Werbe-Programm freuen.

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

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

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

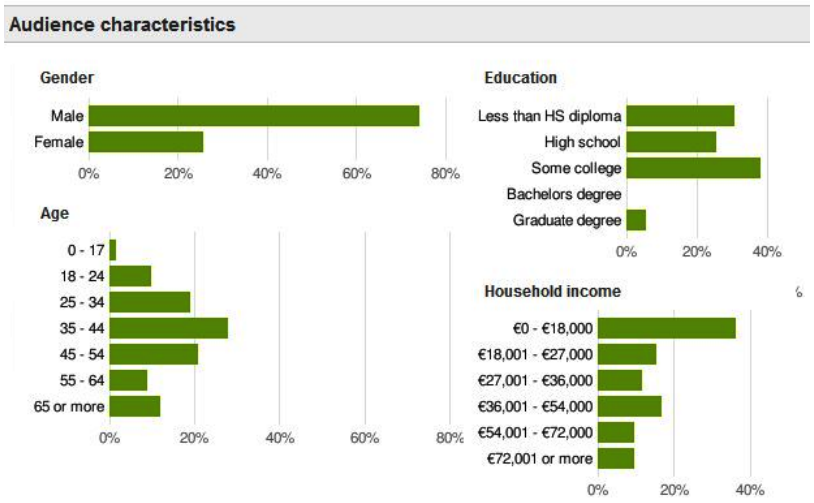


Abbildung 2.2: Ad-Planner Besucherstatistik (Beispiel)

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

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

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

Google Attribution

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

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

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

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

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

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

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

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

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

Smartphones und Android

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

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

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

Mozilla Firefox

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

- Die Default-Startseite ermöglicht es Google, ein langlebiges Cookie im First-Party Context zu setzen und den Browser damit praktisch zu personalisieren. Die standardmäßig aktive Richtlinie für Cookies ermöglicht es Google exklusive, auch als Drittseite das Surfverhalten zu verfolgen, da mit dem Start ein Cookie vorhanden ist.

- Sollte die Startseite modifiziert worden sein, erfolgt die "Personalisierung" des Browsers wenige Minuten später durch Aktualisierung der Phishing-Datenbank.

- Diese “Personalisierung” ermöglicht es Google, den Nutzer auf allen Webseiten zu erkennen, die mit Werbeanzeigen aus dem Imperium oder Google-Analytics verschmutzt sind. Im deutschsprachigen Web hat sich diese Verschmutzung auf 4/5 der relevanten Webseiten ausgebreitet.

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

Google DNS

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

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

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

Kooperation mit Geheimdiensten (NSA, CIA)

Es wäre verwunderlich, wenn die gesammelten Datenbestände nicht das Interesse der Geheimdienste wecken würden. Das EPIC bemühte sich jahrelang auf Basis des Freedom of Information Act, Licht in diese Kooperation zu bringen. Die Anfragen wurden nicht beantwortet.[1]

Erst durch die von Snowden/Greenwald veröffentlichten Dokumente wurde mehr bekannt. Google ist seit 2009 einer der ersten PRISM-Partner der NSA. Das bedeutet, dass der US-Geheimdienst vollen Zugriff auf die Daten der Nutzer hat. Von allen auf der Folie genannten PRISM-Firmen wurden über-spezifische Dementis veröffentlicht, dass sie nie von einem Programm mit dem Namen PRISM gehört hätten und demzufolge nicht wissentlich mit der NSA im Rahmen von PRISM kooperieren würden. Rajesh De, Leiter der Rechtsabteilung der NSA, dementierte die Dementis[2] und stellte klar, dass die Internetfirmen zwar den intern verwendetet Namen PRISM nicht kannten, dass die Datensammlung aber mit *voller Kenntnis und Unterstützung* der Unternehmen erfolgte.

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

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

Wenn Googles Verwaltungsratschef Eric Schmidt auf der SXSW-Konferenz 2014 behauptet, durch Einführung der SSL-Verschlüsselung zwischen Datencentern seien die Daten der Google-Nutzer jetzt vor der NSA sicher[3], dann kann man es als PR-Gag

[1] https://epic.org/2010/09/epic-files-suit-for-documents.html
[2] http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google-yahoo-co-nsa-anwalt-internetfirmen-wussten-von-ausspaehaktionen-12855553.html
[3] https://www.heise.de/-2138499

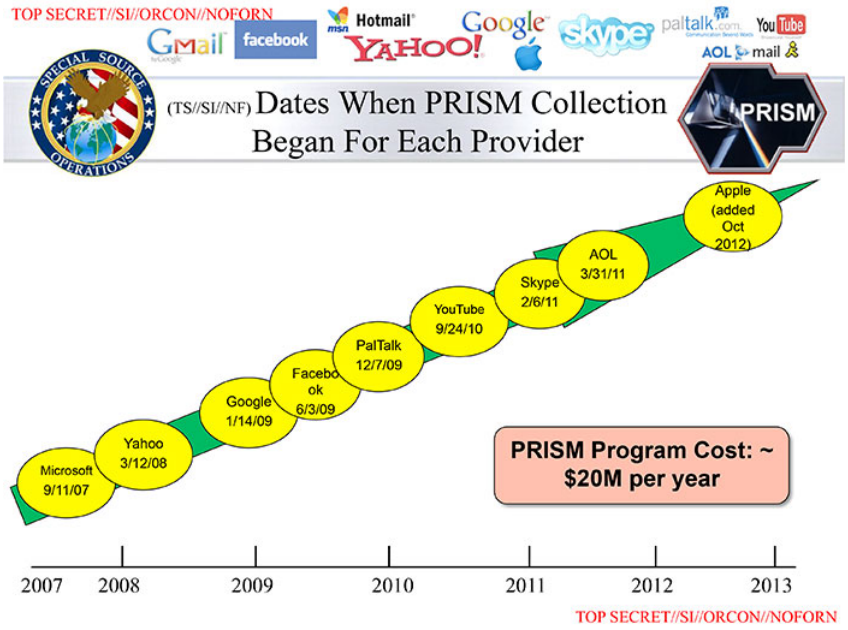


Abbildung 2.3: NSA-Folie zu den PRISM-Partnern

abtun. Google ist aufgrund geltender Gesetze zur Kooperation mit den weitreichenden Späh-Programmen der NSA verpflichtet.

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

Kooperation mit Behörden

Auf Anfrage stellt Google den Behörden der Länder die angeforderten Daten zur Verfügung. Dabei agiert Google auf Grundlage der nationalen Gesetze. Bei daten-speicherung.de findet man Zahlen zur Kooperationswilligkeit des Imperiums. Durchschnittlich beantwortet Google Anfragen mit folgender Häufigkeit:

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

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

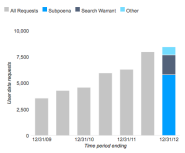


Abbildung 2.4: Steigerung der Auskünfte von Google an Behörden

Die (virtuelle) Welt ist eine "Google" - oder?

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

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

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

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

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

Google dominiert unser (virtuelles) Leben.

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

2.1.2 Weitere Datensammler

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

Acxiom konnte bereits 2001, noch bevor Facebook als Datenquelle zur Verfügung stand, auf umfangreiche Datenbestände verweisen. Als das FBI die Namen der angeblichen 9/11 Attentäter veröffentlichte (von denen noch heute einige quicklebendig sind), lieferte Acxiom mehr Daten zu diesen Personen, als alle Geheimdienste zusammen - inklusive früherer und aktueller Adressen, Namen der Mitbewohner usw. Das war der Beginn einer Zusammenarbeit. Im Rahmen der Zusammenarbeit mit FBI und CIA führten die Daten von Acxiom mehrfach zu Anklagen und Abschiebungen.

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

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

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

> *3 Milliarden Verbraucherprofile aus 700 Millionen täglichen Social-Media-Nachrichten, Daten über die Nutzung von 15 Millionen Webseiten und Einkäufe bei 1 500 Händlern.*

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

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

- realen Namen, genutzte E-Mail Adressen, Telefonnummern und Kreditkarten
- Historie von online und offline Einkäufen
- Historie des Surfverhaltens im Internet

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

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

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

Ein Beispiel: laut Tinder Datenschutz Policy[4] werden folgende Daten gesammelt:

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

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

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

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

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

Towerd@ta sammelt die Informationen anhand von E-Mail Adressen. Jeder kann auf der Website eine Liste von E-Mail Adressen hochladen, bezahlen und nach Zahlungseingang die Daten abrufen. Ein kleiner Auszug aus der Preisliste[5] soll den Wert persönlicher Informationen zeigen:

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

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

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

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

2.2 Techniken der Datensammler

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

[5] https://www.towerdata.com/email-intelligence/pricing

ansprechen. Das und vieles mehr ist heute schon möglich.

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

Techniken zum Tracking des Surfverhaltens

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

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

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

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

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

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

Werbebanner und Like-Buttons können einerseits in der gleichen Weise wie HTML-Wanzen für das Tracking verwendet werden. Außerdem verrät man mit Klicks auf Werbung oder Like Buttons mehr private Informationen, als man eigentlich veröffentlichen möchte. S. Guha von Microsoft und B. Cheng sowie P. Francis vom Max-Planck-Institut für Software Systeme haben ein Paper veröffentlicht, wie man homosexuelle Männer anhand der Klicks auf Werbung erkennen kann[9]. Das Verfahren kann für verschiedene Fragestellungen angepasst werden. Die Klicks auf Facebook Like Buttons können in der gleichen Weise ausgewertet werden. Forscher der Universität Cambridge (Großbritannien) konnten bei einer Untersuchung die sexuelle Orientierung und politische Einstellung der Nutzer anhand der Klicks auf Like Buttons vorhersagen[10].

[6] https://www.heise.de/-1628313
[7] https://www.heise.de/-1626368
[8] https://anonymous-proxy-servers.net/blog/index.php?/archives/377-Tracking-mit-Cookies.html
[9] http://arstechnica.com/tech-policy/news/2010/10/more-privacy-headaches-for-facebook-gay-users-outed-to-advertisers.ars
[10] https://www.heise.de/-1820638

Immer häufiger nutzen Kriminelle die großen Werbenetzwerke, um mit ihrer Schadsoftware möglichst viele Rechner anzugreifen. Kriminelle kaufen passende Werbeplätze und lassen bösartige Werbebanner ausliefern oder locken die Surfer mit Anzeigen auf Malware Webseiten. Diese Angriffe werden als Malvertising bezeichnet (abgeleitet von *malicious advertising*) und nehmen derzeit stark zu. Die Sicherheitexperten von Cyphort registrierten 2015 einen Anstieg von 325% und erwarten eine Fortsetzung dieses Trends für 2016.[11]

EverCookies nutzen moderne HTML5 Techniken wie DomStorage, ETags aus dem Cache u.a. als Ersatz für Cookies, um den Surfer zu markieren und später anhand dieser Markierungen wiederzuerkennen. Der polnische Informatiker Samy Kamkar hat eine Webseite zur Demonstration von EverCookie Techniken[12] erarbeitet. 38% der populären Webseiten nutzen bereits verschiedene EverCookie Techniken (Stand: Okt. 2012).

Browser Fingerprinting nutzt verschiedene Merkmale des Browsers wie z. B. Browserversion, installierte Schriftarten, Bildschirmgröße, bevorzugte Sprachen und weitere Daten, um einen Fingerprint zu berechnen. Dieser Fingerprint ist für viele Surfer eindeutig. Das Projekt Panopticlick [13] der EFF.org zeigte, dass mehr als 80% der Surfer damit eindeutig erkennbar sind. Die Erkennungsrate stieg auf 94%, wenn Flash- oder Java-Applets zusätzlich genutzt werden konnten.

Für das Fingerprinting des Browsers werden verschiedene Techniken eingesetzt:

1. HTTP-Header: Es werden die Informationen ausgewertet, die der Browser bei jedem Aufruf sendet (Sprache, Browsername und -version, Betriebssystem und -version, unterstützte Zeichensätze, Dateitypen, Kodierungen).
2. JavaScript basiert: Informationen werden per JavaScript ausgelesen (installierte Schriften, Bildschirmgröße, Größe des Browserfensters).
3. Canvas basiert: In einem HTML5 Canvas Element wird ein Text gerendert und das Ergebnis via JavaScript als Bild ausgelesen und ein Hash über alle Pixel als individuelles Merkmal berechnet. Das Ergebnis unterscheidet sich von Browser zu Browser aufgrund installierter Schriften, Software für das Rendering usw. Das Tracking-Verfahren wurde 2012 in dem wiss. Paper *Perfect Pixel: Fingerprinting Fingerprinting Canvas in HTML5*[14] beschrieben.
   Mittels Canvas Font Fingerprinting können die installierten Schriftarten ermittelt werden. Das Verfahren wurde 2016 in dem *OpenWPM Paper* beschrieben.
4. Plug-in basiert: Informationen werden per Flash- oder Java-Plugin ausgelesen (Schriftarten, Betriebssystem, Kernel, Multi-Monitor Setups, Bildschirmgröße).
5. Add-on basiert: Durch Seiteneffekte werden evtl. vorhandene Browser Add-ons analysiert (NoScript Whitelist, AdBlock Blacklist, User-Agent Spoofing).
6. Hardware basiert: Informationen über die Hardware des genutzten Rechners werden gesammelt (Vibrator-API, Zugriff auf Mikrofon und Webcam, Performance der Grafikhardware und Besonderheiten im Soundsystem).

Die Studien *Dusting the Web for Fingerprinters*[15] (2013) und *The web never forgets*[16] (2014) der KU Leuven (Belgien) und OpenWPN (2016) der Princeton University haben nachgewiesen, das Fingerprinting für das Tracking genutzt wird. Mit dem *FP-Insector* haben US-amerikanische Forscher 2020 nachgewiesen, dass das Browserfingerprinting als Trackingtechnik bei fast einem Viertel der Top 10.000 Webseiten eingesetzt wird, insbesondere bei News und Shopping Webseiten.[17]

[11] http://www.cyphort.com/about/news-and-events/press-releases/cyphort-labs-issues-special-report-on-the-rise-in-malvertising-cyber-attacks
[12] https://samy.pl/evercookie
[13] https://panopticlick.eff.org/browser-uniqueness.pdf (PDF)
[14] http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf
[15] http://www.cosic.esat.kuleuven.be/publications/article-2334.pdf
[16] https://securehomes.esat.kuleuven.be/ gacar/persistent/the_web_never_forgets.pdf
[17] https://www.golem.de/news/browser-fingerprinting-neue-methoden-gegen-cookie-loses-tracking-2008-150518.html

- *Bluecava* nutzt ausschließlich Browser Fingerprinting und protzt mit 30% besseren Ergebnissen als Cookie-basierte Techniken.[18]
- *Zanox.com* nutzt den Fingerprint des Browsers, wenn Cookies gelöscht oder per Browser-Einstellung blockiert werden.[19]
- *WebTrekk* berechnet einen Fingerprint auf Grundlage von Geolocation anhand der IP-Adresse, Bildschirmgröße und Farbtiefe des Monitors, innere Größe des Browserfensters, bevorzugte Sprache, User-Agent des Browsers, Version des Betriebssystems sowie Einstellungen für Java, JavaScript und Cookies.[20]
- *Multicounter* nutzt den Fingerprint zusätzlich zu Cookies oder EverCookies zur Verbesserung der Erkennungsraten.[21]
- *Anonymizer Inc.* verwendet Browser Fingerprinting auf sämtlichen Webseiten, verschweigt es aber im Privacy Statement. (Eine seltsame Auffassung für jemanden, der Anonymität verkaufen will.)
- *Yahoo! Web Analytics* nutzt Fingerprinting, wenn Cookies blockiert werden.
- Canvas Fingerprinting wird u.a. von den Trackindiensten *doubleverify.com*, *lijit.com* und *alicdn.com* genutzt. Auf 14.371 Webseiten wurden Trackingscripte mit Canvas Fingerprinting nachgewiesen. (Stand: 2016)
- AudioContext Fingerprinting wurde bei drei Trackingdiensten nachgewiesen, die jedoch nur einen sehr geringe Reichweite haben und nur auf wenigen Webseiten eingebunden sind.

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

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

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

Wischen, Tippen, Zoomen sind die üblichen Gesten für die Bedienung der Touchscreens auf Smartphones. Ein australisches Forschungsteam präsentiert auf der PETS 2018 das Paper *Quantifying the Uniqueness of Touch Gestures for Tracking*[22], in dem gezeigt wird, dass diese Touchgesten individuell unterschiedlich sind und für die Wiedererkennung von Smartphone Nutzern geeignet sind.

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

[18] http://www.bluecava.com/visitor-insight-campaign-measurement
[19] http://blog.zanox.com/de/zanox/2013/09/11/zanox-stellt-tpv-fingerprint-tracking-vor/
[20] http://www.webtrekk.com/de/index/datenschutzerklaerung.html
[21] http://www.multicounter.de/features.html
[22] https://petsymposium.org/2018/files/papers/issue2/popets-2018-0016.pdf

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

Tracking von E-Mail Newslettern

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

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

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

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

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

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

- Neben kleinen Bildern können weitere HTML-Elemente wie CSS Stylesheets, Media Dateien oder Link Prefetching in einer E-Mail genutzt werden. Der E-Mail Privacy Test[23] zeigt eine umfangreiche Liste. Diese Elemente werden in der Praxis aber kaum genutzt.

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

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

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

Tracking von Dokumenten (PDF, Word usw.)

Die Firma ReadNotify bietet beispielweise einen Service, der Word-Dokumente und PDF-Dateien mit speziellen unsichtbaren Elementen versieht. Diese werden beim Öffnen des Dokumentes vom Server der Firma nachgeladen und erlauben somit eine Kontrolle, wer wann welches Dokument öffnet. Via Geo-Location ermittelt ReadNotify auch den ungefähren Standort des Lesers. Aus der Werbung von ReadNotify: [24]

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

[23] https://emailprivacytester.com/
[24] https://ssl1.readnotify.com/readnotify/pmdoctrack.asp

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

2.3 Tendenzen auf dem Gebiet des Tracking

Obwohl 80% der Internetnutzer das Tracking des Surfverhaltens ablehnen, wird es stetig weiter ausgebaut. Dabei wird es sowohl technisch durch die großen Datensammler immer weiter ausgebaut und durch politische Entscheidungen werden Datensammlungen erleichtert.

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

	Anzahl der Cookies
2009	3.602
2011	5.675
2012	6.485
2015	12.857

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

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

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

   (a) Die Google-Familie ist unangefochten die Nummer Eins. 44% der weltweiten Umsätze in der Onlinewerbung werden durch diese Gruppe erzielt. Das Google Imperium hat in den letzten Jahren die Firmen *YouTube, DoubleClick mit falkad.net, FeedBurner, Springs, Adscape, AdMob, Teracent, Invite Media, Admeld, Adelphic, Wildfire Interactive* u.a.m. aufgekauft. Nach dem OpenWPM Report von 2016 gehören die TOP5 Tracking Dienste alle zur Google Familie und von den TOP20 Tracking Diensten gehören 12 zum Google Imperium. Die folgende Tabelle zeigt, wie das Google Imperium dadurch seine Präsenz auf den 1000 populärsten Webseiten in den letzten Jahren ausbauen konnte:

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

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

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

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

   - Im Februar 2013 hat Facebook eine Kooperation mit den Datenhändlern *Axciom* und *Datalogix* bekannt gegeben. Diese Firmen werten umfangreiche Daten aus der realen Welt aus (Kreditkartenzahlungen, Rabattkarten usw.). Damit sollen die Werbeeinblendungen bei Facebook individueller und zielgerichteter auf die Interessen der Mitglieder zugeschnitten werden.
   - PayPal.com will sein Bezahlsystem auch offline in der realen Welt anbieten und verspricht den teilnehmenden Geschäften, dass sie mehr über die Vorlieben ihrer Kunden erfahren werden. Natürlich wird auch PayPal.com mehr über die realen Interessen der Kunden erfahren.
   - Google hat 2014 die *Ladenbesuchmessung* eingeführt und beobachtet anhand der Geolocation der Android Smartphones, welche GEschäfter der Besitzer des Smartphones in der realen Welt besucht.
   - Patentanmeldungen von Google und Firmen Akquisitionen zeigen, dass das Imperium zukünftig auch Daten in der realen welt sammeln möchte. Anfang 2014 kaufte Google z. B. mit Nest einen Hersteller von Thermostaten und Rauchmeldern für 3,1 Milliarden Dollar. Die Thermostate von Nest sind in Millionen Haushalten eingebaut und mit Temperatur-, Helligkeits- sowie Luftfeuchtigkeitssensoren ausgerüstet, die via Internet ausgelesen werden können.

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

   - Außerdem interessiert sich Google für die Offline Einkäufe mit Kreditkarten. Über Partnerschaften kennt Google 70% der Zahlungen mit Kreditkarten in den USA (Stand: Mai 2017). Ähnliche Partnerschaften in Europa sind in Vorbereitung.[25]

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

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

ist.

Die EFF.org kommentierte:

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

Durch die Snowden-Dokumente wurden konkrete Beispiele bekannt.[26]

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

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

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

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

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

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

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

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

[26] https://www.eff.org/deeplinks/2013/12/nsa-turns-cookies-and-more-surveillance-beacons
[27] https://netzpolitik.org/2015/merkel-stellt-sich-gegen-datenschutz-und-netzneutralitaet/

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

7. Der *Point of no Return* ist längst überschritten. Am 06. Okt. 2015 hat der Europäische Gerichtshof (EuGH) das Safe Habour Abkommen für ungültig erklärt[28], dass bisher den Datentransfer in die USA erlaubte. Die Verquickung von Facebook mit den US-Geheimdiensten im Rahmen von PRISM spielte eine wesentliche Rolle bei der Urteilsfindung.

   Google und Facebook haben daraufhin erklärt, dass sie auch ohne Safe Habour Abkommen so weitermachen wie bisher und die Daten europäischer Nutzer in die USA transferieren und dort verarbeiten werden[29]. Sie sehen die EU-Standardvertragsklauseln nach Artikel 26, Absatz 2 der EU-Datenschutzrichtlinie von 1995 (EC95/46) als ausreichende Grundlage an. In dieser Ansicht werden sie von der EU-Kommision unterstützt.[30]

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

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

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

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

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

2.4 Crypto War 3.0

Im Januar 2015 hat der britische Premierminster Cameron den **crypto war 3.0** mit der Forderung eröffnet, dass **jede Kommunikation für Geheimdienste einsehbar sein muss**. Weitere Politiker wie Obama, der damalige Bundesinnenminister de Maizière oder der australische Justizminister Keenan assistierten. Als hinreichender Grund wird der allgegenwärtige TERRORISMUS kolportiert, der unsere demokratischen Werte bedroht.

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

[28] https://www.heise.de/tp/artikel/46/46186/1.html
[29] https://www.golem.de/news/safe-harbor-urteil-google-und-microsoft-suchen-neue-wege-des-datentransfers-1510-116945.html
[30] http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm

Damit sind nicht Googles Werbeeinnahmen gemeint sondern industrielle Anwendungen, mit den denen richtig viel Geld umgesetzt wird (z. B. im Bereich Banken, Börsen usw.).

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

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

- Skype wurde 2005 durch Anwendung des CALEA Act. gezwungen, Schnittstellen für die Überwachung bereitzustellen. Diese Überwachung wurde ständig weiter ausgebaut und heute liest auch Microsoft als Betreiber des Dienstes mit.
- Blackberry wurde in Kanada, in Indien und in anderen Ländern gezwungen, den Behörden die Schlüssel für die Entschlüsselung zur Verfügung zu stellen.

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

- Ein Anti-Terror Gesetz sollte alle Anbieter von Messaging Diensten in Russland zwingen, dem Geheimdienst FSB die Möglichkeit zur Entschlüsselung der Kommunikation zu geben. Außerdem sollen die Inhalte der Kommunikation für 6 Monate und die Metadaten für 3 Jahre gespeichert werden. Der Versuch der Durchsetzung dieses Gesetztes gegenüber dem Messenger Telegram endete in einem Fiasco[31]. Gegenwärtig wird die Durchsetzung des Gesetzes nicht verfolgt.
- In Australien wurde im Dezember 2018 das Assistence and Access Bill verabschiedet, welches ebenfalls die Anbieter von Messaging Diensten zur Hinterlegung eines Generalsschlüssels bei den Strafverfolgungsbehörden verpflichtet, um verschlüsselte Kommunikation entschlüsseln zu können. Anbieter von Messaging Diensten wie die Signal haben es abgelehnt, dem Gesetz Folge zu leisten. Die Durchsetzung des Gesetzes wird ebenfalls nicht verfolgt.
- In Deutschland hat Bundesinnenminster Seehofer im Mai 2019 ähnliche Vorstellungen geäußert. Nach seinen Vorstellungen sollten alle Messaging Dienste gezwungen werden, die gewünschten Kommunikationsdaten selbst zu entschlüsseln und in entschlüsselter Form den Strafverfolgungsbehörden zur Verfügung zu stellen. Die vehemente Kritik des Bundesverbandes für IT-Sicherheit, eco-Verband der Internetwirtschaft, CCC, Digitale Gesellschaft... u.a.m. verhinderte die Umsetzung dieser Pläne.
- Ende Nov. 2020 wurde der deutsche Vorschlag für eine Entschließung des EU-Rates verabschiedet, die die Betreiber von Messaging Diensten zur Kooperation mit Behörden und Geheimdiensten verpflichten soll. Es werden darin keine konkreten Verfahren zur Zusammenarbeit vorgegeben. Den Beteibern wird die magische Hausaufgabe der Quadratur des Kreise gestellt, eine sichere Verschlüsselung zu entwickeln und gleichzeitig die entschlüsselten Inhalte den Behörden auf Wunsch zur Verfügung zu stellen. Konkrete Gesetze sollen folgen.

  Die Datenschutzkonderenz von Bund und Ländern hat die Pläne zurück gewiesen. Die *Aushölung der Verschlüsselung*, wie vom EU-Rat gefordert, ist kontraproduktiv und könne von Kriminellen und Terroristen umgangen werden.

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

Seit Mitte 2018 ist daher ein Umdenken bei den Befürwortern der Überwachung erkennbar. Es wird keine Entschlüsselung der Kommunikation gefordert, aber die Betreiber von Messaging Diensten sollen Behörden dabei unterstützen, sich als ßtille

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

Teilnehmerïn eine verschlüsselte Kommunikation einzuklinken und so Chats bzw. Gruppenchats live und unbemerkt belauschen zu können:

> *It's relatively easy for a service provider to silently add a law enforcement participant to a group chat or call...*
> *We're not talking about weakening encryption or defeating the end-to-end nature of the service. In a solution like this, we're normally talking about suppressing a notification on a target's device, and only on the device of the target and possibly those they communicate with. That's a very different proposition to discuss and you don't even have to touch the encryption.*

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

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

Frontdoor Diskussion: Auf dem Grünen Polizeikongress im Nov. 2019 haben Conztanze Kurz (Sprecherin des CCC) und Konstantin v. Notz (Grüne) den Vorschlag unterstützt, dass Anbieter von Messaging Diensten eine modifizierte Version der App bereitstellen könnten, in der die Ende-zu-Ende Verschlüsselung zugunsten der Strafverfolgung kompromittiert wurde. Diese Version könnte in Kooperation mit Google bzw. Apple auf den Smartphones der Zielpersonen verteilt werden. Diese *Frontdoor* genannte Option hätte einige Vorteile gegenüber einer *Backdoor*, die die Krypto aller Messaging Apps kompromittiert, oder gegenüber Bundestrojanern, die den Schwarzmarkt für Exploits anheizen werden.[32]

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

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

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

Im Vorfeld hatte Kommissarin Ylva Johansson (Inneres) angekündigt, dass Anbieter von Krypto-Messengern zukünftig ihre Plattformen routinemäßig nach pädokriminellen Inhalten durchsuchen müssten. Als Begründung nannte sie den explosionsartigen Anstieg der gemeldeten pädokriminellen Videos von 300.00 zwischen 2015 und 2017 auf über 3,5 Millionen aktuell in den USA. (Für Europa nannte sie keine Zahlen.)

In ihrer Argumentation verschweigt Kommissarin Johansson die Gründe für den Anstieg. Einerseits gibt es in dieser ekligen Branche den gleichen starken Trend weg von Fotos hin zu Videos wie im gesamten Internet. Außerdem wurden seit 2018 mit Microsofts PhotoDNA und vergleichbaren Produkten von Google, Facebook u.a. technische Lösungen ausgerollt, die die automatisierte Erkennung dieser illegalen Inhalte stark verbesserten und somit die Erkennungsraten drastisch steigern konnten. Bei

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

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

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

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

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

- In Deutschland nimmt die im Nov. 2015 angekündigte Bundes-Hacker-Behörde zur Unterstützung von Geheimdiensten und Strafverfolgung beim Brechen von Verschlüsselung langsam Gestalt an. Die *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* (Zitis) soll seit 2017 mit 60 Mitarbeitern einsatzbereit sein und dann schrittweise auf 400 Mitarbeiter ausgebaut werden.[33]

  Der bis 2015 vom BKA eingesetzte *Bundestrojaner* der Firma DigiTask wurde vom CCC nach nur 11 Einsätzen enttarnt. In den Folgejahren gab es technische Probleme mit der selbst entwickelten RCIS 1.0 (*Remote Control Interception Software*), die in der Praxis unbrauchbar war. Seit Mitte 2018 ist eine Software von FinFischer für die Online-Durchsuchung und Quellen-TKÜ verfügbar, die eine brauchbare Einsatzreife erlangt haben soll. Neben dem BKA möchte auch der Verfassungsschutz dieses Spielzeug einsetzen, beispielsweise wenn mal wieder die Beobachtung einer tterroristischen Vereinigungnnach §129a konstruiert wurde. Das würde die Einsatzzahlen in Zukunft deutlich nach oben treiben.

- In den USA soll *Rule 41 of the US Federal Rules of Criminal Procedure* ab Dez. 2016 das staatliche Hacken von Tor- und VPN-Nutzern für das FBI massiv erleichtern, unabhägig davon, in welchem Land die Tor-Nutzer sich befinden.[34]

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

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

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

2.5 Fake News Debatte

Manche nennen es *Fake News*, andere sprechen von *alternativen Fakten*, umgangssprachlich nennt man es *Lügen* und in den wundersamen Geschichten des Baron von Münchhausen

[33] https://netzpolitik.org/2016/bundesregierung-will-entschluesselungsbehoerde-schaffen

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

erlangte das Phänomen literarischen Weltruhm.

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

2.5.1 Der Kampf gegen Fake News

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

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

2. Mit dem Netzwerkdurchsetzungsgesetz (NetzDG) werden stärkere Geschütze aufgefahren. Betreiber von Social Media Plattformen sollen Fake News entfernen, bevor sie viral werden und eine größere Reichweite erlangen. Dafür wird Facebook im deutschsprachigem Raum vom Recherekollektiv Correctiv unterstützt, die selbst schon Fake News verbreitet haben, um ihre politische Agenda zu verfolgen.

   Viele Rechtsexperten halten das NetzDG für verfassungswidrig, da es die Meinungs- und Pressefreiheit unzulässig stark einschränkt. Auch der UN-Sonderberichterstatter für Meinungsfreiheit rügt das NetzDG [35]. Das Gesetz gefährdet die Menschenrechte auf Meinungsfreiheit und Privatsphäre. Im Zweifel würden Internetfirmen auch legale Inhalte löschen, um die Gefahr von Bußgeldzahlungen zu minimieren. Eine passendere Bezeichnung für das Gesetz wäre *Meinungsbeschränkungsgesetz* (neusprech.org).

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

   - Ende April 2017 hat Google eine Änderung seines Suchalgorithmus bekannt gegeben, um den Zugang zu minderwertigen Informationen wie Verschwörungstheorien und Fake News zu erschweren. Es werden jetzt die Mainstream Meinungen bevorzugt und Webseiten mit abweichenden Meinungen abgewertet, wenn die Such-Historie eines Nutzers nicht darauf schließen lässt, dass er gezielt nach alternative Meinungen sucht.
     Einige Webseiten wie z. B. die World Socialist Web Site der 4. Internationale berichten von einem Rückgang der Besucher bis zu 70% durch diese Änderung. [36] [37]

   - Im Nov. 2017 hat Google CEO Erich Schmidt bekannt gegeben, dass die russische Nachrichtenseite RT.com und das Portal Sputnik News im Google News Service benachteiligt werden sollen, um die Reichweite zu reduzieren.[38]

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

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

[35] https://netzpolitik.org/2017/un-sonderberichterstatter-netzwerkdurchsetzungsgesetz-verstoesst-gegen-menschenrechte/
[36] https://www.wsws.org/de/articles/2017/07/28/goog-j28.html
[37] https://www.wsws.org/de/articles/2017/08/05/goog-a05.html
[38] https://www.rt.com/news/410444-google-alphabet-derank-rt/

2.5.2 Fake News Beispiele

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

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

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

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

  Das *Massaker von Racak* war die Begründung für die NATO, um an der Seite der UCK in den Bürgerkrieg einzugreifen und Belgrad zu bombardieren. Auch Deutschland hat sich an diesem völkerrechtswidrigen Angriff beteiligt.

- FAKE: *Irakische Soldaten haben beim Überfall auf Kuweit frühgeborene Säuglinge aus den Brutkästen gerissen und auf dem Boden des Krankenhauses liegen gelassen, wo die Säuglinge starben.* (Brutkastenlüge, vom damaligen US-Präsidenten George H. W. Bush und von Menschenrechtsorganisationen vielfach zitiert.)

  WAHR: Die *Brutkastenlüge* wurde völlig faktenfrei von der PR-Agentur Hill & Knowlton im Auftrag der kuwaitischen Exil-Regierung erfunden. Die *Krankenschwester*, die als Zeugin aussagte, war die Tochter des des kuwaitischen Botschafters in den USA.

- FAKE: *Der Irak hat Massenvernichtungswaffen! Insbesondere verfügt Dikator Saddam Hussein über mobile Biowaffen Labore, die auf Tiefladern montiert sind und hochbeweglich.* (US-Verteidigungsminister Rumsfeld und US-Außenminister C. Powell)

  WAHR: Alles komplett erlogen, die Story wurde unter Mithilfe des BND produziert und in der UNO als Grund für einen Überfall auf den Irak präsentiert. Nach dem Bericht der Iraq Survey Group (ISG) besaß der Irak 2003 keine ABC-Waffen.[39]

- FAKE: *Whistleblower Edward Snowden könnte ein russischer Spion sein.* (G. Maaßen, Chef des BfV) oder *Snowden ist ein Russen-Agent.* (J. R. Schindler)

  WAHR: E. Snowden ist gegen seinen Willen in Russland gestrandet, weil der US-Geheimdienst CIA unprofessional gearbeitet hat und unfähig war, Snowden festzusetzen. Russland hat ihm in auswegloser Situation Asyl gewährt.

- FAKE: *Es wird ein No-Spy-Abkommen mit den USA geben.* (Bundeskanzlerin A. Merkel, Innenminister H.-P. Friedrich, Kanzleramtsminister R. Pofalla, S. Seibert)

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

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

  WAHR: Die Mitglieder der AfD gehören überwiegend zur Mittelschicht. Der Anteil der Geringverdiener (unter 2.000 Euro Netto) unter den AfD-Anhängern entspricht mit 27% der Anhängerschaft der CDU (28% Geringverdiener) und ist geringer als bei SPD (32%) und Linke (37%).[40]

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

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

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

  WAHR: Es gab keinen Angriff auf die Telekom, der Ausfall der Router war nur ein Kolateralschaden. Die kriminellen Betreiber des Mirai Botnetzes wollten Zyxel-Router angreifen, die der irische Provider Eir an seine Kunden verteilte und die einen Security Bug im TR-069 Interface haben. Die Telekom Router hatten sich bei den automatisierten Tests des Mirai Botnetzes auf Verwundbarkeit selbst abgeschaltet.[41]

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

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

  WAHR (nach Ländern sortiert):

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

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

  - Bezüglich der Präsidentschaftswahlen in Frankreich teilte der Chef der französischen Nationalen Agentur für Sicherheit der Informationssysteme (ANSSI), Guillaume Poupard, laut der Agentur AP mit, das es keine Spur von russischen Hackerangriffen bei den Wahlen gab.[44]

  - Auch bei den US-Wahlen hatten sich keine russischen Hacker eingemischt. Laut Aussage von Assange wurden die Hillary-E-Mails von dem DNC-Mitarbeiter Seth Rich[45] an Wikileaks geliefert, der im Nov. 2016 beim Joggen erschossen wurde. Wikileaks versprach $20.000 Belohnung für sachdienliche Hinweise, die zur Verurteilung des Mörders von Seth Rich führen können.[46]

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

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

[41] https://www.heise.de/-3520212
[42] https://www.golem.de/news/deutsche-telekom-router-hacker-bekommt-bewaehrungsstrafe-1707-129183.html
[43] https://www.der-postillon.com/2017/07/hacker.html
[44] http://www.washingtontimes.com/news/2017/jun/2/macron-hack-shows-no-sign-russian-involvement-desp/
[45] https://de.sputniknews.com/politik/20170517315781593-usa-russland-leaks-hillary-mord
[46] https://twitter.com/wikileaks/status/763041804652539904
[47] https://consortiumnews.com/2017/07/24/intel-vets-challenge-russia-hack-evidence/

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

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

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

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

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

  WAHR: Drei Tage später wurden die Lockdown Maßnahmen verkündet, die ab 23. März in Deutschland in Kraft traten: Kontaktverbot, Schließung der Geschäfte außer Baumärkte und Lebensmittelversorgung, Schließung der Restaurants, Bars, Spielplätze und des gesamten öffentlichen Lebens, Verbot von Reisen und Demonstrationen...

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

- Im Zeitalter von Twitter und Facebook ist es einfach, den gelangweilten Mob zu einem Shitstorm zu orchestrieren. Ein Beispiel ist Oberst Pedro Banos, der im Juni 2018 den Posten des Geheimdienstkoordinators in Spanien übernehmen sollte. Oberst Banos ist ein absoluter Experte auf dem Gebiet des islamischen Terrorismus. Er hat aber nie seine Meinung verschwiegen, das die Politik der NATO Staaten wesentlich mitverantwortlich dafür ist. In einer Twitter Kampagne wurde er als *pro-russisch* abgestempelt. (Für einen NATO Geheimdienstler der schlimmste Vorwurf.) Der Staatspräsident musste Oberst Banos wenige Tage nach der Ernennung aufgrund des Rummels wieder entlassen. General Miguel Ballesteros wurde zum neuen Geheimdienstchef ernannt, der ein Freund der NATO Politik war. Ende 2018 wurde bekannt, dass die britische *Integrity Initiative* den Shitstorm gegen Banos orchestrierte.[53]

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

[48] https://consortiumnews.com/2018/07/03/former-us-envoy-to-moscow-calls-intelligence-report-on-alleged-russian-interference-politically-motivated
[49] https://www.cnet.com/news/over-40-of-republicans-think-bill-gates-will-use-covid-19-vaccines-to-implant-microchips/
[50] https://twitter.com/bmg_bund/status/1238780849652465664
[51] https://www.facebook.com/bmg.bund/posts/1528002687362904
[52] https://www.zdf.de/nachrichten/panorama/coronavirus-deutschland-europa-usa-100.html
[53] https://www.nachdenkseiten.de/?p=47955

  - In Großbritannien wurde die bisher größte Kampagne der Integrity Initiative durchgeführt. Ziel war es, den Chef der Labour Partei J. Corbyn zu diskreditieren. Auch Corbyn wurde als pro-russisch abgestempelt und als Gefahr für die Demokratie. Eine Analyse von ConsortiumNews[54] zeigt, dass jene namentlich in den Dokumenten genannten Journalisten, die sich an der Kampagne gegen Corbyn beteiligten, ein weiteres Ziel hatten: J. Assange.
  - In Italien folgte die Berichterstattung in den Medien über den Fall Skripal nicht dem vorgegebenen Narrativ aus GB. Der italienische Cluster der Integrity Initiative wurde aktiv, um die Berichterstattung im Mainstream auf Linie zu bringen.
  - Norwegen ist traditionell skeptischer gegenüber der US-Politik und zu wenig anti-russisch eingestellt. Norwegische Journalisten tendieren dazu, Informationen von russischer Seite die gleich Gewichtung zuzusprechen, wie Informationen aus westlichen NATO Ländern oder den USA. Seit 2016 ist die Integrity Initative in Norwegen aktiv, um durch geeignete Maßnahmen etwas gegen diese gefährliche Starrköpfigkeit zu unternehmen.

  Für russische Medien ist es *the biggest story of 2018*, in deutschen Medien habe ich mit Ausnahme von Telepolis[55] [56] [57] [58] fast nichts über die Integrity Initiative gelesen. Am gleichen Tag, als Anonymous die Dokumente über den deutschen Cluster der Integrity Initiative veröffentlichte, hat der Spiegel ein Fake News Fall im eigenen Haus publik gemacht und alle deutschen Medien waren mit Claas Relotius[59] beschäftigt. Als am 03. Jan. neue Dokumente zur Integrity Intiative veröffentlicht wurden, war in Deutschland der Promi-Leak[60] das große Ereignis, das andere Leaks überdeckte.

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

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

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

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

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

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

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

[54] https://consortiumnews.com/2019/01/14/the-twitter-smearing-of-corbyn-and-assange/
[55] https://www.heise.de/tp/features/Integrity-Initiative-Britische-Beeinflussungskampagne-gegen-Russland-4232365.html
[56] https://www.heise.de/tp/features/Infowar-oder-Absurdistan-Britisches-Aussenministerium-im-Strudel-der-Desinformation-4253994.html
[57] https://www.heise.de/tp/features/Neues-von-der-britischen-Beeinflussungskampagne-des-ominoesen-Institute-of-Statecraft-4266174.html
[58] https://www.heise.de/tp/features/Integrity-Initiative-taucht-ab-4286004.html
[59] http://www.spiegel.de/kultur/gesellschaft/fall-claas-relotius-spiegel-legt-betrug-im-eigenen-haus-offen-a-1244579.html
[60] https://www.heise.de/-4265180
[61] https://twitter.com/BuzzFeedNewsDE/status/1064538241880203264
[62] https://www.privacy-handbuch.de/diskussion.htm#08_01_19

Andere Beispiele sind falsche Politiker Zitate, mit denen man hohe Klickraten und Likes erzielt, die aber leicht als Fake erkennbar sind, wie zum Beispiel das Zitat in Abb. 2.5 aus dem Blog von Sven Liebich. In einem Spiegel Interview sagte M. Schulz, dass man die Typen von der AfD bekämpfen muss, aber er sagte nichts von Lagern.[63]

Abbildung 2.5: Fake News: Falsches Zitat von M. Schulz mit hohen Klickraten

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

2.5.3 Medienkompetenztraining

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

Ein bisschen Medienkompetenztraining an Fake News Beispielen:

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

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

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

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

[63] http://www.spiegel.de/politik/ausland/martin-schulz-ueber-afd-diese-typen-muss-man-bekaempfe-a-1078912.html
[64] https://www.youtube.com/watch?v=VwrYIuAvMPE

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

> *Die Zahl der Vergewaltigungen ist im ersten Halbjahr 2017 im Vergleich zum Vorjahreszeitraum in Bayern um 47,9 Prozent angestiegen. [...] Gerade die Zahl der durch Zuwanderer begangenen Vergewaltigungsdelikte ist mit +90,9 Prozent ein Offenbarungseid gescheiterter Grenzsicherung.*
>
> *Klartext: Ohne die massenhaften illegalen Grenzübertritte hätte es auch nicht den explosionsartigen Anstieg an Vergewaltigungen gegeben, nicht nur in Bayern.*

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

Eine genauere Analyse[66] der Zahlen zeigt, dass die Zahl der Vergewaltigungen im Vergleich zum Vorjahr nur gering gestiegen ist, um 5% von 68 auf 71 und damit innerhalb der normalen Schwankungen. Die Zahl der tatverdächtigen Deutschen ist etwas gesunken und die Zahl der tatverdächtigen Zuwanderer ist von 8 auf 17 gestiegen. Ein explosionsartiger Anstieg durch 1,5 Mio Zuwanderer sieht anders aus.

2.5.4 Fake News oder Propaganda - was ist der Unterschied?

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

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

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

Es wurden neben Fake News auch alle anderen propagandistischen Methoden verwendet. Die Berichterstattung des ÖRR wurde vom Programmbeirat der ARD als fragmentarisch, tendenziös, mangelhaft und einseitig gerügt[68]. Und das nennt man **Propaganda**.

2.6 Geotagging

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

[65] https://www.heise.de/tp/features/Vergewaltigungen-in-Bayern-Herrmann-muss-Schockzahlen-zurechtruecken-3837889.html
[66] https://www.heise.de/tp/features/Vergewaltigungen-in-Bayern-Herrmann-muss-Schockzahlen-zurechtruecken-3837889.html
[67] https://www.rt.com/news/369828-russia-america-relations-trump-advisor/
[68] https://www.heise.de/tp/features/Ukraine-Konflikt-ARD-Programmbeirat-bestaetigt-Publikumskritik-3367400.html

2. Die Analyse des Soziales Umfeldes ist mit den Standortdaten ebenfalls möglich. Die Summe aller Standortdaten ist mehr, als die Anhäufung der Standorte von Person A, B und C. Wie die Studie *Inferring social ties from geografic coinsidences*[69] zeigt, ermögliche diese Sammlung detaillierte Informationen über das soziale Umfeld, auch wenn man bei Facebook nicht befreundet ist. Die Standortdaten der Smartphones verraten, mit wem man regelmäßig ein Bier trinkt, mit wem man ins Bett steigt, ob man an Pegida Demonstrationen teilnimmt oder sich in Antifa Zirkeln trifft und vieles mehr.

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

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

   Die Firma Dataminr bietet Kunden via API Zugriff auf die Twitter Postings und wirbt in einem Flyer am Beispiel eines Studentenprotestes in Südafrika damit, wie man das neue Geospatial Analyse Tool Bild 2.6 zum Monitoring von politischen Demonstrationen nutzen kann.

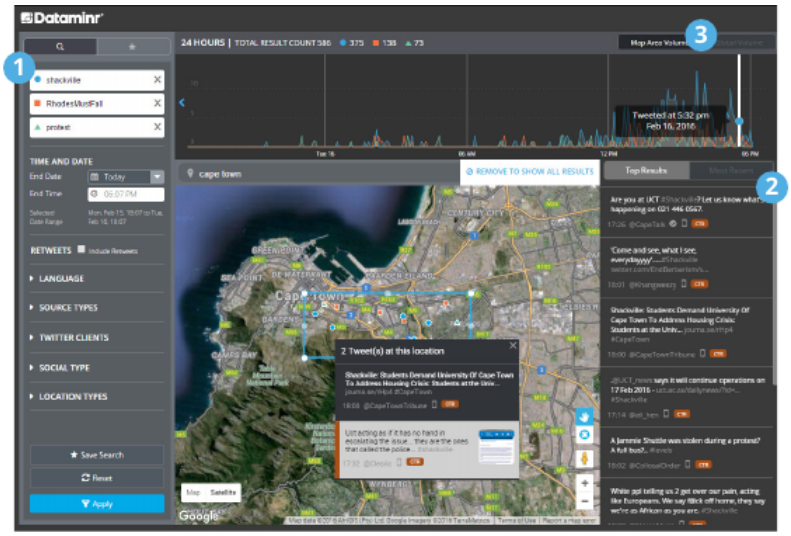


Abbildung 2.6: Auswertung der Twitter Postings eines Studentenprotestes in Südafrika aufgrund der Geoloaction der Postings

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

   Es entsteht ein fast vollständiges Modell. Mit der Beobachtung dieser Signale kann man ganze Firmen, ganze Städte, eine ganze Gesellschaft röntgen [70].

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

[69] http://www.pnas.org/content/107/52/22436.short
[70] https://www.heise.de/tr/artikel/Immer-im-Visier-276659.html

trackt. Muslimische Communities werden systematisch analysiert, ohne dass die betroffenen Personen im Verdacht einer Straftat stehen. Das Geotracking von GPS-fähigen Smartphones und GPS-Modulen moderner Fahrzeuge durch das FBI erfolgt ohne richterlichen Beschluss.

> *. . . the pushpins on the new FBI geo-maps indicate where people live, work, pray, eat and shop, not necessarily where they commit or plan crimes* [71].

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

Die Daten werden mit verschiedenen Methoden gesammelt:

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

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

- Mit Einführung des iPhone 4 hat Apple seine Datenschutzbestimmungen geändert. Die gesamte Produktpalette von Apple (iPhone, Laptops, PC. . .) wird in Zukunft den Standort des Nutzers laufend an Apple senden. Apple wird diese Daten Dritten zur Verfügung stellen. Wer Zugang zu diesen Daten hat, wird nicht näher spezifiziert.[72]

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

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

  Das chinesische Staatsfernsehen bezeichnete die Möglichkeit des Auslesens häufig besuchter Orte im iPhone als Risiko für die nationale Sicherheit [73], da die Daten bei US-Firmen gespeichert werden, die im Rahmen von PRISM mit der NSA kooperieren.

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

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

[71] https://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims
[72] https://www.apple.com/chde/legal/privacy/
[73] https://www.heise.de/-2257924

Abbildung 2.7: Lokalisierung eines Smartphones durch Facebook

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

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

Nichts zu verbergen?

Wer ein praktisches Beispiel braucht: Krankengeld gestrichen und Job verloren, weil er auf Facebook Urlausbfotos veröffentlichte. Andreas H. litt an Depressionen. Er ging zum Arzt und wurde krank geschrieben. Seine Ärzte rieten ihm zu einem Urlaub. Facebook-Fotos mit Surfbrett am Strand kosteten ihn erst das Krankengeld - und dann den Job.[74]

2.7 Kommunikationsanalyse

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

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

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

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

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

Zivile Kommunikations-Analyse

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

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

Ein Beispiel

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

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

Durch Auswertung aller zur Verfügung stehenden Kommunikationsdaten von *Anton* und *Beatrice* erhält man ein umfangreiches Netz ihrer sozialen Kontakte (Bild 2.8). Dabei wird nicht nur die Anzahl der Kommunikationsprozesse ausgewertet, es wird auch die zeitliche Korrelation einbezogen.

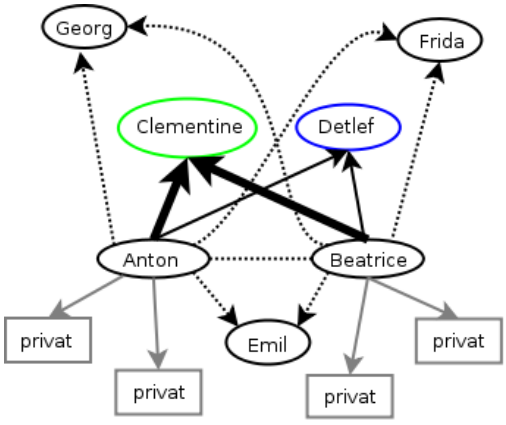


Abbildung 2.8: Soziales Netz von Anton und Beatrice

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

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

Frida unterhält vor allem einen engen Kontakt zu *Detlef*, was zu einer Umbewertung der Positionen von *Detlef* und *Clementine* führt (Bild 2.9). Bei *Emil* handelt es sich evtl. um einen zufällig gemeinsamen Bekannten von *Anton* und *Beatrice*, der nicht in die "mg" eingebunden ist.

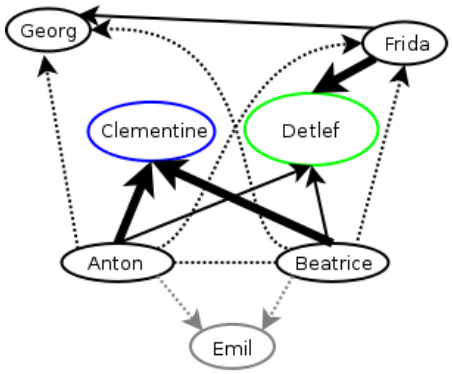


Abbildung 2.9: Präzisierte Struktur der "mg"

Reale Datenmmengen

Reale Kommunikationsnetzwerke sind wesentlich komplexer. Auf Grundlage der Daten, die von T-Mobile über den Politiker Malte Spitz gespeichert wurden, hat Michael Kreil von OpenDataCity die Grafik in Bild 2.10 mit den Rohdaten erstellt.

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

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

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

2.8 Überwachungen im Internet

Unter https://www.daten-speicherung.de/index.php/ueberwachungsgesetze findet man eine umfassende Übersicht zu verschiedenen Sicherheitsgesetzen 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!** [75]

[75] http://www.dubistterrorist.de

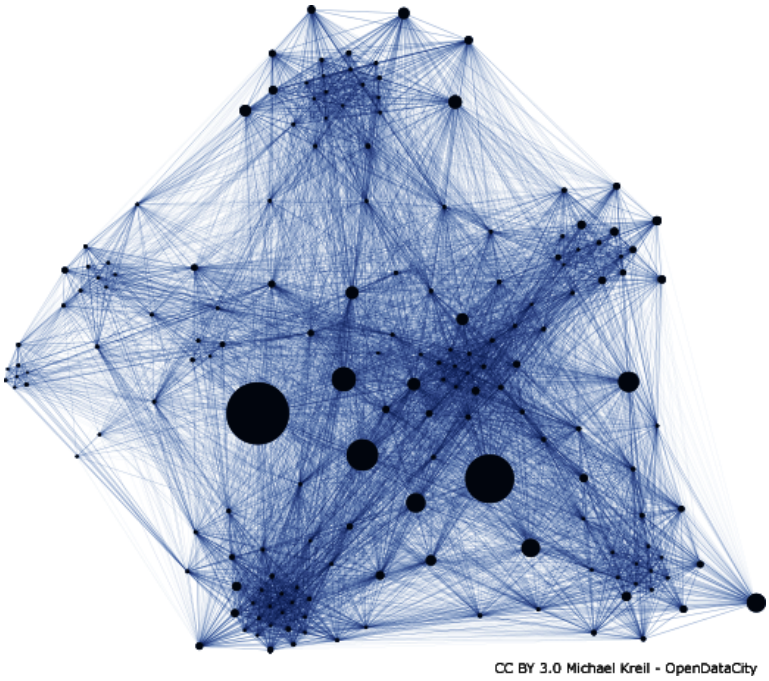


Abbildung 2.10: Kommunikationsnetzwerk von Malte Spitz

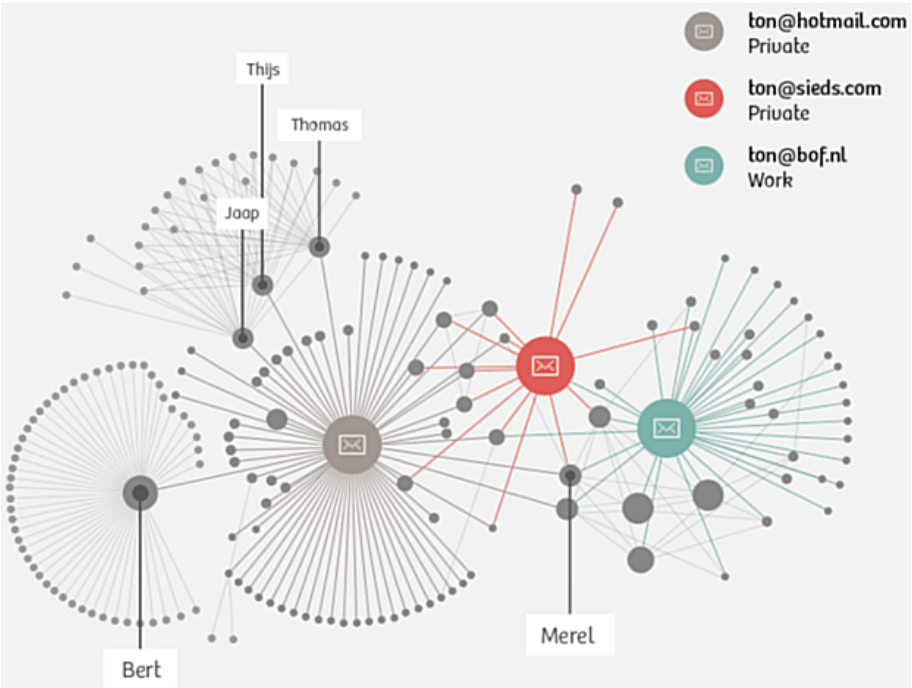


Abbildung 2.11: Aufbereitete Kommunikationsdaten von Ton Siedsmas

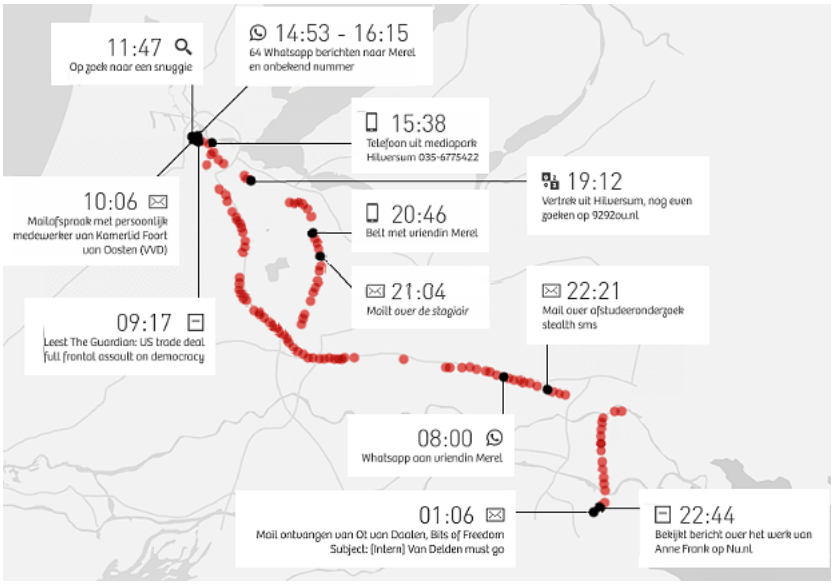


Abbildung 2.12: Standortdaten eines Tages von T. Siedsmas

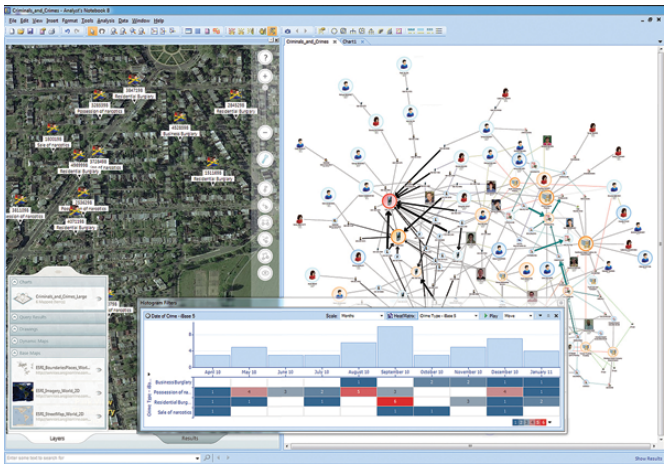


Abbildung 2.13: Screenshot von *i2 Analyst's Notebook* (IBM)

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

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

- 1997 wurde die Vorratsdatenspeicherung aufgrund verfassungsrechtlicher Bedenken abgelehnt.
- 2002 wurde ein ähnlicher Gesetzentwurf vom Deutschen Bundestag abgelehnt und die Bundesregierung beauftragt, gegen einen entsprechenden Rahmenbeschluß auf EU-Ebene zu stimmen (Bundestag-Drucksache 14/9801).
- 2005 hat das EU-Parlament mit Mehrheit der christ- und sozialdemokratischen Fraktionen die Richtlinie zur 6-monatigen Datenspeicherung der Verbindungs- und Standortdaten (VDS) beschlossen (Directive 2006/24/EG). Um die Richtlinie mit einfacher Mehrheit in der EU-Kommision ohne Mitsprache des Parlamentes verabschieden zu können, wurde sie nicht als Sicherheits- und Polizeimaßnahme behandelt sondern als Maßnahme zur *Regulierung des Binnenmarktes* definiert, was außerdem die EU-Länder zu einer Umsetzung zwingt.
- 2006 hat der Wissenschaftliche Dienst des Bundestages ein Rechtsgutachten mit schweren Bedenken gegen die VDS vorgelegt.
- Ein Vergleich der Zahlen der Kriminalitätsstatistik des BKA für die Jahre 2007, 2008 und 2009 zeigt, dass die VDS im Jahr 2009 nicht zur einer Verbesserung der Aufklärungsrate von Straftaten im Internet führte und keine Einfluss auf die Tendenz der Entwicklung hatte. Es gibt mehr Straftaten im Internet bei abnehmender Aufklärungsrate.

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

- 2010 erklärt das Bundesverfassungsgericht in einem Grundsatzurteil das Gesetz zur VDS als nicht vereinbar mit dem Grundgesetz. (Az: 1 BvR 256/08)[76]
- 2012 zeigte das Max-Planck-Instituts (MPI) für ausländisches und internationales Strafrecht in einer umfangreichen wissenschaftlichen Analyse, dass KEINE *Schutzlücke* ohne Vorratsdatenspeicherung besteht und widerspricht damit der Darstellung von mehreren Bundesinnenministern und BKA-Chef Ziercke, wonach die VDS für die Kriminalitätsbekämpfung unbedingt nötig wäre. Die in der Presse immer wieder herangezogenen Einzelbeispiele halten einer wissenschaftlichen Analyse nicht stand.[77]
- 2012 gibt es einen nicht erfolgreichen Anlauf, die VDS international im Rahmen der UNODC als verpflichtende Richtlinie zu etablieren. Der Verfassungsschutz hat diesen Versuch offensiv unterstützt.[78]
- 2014 wird die Richlinie 2006/24/EG vom EuGH als nicht vereinbar mit der Charta der Grundrechte der Europäischen Union gekippt. (Urteil C-293/12 und C-594/12)

[76] http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html
[77] https://www.ccc.de/de/updates/2012/mythos-schutzluecke
[78] https://netzpolitik.org/2012/uno-bericht-der-kampf-gegen-terroristen-beginnt-im-internet-mit-vorratsdatenspeicherung-und-identifizierungspflicht/

- 2015 wird im Eilverfahren ein neues Gesetz zur *Speicherpflicht für Verkehrsdaten* verabschiedet. Bundesjustizminister H. Maas konnte auf der Pressekonferenz zur Verabschiedung des Gesetzentwurfes im Bundeskabinett auf Nachfrage keinen Grund nennen, warum die Vorratsdatenspeicherung notwendig sein soll:

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

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

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

- Am 16.10.2015 hat der Bundestag erneut das neue Gesetz zur Vorratsdatenspeicherung beschlossen. Verfassungsklagen wurden inzwischen eingereicht.
- 2017 legt der Wissenschaftliche Dienst zum wiederholten Mal ein Gutachten zur Vorratsdatenspeicherung vor, dass zu dem Schluss kommt, dass das aktuelle Gesetz nicht nicht mit geltendem EU-Recht vereinbar ist. In mehreren Punkten verstößt das neue Gesetz gegen die Vorgaben des Europäischen Gerichtshofes.[79]

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

Bestandsdatenauskunft Der IT-Sicherheitsforscher Pete Swire hat im April 2012 ein Paper[80] veröffentlicht, in dem er die aktuellen Tendenzen in der Überwachung aufzeigt. Weil das *Lauschen am Draht* in allen Variationen zunehmend uneffektiv wird, wollen Geheimdienste und Strafverfolger Zugriff auf die *Daten in der Cloud*. Dazu zählen auch E-Mail Accounts. Die Hürden für den Zugriff sollen dabei möglichst gering sein.

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

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

Die PiratenPartei kommentierte den Gesetzentwurf kurz und bündig:

> *Der Entwurf der Bundesregierung ist schlicht verfassungswidrig.*

Zensur im Internet: Die Zensur sollte in Deutschland im Namen des Kampfes gegen Kinderpornografie im Internet eingeführt werden. Man wurde nicht müde zu behaupten, es gäbe einen Millionen Euro schweren Massenmarkt, der durch Sperren von Webseiten empfindlich ausgetrocknet werden kann. Die Aussagen wurden geprüft und für falsch befunden [81].

[79] https://netzpolitik.org/2017/gutachten-gesetz-zur-vorratsdatenspeicherung-erfuellt-vorgaben-des-eugh-nicht/
[80] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038871
[81] http://blog.odem.org/2009/05/quellenanalyse.html

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

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

Die verfassungsrechtlichen Bedenken gegen die Zensur hat der wissenschaftliche Dienst des Bundestages in einem Gutachten zusammengefasst[84]. Auch eine Abschätzung der EU-Kommision kommt zu dem Schluss, dass diese Sperrmaßnahmen **notwendigerweise eine Einschränkung der Menschenrechte voraussetzen**, beispielsweise der freien Meinungsäußerung.

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

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

Damit wird sich das BKA bis zu einem gewissen Grad jeglicher Kontrolle, der justiziellen und erst recht der parlamentarischen, entziehen können [85].

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

[82] http://ak-zensur.de/2010/08/kapitulation.html
[83] http://www.eco.de/verband/202_8727.htm
[84] https://netzpolitik.org/wp-upload/bundestag_filter-gutachten.pdf
[85] http://www.berlinonline.de/berliner-zeitung/print/politik/725127.html

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.

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

- Doppeleinstellung in Sachen §129 [86]
- Razzien im Vorfeld des G8-Gipfels waren rechtswidrig [87]
- Konstruieren und Schnüffeln mit §129a [88]
- Durchsuchungen beim LabourNet waren rechtswidrig [89]

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

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

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

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

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

[86] http://de.indymedia.org/2008/10/228421.shtml
[87] http://www.ag-friedensforschung.de/themen/Globalisierung/g8-2007/bgh.html
[88] http://www.neues-deutschland.de/artikel/175230.konstruieren-und-schnueffeln-mit-s-129a.html
[89] http://www.labournet.de/ueberuns/beschlagnahme/index.html

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

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

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

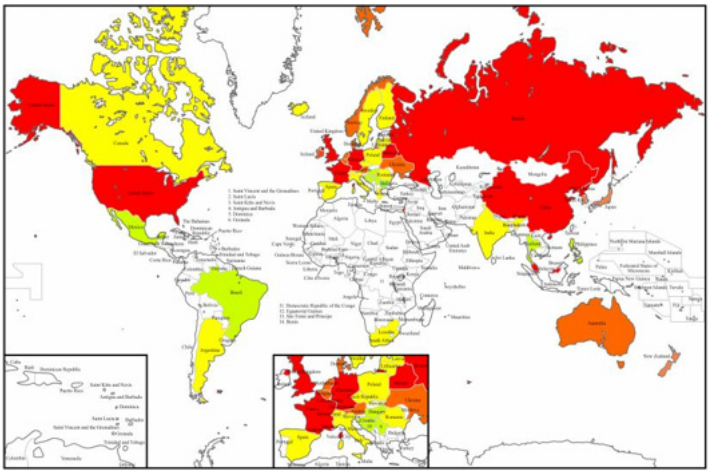


Abbildung 2.14: Vergleich der elektronischen Polizeistaaten

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

Ähnliche Meldungen hatten in den letzten Jahren viel weniger Resonanz:

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

2.9 Terrorismus und der Ausbau der Überwachung

Nach den Anschlägen von Paris im Nov. 2015 eskaliert der Ausbau der Überwachung und wird als die angebeblich einzige Alternative zum Schutz der Bevölkerung diskutiert. Die EU erlaubt Frankreich sogar die Verletzung der Euro-Stabilitätskriteriern[90], weil

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

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

Jemand hat die Toten durch Terroranschläge in Europa in den letzten Jahrzehnten aufgeschlüsselt. Die Grafik 2.15 auf Basis der Daten der *Global Terrorism Database*[91] zeigt, dass Europa hinsichtlich Terrorgefahr noch nie so sicher war, wie heute.

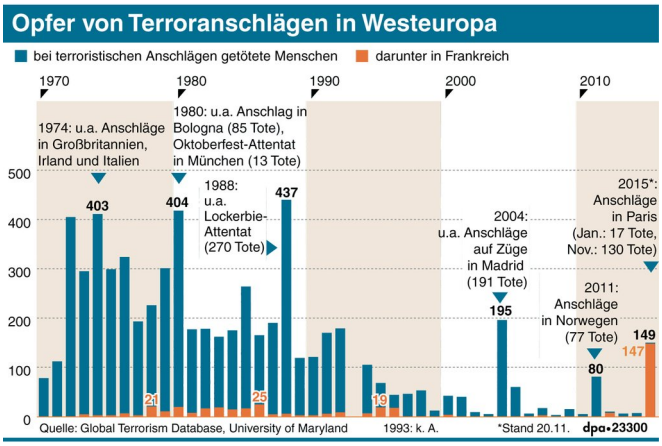


Abbildung 2.15: Opfer von Terroranschlägen in Westeuropa

Die jährlichen *EU Terrorism Reports* von Europol zeigen das gleiche Bild. 2005/2006 gab es fast 500 Terroranschläge pro Jahr in Europa, also mehr als ein Anschlag pro Tag und mehr als 700 Verhaftungen (siehe: TE-SAT Report für 2006 [92]). Hauptverantwortlich waren die ETA, die IRA und die italienischen Korsen. In dieser Zeit wurde ein Anschlag mit 191 Toten in Madrid zwar zur Kenntnis genommen, ein bisschen diskutiert und am nächsten Tag wieder vergessen.

Bis 2010 konnte durch politische Maßnahmen die Zahl der Terroranschläge im Vergleich zu 2006 halbiert werden, es gab nur noch 246 Anschläge[93]. Der Europol-Bericht TE-SAT 2014 listet noch 152 Terroranschläge mit 7 Toten auf, der niedrigste Stand.[94]

2015 wurde wieder ein Anstieg bei Terroranschlägen verzeichnet (insgesamt 211 Anschläge). Während sich linke und separatitische Anschläge weiter verringerten (nur noch 65), kam es zu einer Zunahme von jihadistischen Anschlägen vor allem in Frankreich. Dabei starben 148 Personen, da jihadististische Selbstmordattentäter eine möglichst hohe Zahl von Todesopfern erzielen wollen. 687 potentielle islamistische Attentäter wurden verhaftet, davon wurden 98% verurteilt.[95]

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

In Deutschland gab es einen Anschlag in diesem Kontext, der Terrorist Anis Amri fuhr

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

mit einem LKW im Dez. 2016 in den Berliner Weihnachtsmarkt. Auch dieser Terrorist war den Sicherheitsbehörden bekannt, er war in den Wochen vor dem Anschlag das Top-1-Thema der deutschen Terrorabwehr, BKA und Verfassungschutz waren über die Gefahr informiert, der marokkanische Geheimdienst hatte gewarnt und trotzdem. . . .[96]

Als Konsequent aus dem Anschlag forderten Bundesinnenminister Thomas de Maizière (CDU) und andere Politiker reflexartig einen Ausbau der Überwachung. Insbesondere die Videoüberwachung steht auf der Wunschliste. C. Ströbele, ehem. Mitglied des Bundestages und der PKGr, zieht andere Konsequenzen aus dem Fall Amri:[97]

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

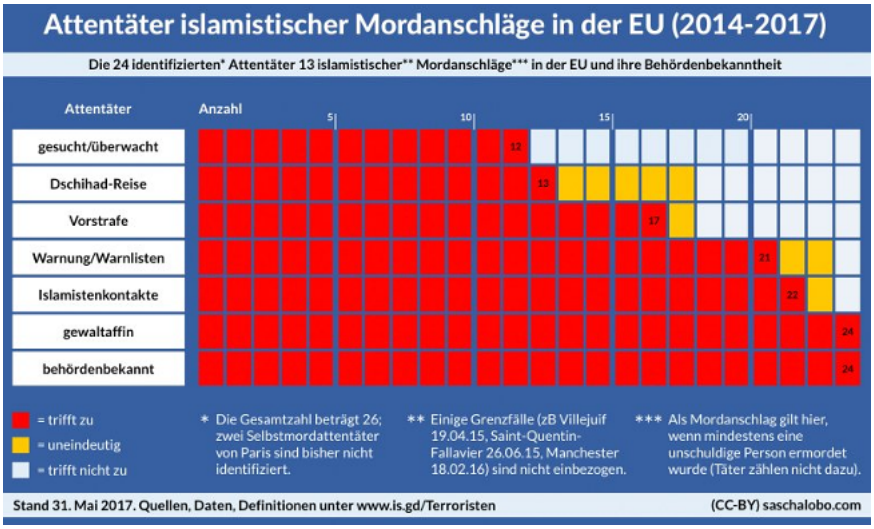


Abbildung 2.16: Alle 24 Terroristen mit islamistischen Hintergrund waren vor den Anschlägen als gewaltbereite Gefährder bekannt

Die Terrorgefahr in Europa wurde im letzten Jahrzehnt nicht durch den Ausbau der Überwachung reduziert, sondern durch einen politischen Integrationsprozess der separatistischen Gruppen. Warum wird dieses erfolgreiche Konzept jetzt nicht mehr diskutiert? Das Frankreich und Belgien auf diesem Gebiet der Integration massive Defizite haben, ist seit Jahren bekannt. Der vom franz. Präsidenten Hollande ausgerufenen *Krieg gegen den Islamismus* ist keine Lösung, auch nicht mit 5.000 Mann mehr Personal für die Dienste.

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

Manchmal bin ich schockiert, wie stark die emotionale Wirkung der Panik-Medien geworden ist. Eine Mutter sprach einigen Tagen nach dem Anschlag in Paris in privater Runde über die Angst, dass ihre 17-jährige Tochter einem Terroranschlag zum Opfer fallen könnte, wenn sie abends allein in Berlin unterwegs ist. Ähmm - .... also ich würde eher auf Autounfall oder Unfall mit dem Fahrrad tippen, diese Gefahr ist unver-

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

ändert hoch. Das Fahrrad vom Töchterchen hatte nämlich kein funktionierendes Rücklicht.

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

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

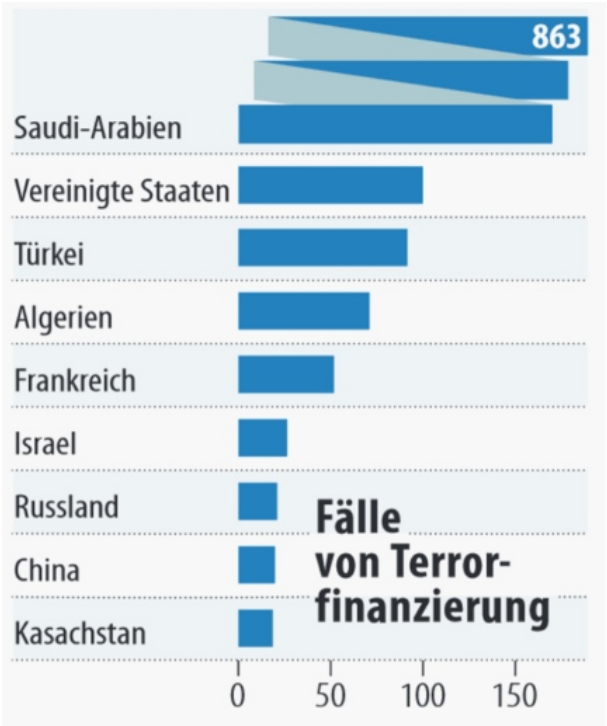


Abbildung 2.17: Staaten, die Terroristen finanzieren

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

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

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

2.10 NSA & Co.

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

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

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

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

Die FISA-Regeln wurden in der Folgezeit immer weiter aufgeweicht, insbesondere nach 9/11 durch den Patriot Act (2001) und den FISA-Amendmends Act (2008). Gemäß den aktuellen Auslegungen darf die NSA von den Telekommunikationsanbietern und Internetfirmen die Übermittlung kompletter Datenbanken verlangen, um darin selbst zu suchen.

2013 ein Déjà-vu

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

Diese Geheimdienste agieren außerhalb jeder Kontrolle.

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

2.11 Bundesamt für Verfassungsschutz auflösen

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

Die Humanistische Union fordert seit Jahren die Auflösung des BfV [99]. Die Piraten-Partei Thüringen forderte im Beschluss des Parteitages im Nov. 2011 eine Auflösung des Thüringer Verfassungsschutzes[100] (wenige Tage bevor der NSU-Skandal bekannt wurde) und kritisiert die Übernahme der Strukturen in das Innenministerium. Die Linke in Hessen plädiert für die Auflösung des Verfassungsschutzes[101] und möchte statt dessen eine Informations- und Dokumentationsstelle einrichten für Bestrebungen gegen die Verfassung (ohne V-Leute und ohne geheimdienstliche Kompetenzen). Als Konsequenz aus dem NSA-Skandal forderte der Chaos Computer Club die Auflösung des BfV zur Wiedereinführung von Grundrechten und Rechtsstaatlichkeit[102].

Auflösungserscheinungen sind beim Verfassungschutz aber nicht erkennbar. Wie in jedem Jahr wird auch 2017 das Budget des Inlangeheimdienstes erhöht, diesmal um 45 Mio. Euro. Damit hat sich der Etat des Geheimdienstes im Vergleich zu 2000 verdreifacht!

V-Leute sind keine Lösung, sondern das Problem

- V-Leute des Verfassungsschutzes hatten erheblichen Anteil an der Radikalisierung der Studentenbewegung 1968. Vor allem der V-Mann Peter Urbach wird immer wieder als Agent Provocateur genannt, der auch Waffen und Molotow-Cocktails lieferte und nach seiner Enttarnung vom Verfassungsschutz ins Ausland gebracht wurde.[103]

- Die Verflechtungen von Verfassungsschutz und *RAF* sind noch immer nicht aufgeklärt. Aus alten Unterlagen der Stasi geht hervor, dass Verena Becker vom Verfassungsschutz "kontrolliert wurde". V. Becker spielte eine wesentliche Rolle beim Mord an Generalbundesanwalt Buback.[104]

- Der Verfassungsschutz hat die rechtsradikale Szene nicht unterwandert, sondern finanziell unterstützt und vor Strafverfolgung geschützt.

  - Laut einem BKA-Report [105] von 1997 soll der Verfassungsschutz rechtsradikale Neonazis systematisch geschützt haben. Die Vorwürfe werden mit konkreten Fällen untermauert. V-Leute wurden vor Durchsuchungen gewarnt und einer Straftat überführte Nazis wurden nicht angeklagt und verurteilt, wenn sie als V-Leute arbeiteten. Informationen wurden zu spät an die Polizei weitergeleitet, so dass rechtsradikale Aktionen nicht mehr verhindert werden konnten.

  - Bereits 2002 hat das LKA Sachsen-Anhalt dem Verfassungsschutz misstraut und aus *ermittlungstaktischen Gründen* nicht über Exekutivmaßnahmen in der rechten Szene informiert. Aus einem Vermerk des Bundesinnenministeriums:[106]

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

  - 2008 wurden Ermittlungen gegen den Neonazi Sebastian Seemann eingestellt. Er baute das verbotene *Blood and Honour* Netzwerk auf und war im schwerkriminellen Millieu aktiv (Drogen- und Waffenhandel). Der Verfassungsschutz warnte ihn vor Exekutivmaßnahmen. Mitarbeiter des Verfassungsschutzes wurden daraufhin wegen Geheimnisverrats und Strafvereitelung im Amt angeklagt. Auf Veranlassung des Innenministers wurden die Anklagen eingestellt.[107]

[99] http://www.humanistische-union.de/fileadmin/hu_upload/doku/publik/huschrift17.pdf
[100] http://www.piraten-thueringen.de/2012/10/verfassungsschutz-auflosen-statt-umbetten/
[101] http://www.fr-online.de/rhein-main/hessen-linke-will-verfassungsschutz-aufloesen,1472796,17278430.html
[102] https://www.ccc.de/de/updates/2013/demonstration-wiedereinfuehrung–rechtsstaatlichkeit
[103] https://www.heise.de/tp/blogs/8/151641
[104] https://www.heise.de/tp/artikel/31/31120/1.html
[105] http://www.spiegel.de/panorama/justiz/verfassungsschutz-soll-rechte-v-leute-vor-strafverfolgung-geschuetzt-haben-a-865154.html
[106] https://www.taz.de/Neonazi-Ermittlungen/!103340/
[107] https://www.nadir.org/nadir/initiativ/azzoncao/donazi3.html

Das ist seit mehreren Jahren bekannt. Konsequenzen? Nur die Landesregierung in Thüringen unter Führung von B. Ramelow (Linke) geht den entgegengesetzten Weg und schafft die V-Leute des BfV ab, weil das V-Leute-System nicht die Sicherheit erhöht, sondern die Demokratie gefährdet.[108] Der Bundesinnenminister möchte die Straffreiheit für staatlichen Spitzel erweitern, damit sie stärker an szenetypischen Aktionen teilnehmen können (z. B Brandanschläge auf Unterkünfte für Asylbewerber u.ä.)

Strategie der Spannung

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

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

- Der V-Mann Melvüt Kar hat drei Terrorzellen aufgebaut und an die Behörden verraten. Melvüt Kar wurde in Deutschland nie angeklagt und lebt unbehelligt in Istanbul in der Türkei.[109]
  - Die erste Terrorzelle mit Mutlu A., Mohamed El-A. und Issam El-S wurde am 17. Februar 2003 von der GSG9 verhaftet und am gleichen Tag aus Mangel an Beweisen wieder freigelassen.
  - Die Verhaftung der zweiten Terrorzelle mit Dzavid B., Nedzad B., Ahmed H., Bekim T. und Blerim T. wurde von den Medien weitgehend ignoriert.
  - Der größte Coup von Mevlüt K. war die Sauerländer Terrorzelle, die von ihm für die Vorbereitung von Terroranschlägen mit Sprengzündern versorgt wurde.

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

- Ein weiterer V-Mann des Verfassungsschutzes in der islamistischen Szene war Yehia Yousif, der mittlerweile in Saudi-Arabien lebt und auch eine Schlüsselrolle in der Radikalisierung der Sauerland Gruppe spielte. Yousif hat wesentlich zum Erstarken salafistischer Gruppen in Deutschland beigetragen.[110]

- Die *Globale Islamische Medienfront* (GIMF) drohte 2007 in Videos mit Terroranschlägen in Deutschland. Im Gerichtsverfahren gegen Mitglieder der GIMF kam heraus, dass der Anführer dieser Gruppe ein V-Mann des Verfassungsschutzes war. Irfan Peci soll monatlich 2.500 - 3.000 Euro vom Verfassungsschutz erhalten haben. Außerdem finanzierte das BfV seine Ausbildung an Waffen in einem Terrorcamp in Bosnien und deckte Straftaten von I. Peci. Gegen den V-Mann wurde keine Anklage erhoben.[111]

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

- Anis Amri, der Attentäter mit dem LKW auf dem Berliner Weihnachtsmarkt 2016, wurde von einem V-Mann des LKA zu dem Anschlag angestachelt. Es ist bekannt, dass der V-Mann nicht nur A. Amri zu Anschlägen in Deutschland anstacheln wollte und dass er das radikalste Mitglied der Gruppe *Abu Walaa* war. Er hat es neben A. Amri auch bei anderen Männern der Gruppe versucht. Dokumentiert ist folgende Aussage von ihm:

[108] https://www.taz.de/Verfassungsschutz-in-Thueringen/!156778/
[109] https://www.heise.de/tp/artikel/35/35986/1.html
[110] https://www.heise.de/tp/blogs/8/150854
[111] https://www.heise.de/tp/blogs/8/150854

Komm, du hast eh keinen Pass, mach hier was, mach einen Anschlag.[112]

Außerdem wurden die Akten beim Berliner LKA über A. Amri gefälscht, um eine vorzeitige Festnahme und Veruteilung wegen bandenmäßiger Kriminalität und gewerbsmäßigen Drogendelikten zu vermeiden. Der Berliner LKA Präsident zeigte sich schockiert und ratlos über diesen Vorgang, der nach dem Attentat bekannt wurde.[113]

Neben A. Amri wurde auch Mikail S. von diesem V-Mann zu Anschlägen angestachelt. Mikail S. wurde rechtzeitig verhaftet. Sein Strafverteidiger sieht es als erwiesen an, das der V-Mann ein *agent provocateur im Dienste des Staates* ist.

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

Schutz gegen Wirtschaftsspionage???

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

Tatsächlich wurde bis zum heutigen Tage in ganz Europa kein einziger Fall amerikanischer oder britischer Wirtschaftsspionage nachgewiesen.[114]

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

Mir sind über 50 solcher Fälle von Wirtschaftsspionage bekannt. Wenn wir auf solche Aktivitäten stoßen, werden wir von unseren Vorgesetzten zurückgepfiffen. Wir dürfen unsere Erkenntnisse meist weder an den Staatsanwalt noch an die betroffenen Firmen weitergeben. Aus Rücksicht auf unsere Verbündeten.[115]

Den spektakulären Fall Enercon[116] findet man leicht, wenn man bei einer Suchmaschine der Wahl die passenden Suchbegriffe nach Wirtschaftsspionage der NSA in Deutschland eingibt, für Hr. Maaßen ist das wohl zuviel verlangt.

Auch dem BND waren die Ambitionen der NSA zur Wirtschaftsspionage seit Jahren bekannt, wie der Ex-General D. Urmann vor dem Untersuchungsschuss des Bundestages erklärte.[117] Wurde Verfassungschutzpräsident Maaßen nicht darüber informiert?

NSU-Skandal

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

[112] https://www.rbb24.de/politik/beitrag/2017/10/amri-von-v-mann-angestachelt-anschlag-berlin-breitscheidplatz.html
[113] https://www.heise.de/tp/features/Fall-Amri-Neues-Dokument-schwere-Vorwuerfe-gegen-das-LKA-3716338.html
[114] https://www.heise.de/-1943975
[115] http://web.archive.org/web/20001208141100/http://www.wdr.de/tv/plusminus/archiv/980414/lauschangr.html
[116] https://de.wikipedia.org/wiki/Enercon
[117] https://www.heise.de/-2569294

- Der V-Mann Florian H.[118] verbrannte beispielsweise in seinem Auto wenige Stunden bevor das BKA ihn als Zeuge vernehmen wollte. Die Polizei diagnostizierte Selbstmord aus Liebeskummer, obwohl seine Freundin nichts von Liebeskummer wusste und es keinen Abschiedsbrief gab. Die Familie des V-Manns erhebt schwere Vorwürfe wegen schlampiger Ermittlungen bei der Polizei.[119]

- Melissa M. (Ex-Freundin von Florina H.) starb, nachdem sie als Zeugin vorgeladen wurde aber bevor sie eine Aussgae machen konnte.

- Sascha W. lebte mit Mellisa M. zusammen und wurde kurz darauf in seiner Wohnung erhängt aufgefunden. Seine Freunde bestreiten, dass es Anzeichen von Lebensmüdigkeit bei ihm gab.

- Der wertvolle V-Mann Thomas R. lieferte dem BfV viele Informationen über den NSU. Vor Gericht verweigerte er die Aussage. Er starb überraschend an einem Zucker-Schock (Diagnose: nicht behandelte schwere Diabetis), bevor er in Beugehaft genommern werden konnte, um eine Aussage zu erzwingen.[120]

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

- 47 Mitarbeiter der Abteilung Rechtsextremismus wurden befördert. Drei Mitarbeiter, die direkt für die Aktenvernichtung verantwortlich waren, wurde auf andere Posten versetzt ohne dienstrechtliche oder strafrechtliche Konsequenzen.[121]

- Am 3. Jahrestag der Aufdeckung des NSU-Skandals besuchte Merkel offiziell das Bundesamt für Verfassungsschutz. Die Wahl dieses Datums für einen offiziellen Besuch ist ein politisches Statement.[122]

- Der Etat des Bundesamtes für Verfassungsschutz wurde um 21 Mio. Euro auf 231 Mio. Euro erhöht.[123]

Aktive Rolle bei neuen Überwachungsgesetzen

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

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

Die Vorratsdatenspeicherung brachte 2009 so gut wie keine Verbesserungen bei der Aufklärung von Straftaten im Internet. Trotzdem forciert der Verfassungsschutz im Hintergrund weiterhin die Einführung der VDS (neudeutsch: Mindestspeicherfrist). Nachdem die VDS schon 2002 als nicht vereinbar mit der Verfassung vom Bundestag abgelehnt wurde und auf EU-Ebene offenbar nicht durchsetzbar ist, beteiligte sich der Verfassungschutz 2012 aktiv an der Formulierung einer internationalen Richtline zur verpflichtenden Vorratsdatenspeicherung im Rahmen der UNODC, die allerdings ebenfalls nicht verbindlich umgesetzt wurde.[124].

[118] http://www.berliner-zeitung.de/nsu-prozess/nsu-prozess-wichtiger-zeuge-im-auto-verbrannt,11151296,24474928.html
[119] http://www.stuttgarter-zeitung.de/inhalt.nsu-untersuchungsausschuss-vorwuerfe-nach-ominoeser-selbsttoetung.a05cce3a-60a5-4d68-9b24-7a6693123002.html
[120] http://www.sueddeutsche.de/politik/nsu-prozess-tod-von-v-mann-corelli-wirft-fragen-auf-1.1940178
[121] http://www.taz.de/Verfassungsschutz-und-NSU/!150371/
[122] https://www.heise.de/tp/news/Der-NSU-und-der-Verfassungsschutz-Dinge-von-gestern-2440935.html
[123] https://www.bundestag.de/dokumente/textarchiv/2014/kw48_ak_inneres/341274
[124] https://netzpolitik.org/2012/uno-bericht-der-kampf-gegen-terroristen-beginnt-im-internet-mit-vorratsdatenspeicherung-und-identifizierungspflicht/

Zukünftige Schwerpunkte des Geheimdienstes

Das Bundesamt für Verfassungsschutz soll in den kommenden Jahren zu einer kleinen Mini-NSA werden. Die Kompetenzen und Fähigkeiten zur Überwachung im Internet soll massiv ausgebaut werden, wie Netzpolitik.org[125] anhand vertraulicher Unterlagen berichtete. Die neu zu schaffende Abteilung *Erweiterte Fachunterstützung Internet* (EFI, 75 neue Mitarbeiter) soll Soziale Netzwerke, Foren u.ä. automatisiert überwachen und dabei überwiegend unterhalb der Schwelle des G10-Gesetzes agieren, also ohne parlamentariche Kontrolle durch die G10-Kommision. Neue Analysemethoden sollen geschaffen werden, um anhand von Metadaten bessere Bewegungs- und Kommunikationsprofile zu erstellen.

Der Abgeordnete C. Ströbele bezeichnte die Aufgabenstellung für die Abteilung EFI als illegal und nicht mit der Verfassung vereinbar.[126]

Der ehemalige Geheimdienstkontrolleur Wolfgang N. forderte ein Sonderstrafrecht für Geheimdienstmitarbeiter. Er fordert, dass Geheimdienstmitarbeiter sich strafbar machen, wenn sie parlamentarische Kontrollgremien belügen und eine Kontrolle der Dienste behindern. Anderenfalls wird es so weitergehen wie bisher, dass BND und Verfassungsschutz das Gesetz brechen können ohne Konsequenzen zu fürchten.

Überwachung politischer Aktivisten

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

- R. Gössler: 38 Jahre zu Unrecht vom Verfassungschutz überwacht [127]
- Verfassungsschutz in Bayern überwacht die linke Szene [128]
- Überwachung einer linken Gruppe durch Verfassungsschutz [129]
- Verfassungsschutz bespitzelt linke Abgeordnete [130]
- Gegner von Stuttgart21 vom Verfassungsschutz überwacht [131]
- Kultur- und Jugendprojekt Conne Island vom BfV überwacht [132]
- mg-Überwachung durch den Verfassungsschutz war illegal [133]
- Ohne demokratische Kontrolle (BfV in Bayern) [134]

2.12 Ich habe doch nichts zu verbergen

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

[125] https://netzpolitik.org/2015/geheime-referatsgruppe-wir-praesentieren-die-neue-verfassungsschutz-einheit-zum-ausbau-der-internet-ueberwachung/
[126] http://www.stroebele-online.de/bundestag/anfragen/8305504.html
[127] https://heise.de/-217246
[128] https://www.heise.de/tp/artikel/35/35942/1.html
[129] https://www.heise.de/tp/blogs/8/151499
[130] https://www.heise.de/tp/artikel/36/36316/1.html
[131] http://www.bei-abriss-aufstand.de/2012/02/25/
[132] http://www.bei-abriss-aufstand.de/2012/02/25/
[133] http://www.l-iz.de/Politik/Sachsen/2014/05/Verfassungsschutz-raeumt-Bespitzelung-von-Conne-ein-55195.html
[134] https://www.heise.de/tp/artikel/35/35942/1.html

Erkennung einer neuen Liebesbeziehung

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

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

Arbeitslos?

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

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

Unzufrieden mit dem Job?

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

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

Kein Studienplatz?

In Großbritannien werden Studienbewerber für bestimmte Fachrichtung geheimdienstlich überprüft. 739 Bewerber wurde bereits abgelehnt, weil aufgrund dubioser Datensammlungen der Geheimdienste befürchtet wurde, dass die Bewerber zu Terroristen werden und die im Studium erworbenen Kenntnisse zur Herstellung von Massenvernichtungswaffen nutzen könnten. Die geheimdienstlichen Gesinnungs-Prüfungen sollen zukünftig ausgeweitet werden.[135]

Einzelbeispiele

- Emma L. hatte sich auf dem Dating-Portal OkCupid zu einem Treffen verabredet. Das Date war ein Reinfall (kommt manchmal vor). Wenig später wurde ihr der Dating-Partner von Facebook als Freund empfohlen, in der *People You May Know*

[135] https://www.heise.de/tp/artikel/44/44538/1.html

Section. Maria L. wurden ihre Tinder-Dates von Facebook als Freunde empfohlen. Es gibt auf Twitter noch viele weitere Beispiele für diese seltsamen Facebook Empfehlungen.[136]

Weder OkCupid nich Tinder geben Daten an Facebook weiter. Die Empfehlungen für Freunde werden anhand der Geolocation (*zur gleichen Zeit am gleichen Ort*) und aufgrund ähnlicher Interessen (*Dating-Webseite besucht*) ermittelt. Daraus könnten sich auch unangenehme Folgen ergeben, wie Netzpolitik.org an Beispielen zeigt.[137]

- Target ist einer der größte Discounter in den USA. Eines Tages stürmte ein wütender Vater in eine Filiale und beschwert sich, dass seine minderjährige Tochter Rabattmarken für Babysachen erhalten hat. Später musste der Vater kleinlaut zugegeben, dass seine Tochter wirklich schwanger war, er selbst aber nichts davon wusste. Target hatte die Schwangerschaft der minderjährigen Tochter an den kleinen Änderungen im Kaufverhalten erkannt.[138]

- Im Rahmen der Zulässigkeitsprüfung für Piloten wurde Herr J. Schreiber mit den vom Verfassungsschutz gesammelten Fakten konfrontiert [139]:

  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 zu einer Stellungnahme jedoch nicht eingeräumt. Es werden Entscheidungen getroffen und wir haben keine Ahnung, welche Daten dabei eine Rolle spielten.

- Ein junger Mann meldet sich freiwillig zur Bundeswehr. Mit sechs Jahren war er kurzzeitig in therapheutischer 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. [140].

- Kollateralschäden: Ein großer deutscher Provider liefert falsche Kommunikationsdaten ans BKA. Der zu Unrecht Beschuldigte erlebt das volle Programm: Hausdurchsuchung, Beschlagnahme der Rechner, Verhöre und sicher nicht sehr lustige Gespräche im Familienkreis. Die persönlichen und wirtschaftlichen Folgen sind schwer zu beziffern [141].

  Noch krasser ist das Ergebnis der *Operation Ore* in Großbritannien. Einige Tausend Personen wurden wegen Konsums von Kinderpornografie angeklagt. Acht Jahre später stellte sich heraus, dass die meisten Betroffen zu unrecht verurteilt wurden, weil sie Opfer von Kreditkarten Betrug waren. 39 Menschen hatten Selbstmord begangen, da ihnen alles genommen wurde. [142].

[136] https://twitter.com/search?q=facebook%20suggest%20tinder
[137] https://netzpolitik.org/2016/facebook-nutzt-standort-fuer-freundesvorschlaege/
[138] http://www.tagebau.com/?p=197
[139] http://www.pilotundflugzeug.de/artikel/2006-02-10/Spitzelstaat
[140] https://blog.kairaven.de/archives/998-Datenstigmaanekdote.html
[141] https://www.lawblog.de/index.php/archives/2008/03/11/
[142] https://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 Webseite des BKA zur Gruppe "mg" ist ein Honeypot, der dazu diente, weitere Sympathisanten zu identifizieren. Die Bundesanwaltschaft verteidigt die Maßnahme als legale Fahndungsmethode.

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

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

Politische Aktivisten

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

1. Erich Schmidt-Eenboom 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"* [143] gibt es bei SPON.

2. Fahndung zur Abschreckung: In Vorbereitung des G8-Gipfels in Heiligendamm veranstaltete die Polizei am 9. Mai 2007 eine Großrazzia. Dabei wurden bei Globalisierungsgegnern Rechner, Server und Materialien beschlagnahmt. Die Infrastruktur zur Organisation der Proteste wurde nachhaltig geschädigt. Wenige Tage nach der Aktion wurde ein Peilsender des BKA am Auto eines Protestlers gefunden. Um die präventiven Maßnahmen zu rechtfertigen, wurden die Protestler als terroristische Vereinigung eingestuft. Das Netzwerk Attac konnte 1,5 Jahre später vor Gericht erreichen, dass diese Einstufung unrechtmäßig war. Das Ziel, die Organisation der Proteste zu behindern, wurde jedoch erreicht.

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

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

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

Kapitel 3

Digitales Aikido

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

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

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

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

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

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

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

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

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

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

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

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

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

3.1 Nachdenken

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

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

Im Internet verwendet diese Person verschiedene Online-Identitäten:

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

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

- Das Facebook Profil enthält umfangreiche Daten: Fotos, Freundeskreis...
- Bei der Nutzung von vielen Webdiensten fallen kleine Datenkrümel an. Auch E-Mails werden von den Datensammlern ausgewertet. Die IP-Adresse des Absenders im Header der E-Mails kann mit anderen Einträgen von Cookies oder User-Tracking-Systemen zeitlich korreliert werden und so können den Surf-Profilen die Mail-Adressen und reale Namen zugeordnet werden.
- Von dem anonymen E-Mail Postfach findet man Daten bei den Empfängern der E-Mails. (Google has most of my emails because it has all of yours.) Auch diese Datenpakete enthalten einen Zeitstempel sowie oft die IP-Adresse des Absenders. Durch zeitliche Korrelation kann das anonymen E-Mail Postfach mit dem Real-Name Postfach und dem Surf-Profil verknüpft werden.

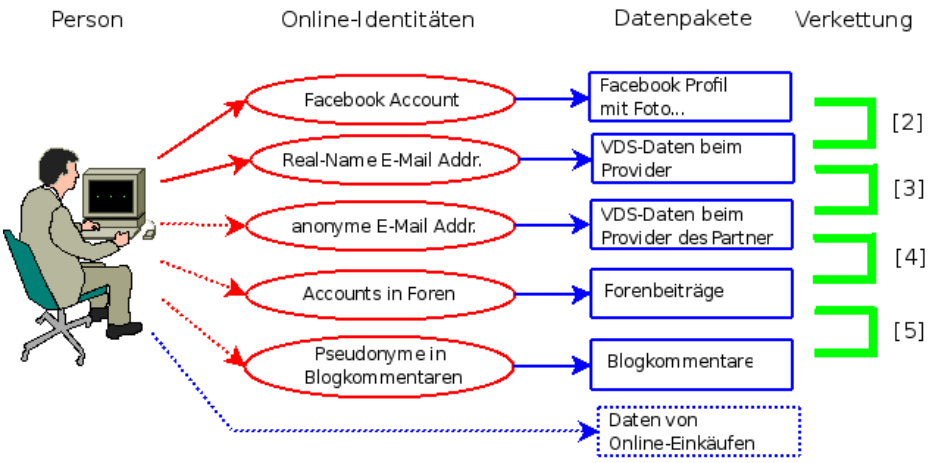


Abbildung 3.1: Datenverkettung

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

Verkettung der Informationen und Datenpäckchen

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

1. Online Communities wie Facebook bieten viele Möglichkeiten. Neben der Auswertung von Freundschaftsbeziehungen gibt es auch viele Fotos. Dieser Datenpool ist schon sehr umfangreich:
   - Wirtschaftswissenschaftler haben eine Methode vorgestellt, um Meinungsmacher und kreative Köpfe in Online-Communities zu identifizieren [1].
   - MIT-Studenten erkennen homosexuelle Neigungen ihrer Kommilitonen anhand der Informationen über Freundschaften in den Facebook-Profilen [2].
   - Der Grünen-Vorsitzende Özdemir pflegte eine Freundschaft mit dem Intensivstraftäter Muhlis Ari, ist in seinem Facebook Profil erkennbar [3].
2. Dem Facebook Profil kann man durch Kombination mit anderen Datenkrümeln den realen Namen und die meisten genutzten E-Mail Adressen zuordnen. Die Firma Rapleaf ist z. B. darauf spezialisiert. Auch pseudonyme Facebook Accounts können 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.

[1] https://www.heise.de/tp/r4/artikel/31/31691/1.html
[2] https://www.heise.de/tp/r4/artikel/31/31181/1.html
[3] https://www.heise.de/tp/r4/artikel/32/32138/1.html

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

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

   - Die Bücher der Anderen (500.000 Rechnungen online einsehbar [4])
   - Die Libris Shops (Zugang zu Bestellungen von 1000 Buchshops [5])
   - Sparkassen-Shops (350.000 Rechnung online einsehbar [6])
   - Acht Mio. Adressen von Quelle-Kunden sollen verkauft werden [7]

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

Durch die Verkettung der Datenpäckchen konnten in dem fiktiven Beispiel alle Online Identitäten de-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 vielerlei Hinsicht beeinflussen, ohne dass dem Betroffenen klar wird, dass hinter scheinbar zufälligen Ereignissen ohne Zusammenhang bewusste Entscheidungen stehen.

- Die Datensammlungen werden mit kommerziellen Zielen ausgewertet, um uns zu manipulieren und Kaufentscheidungen zu beeinflussen.

- Personalabteilungen rastern routinemäßig das Internet nach Informationen über Bewerber. Dabei ist Google nur ein erster Ansatzpunkt. Bessere Ergebnisse liefern Personensuchmaschinen und soziale Netzwerke. Ein kurzer Auszug aus einem realen Bewerbungsgespräch:

  – Personalchef: *Es stört Sie sicher nicht, dass hier geraucht wird. Sie rauchen ja ebenfalls.*
  – Bewerber: *Woher wissen Sie das?*
  – Personalchef: *Die Fotos in ihrem Facebook-Profil ...*

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

- Von der israelischen Armee ist bekannt, dass sie die Profile in sozialen Netzen überprüfen, wenn Frauen den Wehrdienst aus religiösen Gründen verweigern. Zur Zeit verweigern in Israel 35% der Frauen den Wehrdienst. Anhand der sozialen Netze wird der Lebenswandel dieser Frauen überprüft. Es werden Urlaubsfotos in freizügiger Bekleidung gesucht oder Anhaltspunkte für Essen in einem nicht-koscheren Restaurant. Auch aktiv wird dabei gehandelt und Fake-Einladungen zu einer Party während des Sabbats verschickt.

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

[4] https://www.netzpolitik.org/2009/exklusiv-die-buecher-der-anderen
[5] https://www.netzpolitik.org/2009/exklusiv-die-libri-shops-der-anderen
[6] https://www.netzpolitik.org/2009/zugriff-auf-350-000-rechnungen-im-sparkasse-shop
[7] https://www.zeit.de/digital/datenschutz/2009-11/quelle-kundendaten-verkauf

- Identitätsdiebstahl ist ein stark wachsendes Delikt. Kriminelle 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 [8].
- Mit dem Projekt INDECT hat die EU ein Forschungsprojekt gestartet und mit 14,8 Mio Euro ausgestattet, um unsere Daten-Spuren für Geheimdienste zu erschließen.[9]

Ich habe doch nichts zu verbergen...

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

3.2 Ein Beispiel

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

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

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

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

goagirl17@ymail.com

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

flaudi85

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

- g.....17 ist offenbar depressiv. Das verordnete Medikament deutet auf Angstzustände hin, wurde von der Patientin nicht genommen sondern ins Klo geworfen.
- Sie hat Probleme im Studium und will sich krankschreiben lassen, um an Prüfungen nicht teilnehmen zu müssen.
- Außerdem hat sie ein massives Alkoholproblem und beteiligt sich am *Syncron-Saufen* im Internet. Scheinbar ist sie auch vereinsamt.
- F. ist offenbar lesbisch, sie sucht nach einer Frau bei abgefuckt.de.

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

- F. ist im linksradikalen Spektrum aktiv. Sie hat an mehreren Demonstrationen teilgenommen und berichtet über Erfahrungen mit Hausdurchsuchungen. Möglicherweise ist das die Ursache für ihre Angstzustände.
- Öffentlich prangert sie in einem Diskussionsforum die Firma ihres Vaters an (wegen Ausspionierens von Mitarbeitern).
- Ihre linksgerichtete Grundhaltung wird durch öffentliche Unterstützung der Kampagne *Laut ficken gegen Rechts* unterstrichen.
- Von regelmäßiger Arbeit hält sie nicht viel.
- Die 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 Wunschliste bei Amazon und Fotos bei Flickr...

Würden sie als Personalchef diese fiktive Person einstellen?

Welche Ansatzpunkte ergäben sich für den Verfassungsschutz?

Was könnte zukünftig für die Krankenkasse interessant sein?

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

3.3 Schattenseiten der Anonymität

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

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

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

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

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

Ein anonymer Schwarm vereinzelter Individuen kann sich zu einem Shitstorm zusammenfinden. Der Schwarm kann kurzzeitig viel Lärm produzieren ohne gesellschaftlichen

Diskurs und wird dann wieder zerfallen. Er wird kein *Wir!* entwickeln und kann keine gemeinsamen Ziele verfolgen, die über einen kurzzeitigen Hype in den Medien hinaus gehen. Außerdem lassen sich Empörungswellen durch eine kritische Masse anonymer Sockenpuppen leicht manipulieren.

Ein Beispiel für den Konflikt zwischen Anonymität und Vertrauen:

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

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

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

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

3.4 Wirkungsvoller Einsatz von Kryptografie

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

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

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

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

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

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

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

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

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

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

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

   Alternativ könnte man sich den öffentlichen Schlüssel von vertrauenswürdigen Dritten beglaubigen lassen. (Wenn man einen vertrauenswürdigen(!) Dritten findet, der die Identität der Inhaber der kryptografischen Schlüssel wirklich geprüft hat.)

   - OpenPGP bietet dafür das *Web of Trust*, dass die meisten Nutzer nicht ganz verstanden haben und das in der Praxis kaum eine Rolle spielt.
   - Für X509v3 Zertifikate, wie sie beim SSL/TLS Protokoll, bei VPNs oder bei S/MIME verwendet werden, gibt es das Konzept der Certification Authorities (CAs) als *vertrauenswürdigen Dritten*, der Echtheit der Schlüssel bestätigt. Für einen begrenzten Personenkreis kann man eine eigene CA aufsetzen, wenn man die Kompetenz und das Vertrauen der beiteligten Personen genießt.

     Public CAs definieren sich selbst als vertrauenswürdig und sind der Meinung, eine unverschlüsselte E-Mail ist ein ausreichend sicherer Kanal für die Verifikation einer Identität. Die laut Eigenwerbung größte CA ist Verisign. Seit 2002 ist bekannt, dass Verisign auch ein Global Player bei der Überwachungstechnik ist. Die Firma bietet Support für *Lawful SSL Interception*. Das ist nicht sehr vertrauenswürdig, wenn man sich gegen staatliche Überwachung schützen will.

Mit DANE/TLSA gibt es einen Ansatz, die SSL-Zertifikate auf einem kryptografisch gesicherten, unabhängigen Weg zu verifizieren. Leider verbreitet es sich nur langsam und wird von den meisten Programmen (noch?) nicht unterstützt.

Kapitel 4

Spurenarm Surfen

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

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

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

Schutz gegen Tracking erreicht man durch mehrere Maßnahmen:

- Datensammelnden Dienste kan man meiden und Trackingelemente wie Werbebanner, anti-soziale Like-Buttons, JavaScript Trackingcode oder HTML-Wanzen werden blockiert.
- Langfristige Markierungen für das Tracking (Cookies, EverCookies) werden gelöscht oder eingesperrt.
- Features deaktivieren, die sich für Browserfingerprinting eignen.
- ...

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

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

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

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

- Wichtigste Punkt sind regelmäßige Updates von Browser und OS.
- Überflüssige Features deaktivieren, um die Angriffsfläche gering zu halten.

- Man kann den Browser gegen Angriffe härten (z. B. mit *apparmor*).
- Virtualisierung der Surfumgebung kann die lokalen Daten gegen erfolgreich kompromittierte Browser schützen.
- ...

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

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

4.1 Auswahl des Webbrowsers

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

Die *Extented Support Releases*[3] (ESR-Versionen) von Firefox werden im Gegensatz zu den 6-wöchigen Updates des Firefox für ca. ein Jahr gepflegt. Es werden keine neuen Features eingebaut, was sich positiv auf die Stabilität auswirkt. Allerdings fehlen damit auch aktuelle Verbesserungen in der SSL/TLS Verschlüsselung und ähnliche Updates, die u.U. positiv für die Sicherheit sind.

Schnellkonfiguration für einen privacy-freundlichen Firefox

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

Empfehlung für **Firefox 78+**:

- Das Add-on **uBlock Origin** ist ein effizienter und einfach installierbarer Werbe- und Trackingblocker. Eine empfohlene Konfiguration von uBlock Origin steht steht auf www.privacy-handbuch.de/handbuch_21d2.htm zum Download bereit.
- Das Add-on **CanvasBlocker** kann Zugriffe auf Canvas-API, Screen-API und Audio-API faken (geringfügig modifizieren) um ein Fingerprinting des Browsers zu verhindern. Als Einstellungen sind die vorbereiteten *Stealth Settings* empfehlenswert.
- Das Add-on **Skip Redirect** entfernt Umleitungen in der URL. Diese Umleitungen werden häufig genutzt, um die Klicks auf Links zu externen Domains zu tracken. Hinweis: Für WiFi Hotspot Logins muss man das Add-on deaktivieren.
- Das Add-on **Neat URL** entfernt bekannnte Tracking Parameter von Google Analytics, Facebook, Youtube und anderen Trackern aus der URL.

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

- Mit **NoScript** kann man Freigaben für JavaScript und anderen Content verwalten. Außerdem implementiert es einen Schutz gegen XSS-Angriffe. Die Standardkonfiguration von NoScript ist suboptimal, kann man anpassen.
- Außerdem sind weiteren Einstellungen in der Konfiguration privacy-freundlich zu setzen. Um die Werte nicht alle einzeln und umständliche setzen zu müssen, kann man die strenge *user.js* oder die moderate *user.js* Konfigurationsdatei von unserer Webseite https://www.privacy-handbuch.de/handbuch_21u.htm herunterladen und im Browserprofil speichern. Beim Start überschreiben die Werte der *user.js* die Preferenzen.

Um die Installation von privacy-freundlichen **Suchmaschinen** zu vereinfachen, haben wir einige Such-Plugins vorbereitet. Wenn man auf die Webseite https://www.privacy-handbuch.de/handbuch_21browser.htm aufruft, kann man im Suchfeld oben rechts in der Firefox Toolbar ein paar Buchstaben tippen und in dem ausklappenden Menü die gewünschte Suchmaschine hinzufügen.

4.2 Datensparsame Suchmaschinen

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

Für alle alternativen Suchmaschinen gilt, dass sie eine andere Sicht auf das Web bieten und die Ergebnisse sich von Google unterscheiden. Man sollte bei der Beurteilung der Ergebnisse beachten, dass auch Google nicht die reine Wahrheit bieten kann, sondern nur eine bestimmte Sicht auf das Web.

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

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

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

Meta-Suchmaschinen leiten die Suchanfrage an eine oder mehrere Suchmaschinen weiter. Sie sammeln die Ergebnisse ein und sortieren sie neu. Außerdem schützen sie die Privatsphäre der Nutzer, indem sie die Indentität der Nutzer gegenüber den angefragten Suchmaschinen verbergen, da sie als Proxy agieren.

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

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

> *verhindern, werden einige nicht-identifizierende Systeminformationen gemeinsam genutzt.*

Als kleines Schmankerl bietet Startpage.com die Möglichkeit, aus den Suchergebnissen die Webseiten über einen anonymisierenden Proxy aufzurufen. Die aufgerufene Webseite sieht damit nur eine IP-Adresse eines Proxy. Neben den Ergebnissen findet man den Link *Anonym öffnen*.

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

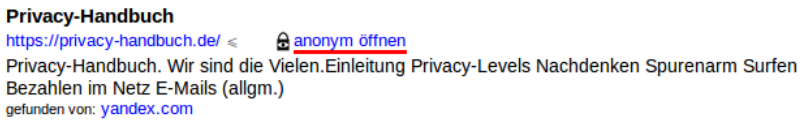
> *Es wurden keine mit Ihrer Suchanfrage übereinstimmenden Dokumente gefunden.*

Das Mycroft Project bietet ein Such-Plugin mit ungefilterten Suchergebnissen, das auch Ergebnisse für die Suche nach *Dildos* anzeigt. In den Einstellungen kann man den Filter auch deaktivieren.

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

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

Metager bietet wie Startpage einen Proxy, um Ergebnisse aus der Suchliste anonym aufzurufen. Die Server stehen in Deutschland.



Meta-Suchmaschinen schützen die Privatsphäre ein bisschen. Sie entfernen eindeutig identifizierende Informationen aus den Daten aber leiten trotzdem einige Daten an Datensammler weiter, teilweise um die großen Platzhirsche abfragen zu können. Diese Daten könnten unter Umständen ausreichen, um den Surfer wiederzuerkennen und evtl. Suchanfragen mit einer konkreten Person zu verknüpfen. Außerdem sind Google & Co. generell an allen Suchanfragen interessiert, um ihre Macht auszubauen, auch wenn sie keinem Nutzer zugeordnet werden können. Deshalb sind privacy-freundliche Suchmaschinen mit eigenem Index empfehlenswerter, als die Nutzung einer Meta-Suche.

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[4] oder DeepL[5] nutzen. Die Translator kennen neben Englisch und Deutsch weitere Sprachen.

Peer-2-Peer Suchmaschine

Yacy [6] 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

[4] https://dict.leo.org
[5] https://www.deepl.com/translator
[6] http://yacy.net

in Java geschrieben, benötigt also eine Java-Runtime (JRE), die es für WINDOWS bei Oracle [7] zum kostenlosen Download gibt. Linuxer können das Paket *default-jre* mit der Softwareverwaltung installieren. Danach holt man sich die Yacy-Software von der Website des Projektes und startet den Installer - fertig. Für Debian, Ubuntu und Linux Mint bietet das Projekt ein Repository [8] mit fertigen Paketen.

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

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

Google ???

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

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

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

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

wird im Moment des Klick eine Google-URL:

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

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

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

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

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

[7] https://java.com/de
[8] https://wiki.yacy.net/index.php/De:DebianInstall

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

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

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

Firefox konfigurieren

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

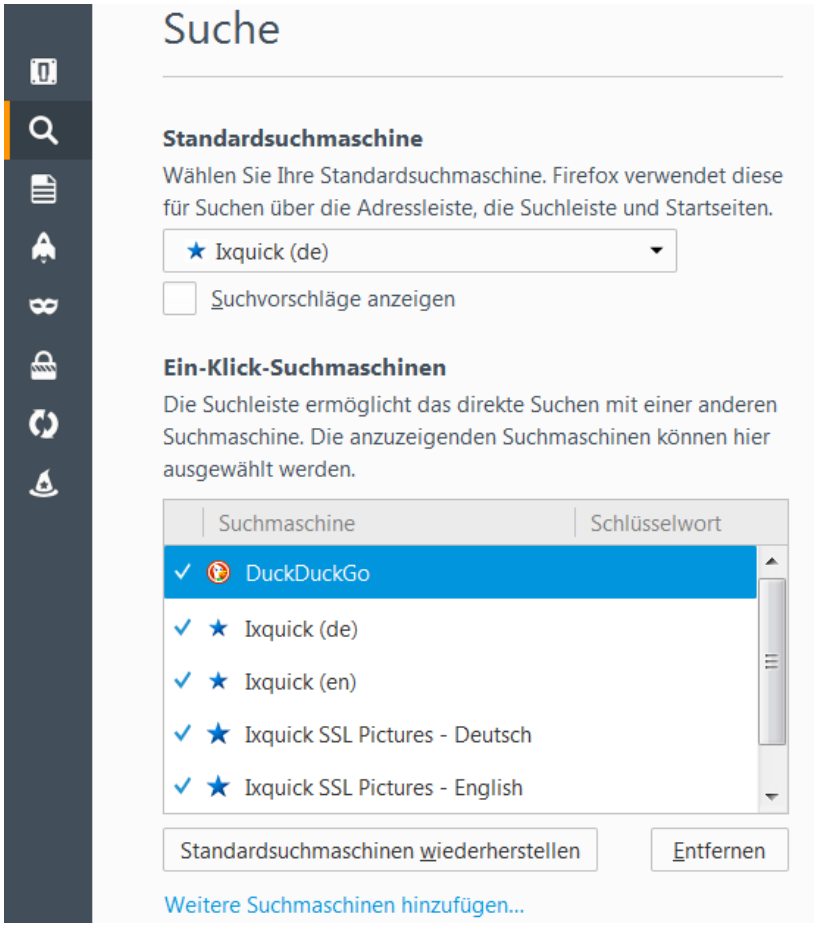


Abbildung 4.1: Suchmaschinen verwalten

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

tory nutzt, wird bei jeder Suchanfrage irgendwie ein Hinweis auf Ubuntu angehängt:

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

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

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

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

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

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

Diese Parameter in der Suchanfrage können einen User-Agent Fake entlarven. Die standardmäßig installierten Suchmaschinen sollte man deaktivieren und statt dessen privacy-freundlichere Plug-ins von mycroft.mozdev.org installieren.[9] zu installieren. In einem Suchformular auf der Webseite gibt man den Namen der Suchmaschine ein und findet schnell ein umfangreiche Liste von Varianten. Für viele Suchmaschinen wie DuckDuckGo, Ixquick, Google, Wikipeadia, Startpage u.a.m. gibt es eine lokalisierte Variante (DE) mit SSL-Verschlüsselung und evtl. ohne Javascript. Diese Variante sollte bevorzugt werden. Ein Klick in der Liste der Ergebnisse installiert das Plug-in (JavaScript freigeben).

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

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

URL-Leiste mit extra Suchfeld

Firefox hat vom Chrome Browser das URL-Eingabefeld mit integrierter Suchfunktion übernommen. Zu diese Idee kann man geteilter Meinung sein. Manchmal ist es besser, wenn man getrennte Eingabefelder für URLs und Suche verwendet, um einen klaren Kopf zu behalten und nicht von der Vorschlägen der KI abgelenkt oder unterschwellig manipuliert zu werden. Die Anzeige des extra Suchfeldes kann man in den Einstellungen aktivieren.

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

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

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

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

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

```
browser.urlbar.oneOffSearches = false
```

[9] https://mycroft.mozdev.org/

GeoIP-spezifische Standardsuchmaschine deaktivieren

Mozilla bekommt nicht nur von Google Geld, damit die Google-Suche als Default genutzt wird, sondern auch von Yahoo. Der Deal war, das US-amerikanischen Nutzer stnadard-mäßig mit Yahoo suchen sollen und alle anderen mit Google.

Um festzstellen, ob es sich um einen US-amerikanischen Nutzer handelt, kontaktiert den Firefox beim Start den Server *location.services.mozilla.com*, um anhand der IP-Adresse entscheiden zu können, welche Suchmaschine genutzt werden soll. Dabei werden neben der Firefox Version auch die Lokalisierung, der Update Kanal und die Distribution übertragen. Um diese überflüssige Verbindungsaufnahme zu unterbinden, kann man unter der Adresse *about:config* folgende Variablen setzen:

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

4.3 Cookies

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

Der Screenshot Bild 4.2 zeigt die Liste der Cookies, die bei einem einmaligen Aufruf der Seite *www.spiegel.de* gesetzt wurden. Es ist nicht ungewöhnlich, dass populäre Webseiten mehrere Datensammler einbinden. Eine Studie der Universität Berkeley [10] hat 2011 beim Surfen auf den Alexa TOP100 Webseiten 5.675 Cookies gefunden (ohne Login oder Bestellung). 4.914 Cookies wurden von Dritten gesetzt, also nicht von der aufgerufenen Webseite. Die Daten wurden an mehr als 600 Server übermittelt. Spitzenreiter unter den Datensammlern ist Google. 97% der populären Webseiten setzen Google-Cookies.

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

- Eine empirische Studie der Universität Leuven von 2014 zeigte, dass bereits damals 44 Trackingdienste mehr als 40% des Surfverhaltens mit Hilfe von First-Party Cookies verfolgen konnten, auch wenn die Cookies für Drittseiten blockiert wurden.[11]
- Ein Beispiel ist der Trackingdienst WebTrekk, der sich auf Webseiten wie *heise.de*, *zeit.de* oder *zalando.de* mit DNS-Aliases als Subdomain der überwachten Webseite First-Party Status erschleicht, um seine Tracking Cookies zu setzen (2013).[12]
- Google kombiniert seit 2017 den Dienst Analytics mit dem AdWords Tracking. Für Google Analytics bindet der Webmaster Trackingcode direkt auf der Webseite ein, der damit First-Party Status erhält und die Cookies für das AdWords Tracking setzt.[13]
- Microsofts folgte im Januar 2018 und hat eine Lösung umgesetzt, die das Cookie mit der Microsoft Click ID für das Conversation Tracking im First-Party Context setzt. Die Microsoft Tracking ID wird als URL-Parameter übertragen und dann von einem JavaScriptchen in ein Cookie geschrieben.[14]
- Facebook folgte den Beispiel von Google und Microsoft im Herbst 2018, nachdem Mozilla angekündigt hat, nach dem Vorbild von Safari das Tracking via Third-Party Cookies in Firefox zu erschweren. Wie bei Microsoft wird die Tracking ID in einem

[10] http://heise.de/-1288914
[11] https://securehomes.esat.kuleuven.be/ gacar/persistent/the_web_never_forgets.pdf
[12] https://anonymous-proxy-servers.net/blog/index.php?/archives/377-Tracking-mit-Cookies.html
[13] https://www.heise.de/-3859526
[14] https://advertise.bingads.microsoft.com/en-us/blog/post/january-2018/conversation-tracking-update-on-bing-ads

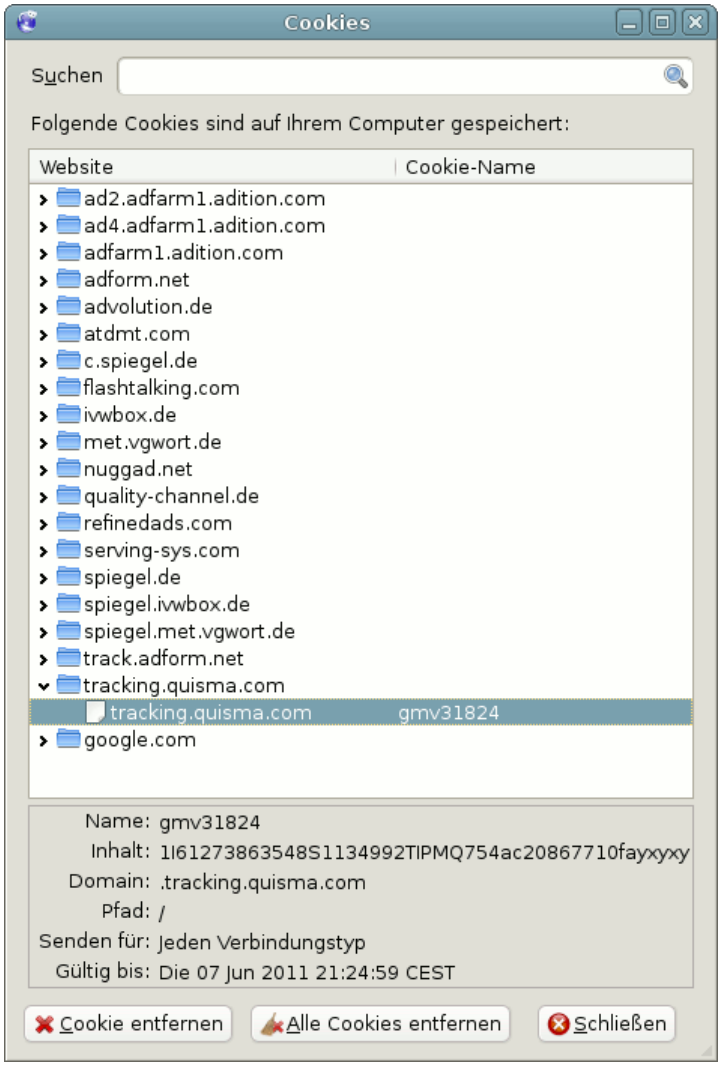


Abbildung 4.2: Liste der Cookies beim Besuch von Spiegel-Online

URL-Parameter übertragen und dann mit JavaScript in ein First-Party Cookie geschrieben.[15]

Die Tracking-Cookies werden auch von der NSA und GCHQ im Rahmen der globalen Überwachung genutzt. Die Geheimdienste beobachten den Datenstrom im Internet und identifizieren Surfer anhand langlebiger Cookies der Trackingdienste. Zielpersonen werden anhand dieser Cookies verfolgt und bei Bedarf mit *Foxit Acid* gezielt angegriffen, wenn die Identifikation für mindestens 2 Wochen stabil möglich ist.[16]

Konzepte zur Verwaltung von Cookies

Es gibt mehrere Ansätze, um Cookies zu verwalten um sich gegen Tracking zu schützen:

Whitelisting: Firefox enthält alles notwendige, um ein Whitelisting für Cookies zu konfigurieren. Diese Einstellungen gelten auch für den DOMStorage und IndexedDB.

1. Standardmäßig wird die Annahme von Cookies und die Speicherung von Daten im HTML5 DOMStorage verweigert.
2. Für vertrauenswürdige Websites, welche die Nutzung von Cookies zur Anmeldung benötigen, werden Ausnahmen definiert.
3. Alle Cookies werden beim Schließen des Browsers gelöscht.

Mit folgender Variable unter *about:config* aktiviert man dieses Verhalten:

```
network.cookie.cookieBehavior = 2
```

First-Party Cookies erlauben: Etwas moderater und weniger nervend beim Surfen ist die Einstellung, Cookies und die Speicherung im HTML5 DOMStorage nur für die aufgerufene Webseite (First Party) zu erlauben.

Mit dieser Einstellung erspart sich die (umständliche) Konfiguration von Freigaben für einzelnen Webseiten, bei den man sich Anmelden möchte. Gleichzeitig schützt diese Variante aber nur unzureichend gegen Tracking, da viele Trackingdienste Techniken entwickelt haben, um das Surfverhaltens mit First-Party Cookies zu verfolgen.

Mit folgender Variable unter *about:config* aktiviert man dieses Verhalten:

```
network.cookie.cookieBehavior = 1
```

Cookies beim Beenden löschen: Es gibt drei Möglichkeiten, die Cookies beim Beenden von Firefox zu löschen, um langfristiges Tracking zu verhindern:

1. Alle Cookies könnten in Session Cookies umgewandelt werden (indem das *Expire Date* entfernt wird). Session Cookies verschwinden beim Beenden von Firefox:

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

2. Nur die Cookies von Drittseiten können in Session Cookies umgewandelt werden, während First-Party Cookies gemäß Lifetime erhalten bleiben:

   ```
   network.cookie.thirdparty.sessionOnly = true
   ```

3. Die Cookies und andere gespeicherte Daten können durch das Löschen der History beim Beenden vom Firefox entfernt werden:

   ```
   privacy.history.custom              = true
   privacy.sanitize.sanitizeOnShutdown = true
   privacy.clearOnShutdown.cookies     = true
   ```

[15] https://marketingland.com/facebook-to-release-first-party-pixel-for-ads-web-analytics-from-browsers-like-safari-249478

[16] https://www.eff.org/deeplinks/2013/12/nsa-turns-cookies-and-more-surveillance-beacons

Die beiden ersten Methoden können unter Umständen durch Trackingdienste erkannt und als individuelle Besonderheiten für das Fingerprinting des Browser verwendet werden. Die dritte Methode ist während des Surfens nicht detektierbar.

Surf-Container verwenden: Surf-Container sind ein Konzept, um Website-übergreifendes Tracking mit Cookies und EverCookies zu verhindern. Sie bieten einen guten Schutz gegen Tracking mit Cookies und EverCookies bei minimaler Beeinträchtigung.

Tracking Cookies blockieren: Firefox bietet die Möglichkeit, bekannte Cookies und EverCookies von Trackingdiensten und Social Media Sites zu blockieren. Dieses Einstellung ist der Standardwert unter Firefox:

```
network.cookie.cookieBehavior = 4
```

Der Schutz durch die Firefox Filter ist allerdings etwas durchlässig und keinen einen Trackingblocker wie das Add-on *uBlock Origin* nicht ersetzen. Es wird beispielsweise das IDE Cookie von Doubleclick nicht blockiert, das wichtigste Trackingcookie von Google (laut Dokumentation), was möglicherweise politische Gründe hat, da Google der Haupsponsor von Mozilla ist. Aber auch bei den Cookies anderer Trackingdienste arbeitet der Filter etwas oberflächlich.

Firefox 79+ kann außerdem Redirect Tracking erkennen und diese Trackingmarkierungen löschen. Beim Redirect Tracking wird der Surfer bei Klick auf einen Link nicht direkt von der Webseite A zur Webseite geleitet (A -> B) sondern von der Webseite A zur Zwischenstation T geschickt, die den Besucher mit Trackingelementen im First-Party Context markiert und dann automatisch zur gewünschten Webseite B weiterleitet (A -> T -> B). Der Redirect wird vom Surfer in der Regel kaum bemerkt. Der Schutz gegen Redirect Tracking wird mit folgendem Parameter aktiviert:

```
privacy.purge_trackers.enabled = true
```

Cookie-Management mit Add-ons: Zusätzliche Add-ons wie *CookieAutoDelete* tun in der Regel das, was der Name vermuten lässt. Sie löschen alle Cookies automatisch, die nicht mehr gebraucht werden.

Das automatische Löschen von irgendwelchen Cookies ist ganz nett, schützt aber nicht gegen Tracking. Viele Trackingdienste verwenden inzwischen EverCookies, um gelöschte Tracking Cookies wiederherzustellen. Diese Add-ons erfüllen zwar ihre Aufgabe, sind aber hinsichtlich Trackingschutz überwiegend wirkungslos.

Empfehlung zum Cookie Management für Firefox 78+

1. Das Webseiten-übergreifende Tracking mit Cookies und EverCookies verhindet man mit den Surf-Containern *First Party.Isolation*.

   ```
   privacy.firstparty.isolate                    = true
   privacy.firstparty.isolate.block_post_message = true
   ```

2. Integrierte Schutzmaßnahmen gegen Tracking-Cookies bleiben aktiviert, wie es der Standard unter Firefox ist, auch wenn die Filter suboptimal sind.

   ```
   network.cookie.cookieBehavior  = 4
   privacy.purge_trackers.enabled = true
   ```

3. Die Lifetime von Cookies wird nicht verändert. Es werden keine Cookies in Sessioncookies umgewandelt, da das unter Umständen von Trackingdiensten erkannt wird und einige Trackingdienste wie z. B. WebTrekk abweichende Cookieeinstellungen als Feature für das Fingerprinting des Browsers verwenden.

   ```
   network.cookie.thirdparty.sessionOnly = false
   ```

4. Das langfristige Tracking verhindert man mit Löschen aller Daten (Cookies, Cache, . . .)beim Schließen des Browsers.

```
network.cookie.lifetimePolicy        = 2
privacy.sanitize.sanitizeOnShutdown  = true
privacy.clearOnShutdown.cache        = true
privacy.clearOnShutdown.cookies      = true
privacy.clearOnShutdown.downloads    = true
privacy.clearOnShutdown.formdata     = true
privacy.clearOnShutdown.history      = true
privacy.clearOnShutdown.offlineApps  = true
privacy.clearOnShutdown.sessions     = true
privacy.clearOnShutdown.siteSettings = true
```

Die beiden oben genannten Maßnahmen sind durch Trackingdienste nicht erkennbar. Beim Surfen verhält sich der Browser wie die Standardkonfiguration von Millionen anderen Nutzern. Es gibt kaum Einschränkungen, gleichzeitig wird Tracking verhindert.

Außerdem werden EverCookies damit in gleicher Weise behandelt wie Cookies. Es ist nicht sinnvoll, für Cookies strengere Maßstäbe als für EverCookies anzulegen und in Kauf zu nehmen, dass man sich von der Masse der Firefox Nutzer unterscheidet.

(Das ist ein Vorschlag! Andere Meinungen sind natürlich zulässig.)

4.4 EverCookies

80% der Internetnutzer lehnen das Tracking ihres Surfverhaltens ab. Viele Surfer ergreifen einfache Maßnahmen gegen Tracking Cookies. Nach einer Untersuchung von AdTiger blockieren 52,5% der Surfer die Annahme von Cookies, die nicht von der aufgerufenen Website stammen (sogenannte Third-Party-Cookies). Andere Studien [17] kommen auf 15%...35% Cookie-Verweigerer unter den Surfern (was mir seriöser erscheint).

Die Tracking-Branche reagiert auf diese Entwicklung mit erweiterten Markierungen, die unter der Bezeichnung *EverCookie* zusammengefasst werden. Zusätzlich zum Tracking-Cookie werden weitere Markierungen im Browser gespeichert. Später kann ein gelöschtes Tracking-Cookie anhand dieser Markierungen wiederhergestellt werden. Nach empirischen Untersuchungen der University of California [18] nutzen 38% der TOP100 Webseiten moderne EverCookie Techniken zur Markierung der Surfer (Stand 2012).

EverCookies - never forget

Der polnische Informatiker Samy Kamkar hat eine Demonstration [19] von EverCookie Techniken erstellt, die verschiedene technische Möglichkeiten basierend auf HTML5 zeigen:

- Local Shared Objects (Flash Cookies)
- Silverlight Isolated Storage
- Cookies in RGB Werten von Bildern
- Cookies in der History speichern
- Cookies in ETags und im Cache
- window.name auswerten

[17] http://smorgasbork.com/component/content/article/84-a-study-of-internet-users-cookie-and-javascript-settings
[18] https://techscience.org/a/2015121502
[19] http://samy.pl/evercookie/

- Internet Explorer userData Storage
- HTML5 DOMStorage Cookies
- HTML5 Database Storage (IndexedDB)
- HSTS Cookies

DOMStorage in Firefox

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

Aktuelle Versionen von Firefox wenden die Beschränkungen für Cookies auch auf den DOMStorage an. Es reicht aus, die Cookies zu deaktivieren. Damit ist auch die clientseitige Datenspeicherung deaktiviert. Der DOMStorage wird auch mit den Cookies gelöscht.

Es wird auf einige Websites empfohlen, den DOMStorage in Firefox zu deaktivieren, da diese HTML5 Technik zum Markieren von Surfern genutzt werden kann. Wir empfehlen diese Deaktivierung den DOMStorage nicht, da es die Funktionalität einiger Webseiten einschränkt und keinen Gewinn an Privatspäre bringt. Da die Verwendung von DOMStorage an die Freigabe von Cookies gekoppelt ist, ist es egal, ob ein Webserver DOMStorage verwenden könnte, wenn er normale Cookies setzen kann, um den Surfer zu markieren.

Indexed Database API

2015 hat das W3C die *Indexed Database API* als Standard verabschiedet. Dabei handelt es sich um eine hierarchische Datenbank im Browser, die mit JavaScript genutzt werden kann. Im Unterschied zum DOM-Storage können nicht nur Key-Value-Paare gespeichert werden, sondern mittels SQL auch komplexe Abfragen realisiert werden.

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

Firefox wendet die Beschränkungen für Cookies auch auf die IndexedDB an.

4.5 Surf-Container als Trackingschutz

Surf-Container sind ein Konzept von Mozilla und TorProject.org, um Website-übergreifendes Tracking mit Cookies und EverCookies zu verhindern.

- Ein Surf-Container enthält alle Daten, die von Webseiten gespeichert wurden, in einer abgeschotteten Umgebung (Cookies, HTML5-Storage, IndexedDB, Cache, TLS Sessions, Shared Workers, HTTP Authentication ... usw.) Diese Daten bilden dann den sogenannten *Context* für das Surfen in diesem abgeschotteten Container.
- Der Zugriff auf Daten in einem anderen *Context* bzw. anderen Surf-Container ist nicht möglich. Somit werden in den verschiedenen *Contexten* unterschiedliche Tracking Markierungen gesetzt oder man könnte sich in unterschiedlichen Surf-Containern mit verschiedene Identitäten bei einer Website anmelden.

Container schützen nicht gegen Tracking anhand des Browser Fingerprint!

- Da das gleiche Browser Profil mit identischer Konfiguration und Add-ons genutzt wird und außerdem die IP-Adresse identisch ist, können viele Trackingdienste eine Verknüpfung des Surfverhaltens in unterschiedlichen Containern herstellen!

- Die Verwendung von AdBlockern und NoScript zur Kontrolle von JavaScript sind deshalb weiterhin nötig, um sich gegen das allgegenwärtige Tracking zu schützen.

Konzepte für Surf-Container in Firefox

Mozilla hat zwei unterschiedlichen Konzepte in Firefox implementiert:

FirstParty.Isolate wurde für den TorBrowser unter dem Titel *Cross-Origin Identifier Unlinkability* entwickelt und ist mit Firefox 58 auch von Mozilla implementiert worden. Es ist ein wesentliches Privacy Feature, das Firefox von anderen Browsern abhebt. Um dieses Feature zu aktivieren, muss man unter *about:config* folgenden Wert setzen:

```
privacy.firstparty.isolate = true
```

Damit wird für jede Domain in der URL-Leiste (Same Origin) automatisch ein neuer Surf-Container erstellt und alle beim Surfen anfallenden Daten werden in einem individuellen *Context* für separat gespeichert.

Webseiten könnten die Javascript API *windows.postMessage* verwenden, um trotzdem Daten zwischen unterschiedlichen Domains auszutauschen, die in unterschiedlichen Containern gekapselt sind. Um diese Lücke zu schließen, muss man unter *about:config* folgenden Wert setzen:

```
privacy.firstparty.isolate.block_post_message = true
```

FirstParty.Isolate kann zu Login Problemen bei einigen Websites führen, die Single Sign-on (SSO) Techniken nutzen. Betroffen sind beispielsweise fast alle Google Dienste, SoundCloud u.a.m. die einen Google Account für die Anmeldung verwenden. Bei diesen Login Problemen kann man mit folgender Option den Schutz aufweichen:

```
privacy.firstparty.isolate.restrict_opener_access = false
```

Ein weiterer, kleiner Nachteil von FirstParty.Isolate ist, dass man bei Webseiten, die Googles reCaptcha zur Erkennung von Bots nutzen, immer die visuellen Captchas lösen muss. Google kann die Daten aus dem Surf-Tracking zur Unterscheidung von Bots vs. Humans verwenden und wer sich von Google beobachten lässt, muss dann keine Captchas lösen. (Googles reCaptcha dominiert den Markt mit 95-99% Anteil.)

userContext steht seit Ende 2016 zur Verfügung. Es werden mehrere Surf-Container bereitgestellt, die man selbst aktiv auswählen muss. Um das Feature zu aktivieren, muss man zuerst unter der Adresse *about:config* folgenden Wert setzen:

```
privacy.userContext.enabled     = true
privacy.userContext.ui.enabled  = true
```

Danach kann man über den Menüpunkt *Datei - Neuer Tab in Umgebung - ...* einen Tab in einem anderen Surf-Container öffnen oder beim Klick mit der rechten Maustaste auf einen Link wählen, in welchem Surf-Container man den Link öffnen möchte.

Anhand einer Farbkennung auf dem Reiter ist erkennbar, zu welcher Umgebung er gehört. Man kann auch selbst weitere Surf-Container definieren. Ob dieses Konzept effektiv eingesetzt wird, hängt in erster Linie von der Disziplin des Anwenders ab.

In unterschiedlichen userContext Containern kann man sich gleichzeitig mit unterschiedlichen Accounts bei einem Webdienst anmelden. Das ist eine der Haupteinsatzmöglichkeiten für dieses Feature.

Hinweis: *userContext* und *FirstParty.Isolate* können (noch) nicht in Kombination mit dem *Private Browsing Mode* verwendet werden. Außerdem funktionieren sie nicht, wenn man in den Datenschutzeinstellungen für die Chronik die Option *niemals anlegen* auswählt.

4.6 JavaScript

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

1. Mit Hilfe von JavaScript kann man ein Vielzahl von Informationen über den Browser und das Betriebssystem auslesen. Bildschirmgröße, Farbeinstellungen, installierte Schriftarten... Diese Informationen können zu einem individuellen Fingerabdruck des Browsers verrechnet werden.

2. EverCookie Techniken nutzen JavaScript, um Markierungen im Browser zu hinterlegen und gelöschte Tracking Cookies wiederherzustellen.

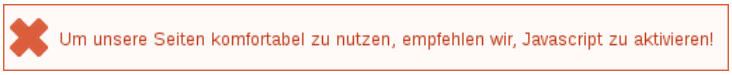
3. Bösartiger JavaScript Code kann aktiv Sicherheitslücken im Browser ausnutzen und den Rechner kompromittieren. Im Januar 2013 lieferten die Server des Werbenetzwerkes OpenX bösartige Scripte aus, die den Rechner über Sicherheitslücken im Internet Explorer kompromittierten. Auch die bisher bekannten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

4. Forscher der Columbia University haben eine side-channel attack vorgestellt, die komplett als JavaScript im Browser läuft: *The Spy in the Sandbox – Practical Cache Attacks in JavaScript*[20]. Mit dem Angriff können beliebige Prozesse außerhalb des Browsers analysiert werden ohne den Rechner zu kompromittieren (spurenfrei). Seitenkanalangriffe sind ein moderner Angriff gegen Kryptografie.

5. Bösartiger JavaScript Code kann sich auch gegen Dritte richten, ohne das der Nutzer es bemerkt. Chinas Great Cannon[21] injiziert JavaScript Code beim Aufruf chinesischer Webseiten, um die PCs der Nutzer als Botnet für DDoS-Attacken zu nutzen.

Prinzip Whitelisting

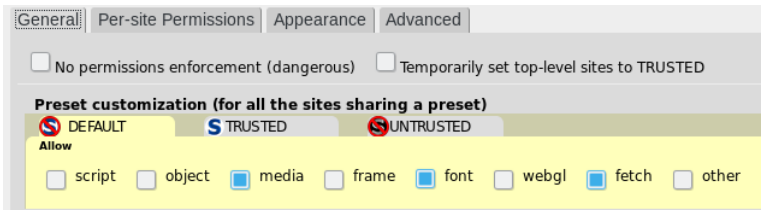
Ein generelles Abschalten ist heutzutage nicht sinnvoll. Ähnlich dem Cookie-Management benötigt man ein Whitelisting, welches JavaScript für vertrauenswürdige Websites zur Erreichung der vollen Funktionalität erlaubt, im allgemeinen jedoch deaktiviert. Gute Webdesigner weisen den Nutzer darauf hin, dass ohne JavaScript eine Einschränkung der Funktionalität zu erwarten ist.



4.6.1 NoScript für Mozilla Firefox

Mit dem Add-on NoScript kann man nicht nur Einstellungen für JavaScript verwalten sondern auch für Flash- und Silverlight Objekte, Frames, Fonts, WebGL u.a.

Nach der Installation kann man die Einstellungen von NoScript anpassen. Auf dem Reiter *General* findet man die Einstellungen für die Kategorien *Default*, *Trusted* und *Untrusted*. Standardmäßig braucht man nur Bilder und Mediendateien. In die Verwaltung der Fonts sollte sich NoScript nicht einmischen, dass wird weiter unten beschrieben.



[20] https://arxiv.org/pdf/1502.07373v2.pdf
[21] https://citizenlab.org/2015/04/chinas-great-cannon/

Vertrauenswürdige Webseiten (*Trusted*) dürfen JavaScript ausführen (Option *script*), das reicht in der Regel. iFrames kann man mit NoScript oder uBlock Origin blockieren (s.u.), ich habe mich für NoScript entschieden. Wenn eine Webseite unbedingt Frames oder WebGL benötigt, dann kann man individuelle Konfigurationen für diese Webseiten definieren. Als *Untrusted* definierte Webseiten dürfen nichts.

Wer es lieber ein bisschen komfortabler und weniger restrikiv mag, der kann die Option *Temporary set top-level sites to TRUSTED* aktivieren. Dann darf die aufgerufene Webseite immer ihre Scripte ausführen. Es werden nur Drittseite blockiert, die oft Trackingscripte enthalten. Viele Webseiten funktionieren damit problemlos.

Auf dem Reiter *Per-site Permissions* kann man die Freigaben für einzelne Webseiten verwalten. NoScript bringt eine Menge Freigaben standardmäßig mit, die man erstmal ausmisten kann. Google braucht man nicht, wenn man keine Google Dienste verwendet und Microsofts Live und Passport auch nicht.

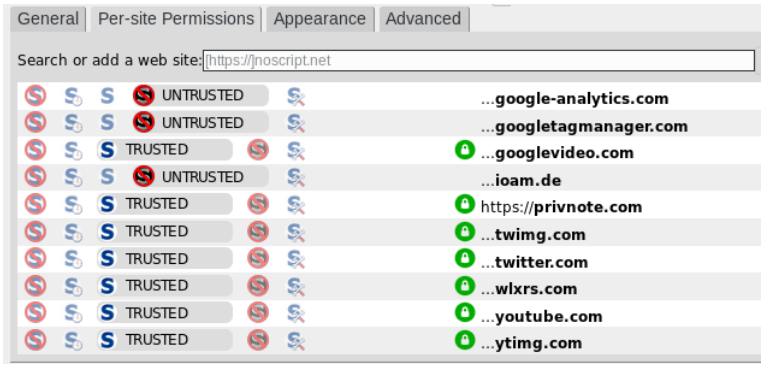


Abbildung 4.3: Per-site Permissions in der NoScript Konfiguration

Ein grünes Schloss bedeutet in den *Per-site Permissions*, dass die Freigabe nur für HTTPS gilt (sicherer). Wenn die Freigabe auch für unverschlüsseltes HTTP gilt, dann wird ein rotes Schloss angezeigt. Mit einem Klick auf das Schloss kann man die Berechtigung umschalten.

Skripte von Drittseiten

Skripte von Drittanbietern (googletagmanager, ioam...) werden üblicherweise nur zum Spionieren verwendet und sind für die Funktionalität selten notwendig. Ausnahmen von dieser Regel sind:

Captchas: Einige Webseiten verwenden Captchas von Drittanbietern als Spamschutz. Die Captchas funktionieren nur, wenn JavaScript für den Captcha-Provider freigegeben wird. Wenn das Captcha auf einer Webseite nicht funktioniert, kann man in der Liste nachschauen, ob evtl. ein Captcha-Provider dabei ist und diese temporär freigeben.

- Für das häufig verwendete Google Captcha muss man JavaScript temporär für *google.com* und *gstatic.com* freigeben.

Videos: Firefox braucht keinen Flash Player, um Videos abspielen zu können, aber man muss JavaScript für einige Drittseiten freigegeben. Dabei handelt es sich in der Regel um Content Delivery Networks (CDN) des Dienstes. Diese CDN-Server sind für die Auslieferung von statischem Content und großen Dateien optimiert.

- Um auf der Youtube Webseite Videos zu sehen, muss man JavaScript für *youtube.com*, *youtube-nocookie.com*, *ytimg.com* und *googlevideo.com* freigeben.
  Da viele Webseiten Youtube Videos einbinden, kann man diese Freigaben dauerhaft speichern.

- Um Vimeo-Videos von abzuspielen, muss man JavaScript für *vimeo.com* und *vimeocdn.com* freigeben.
- Um Videos von Bild.de abzuspielen, muss man JavaScript für *bild.de* und *bildstatic.de* temporär freigeben.
- Für Youporn Videos muss man JavaScript für die Domainnamen *youporn.com* und *phncdn.com* temporär freigeben.
- ...

Schutz gegen XSS-Angriffe

Im Gegensatz zum Internet Explorer und den auf Webkit basierenden Browsern wie Google Chrome hat Firefox keinen eingebauten Schutz gegen XSS-Angriffe. NoScript rüstet diese fehlende Sicherheitsfunktion nach und zeigt eine Warnung bei einem XSS-Angriff:

Die XSS-Protection von NoScript ist standardmäßig aktiv und muss nicht wie beim Internet Explorer oder Google Chrome durch den Webserver mit dem HTTP Response Header *X-XSS-Protection: 1; mode=block* aktiviert werden.

JIT-Compiler

Just-In-Time Compiler sollen die Ausführung von JavaScript beschleunigen. Der JavaScript Code wird nicht Anweisung für Anweisung interpretiert sondern vor der Ausführung durch einen Compiler gejagt, der verschiedene Optimierungen vornimmt. Diese zusätzliche Komplexität schafft auch zusätzliche Fehlerquellen. Es gab bereits mehrere sicherheitskritische Bugs in den JIT-Compilern von von Firefox, beispw. Bug #1607443 in Firefox 72.[22]

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

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

Diese Einstellungen können die Performance einiger Webseiten deutlich verringern.

4.7 iFrames

Einige Trackingdienste verwenden iFrames, um HTML-Wanzen zu laden, wenn JavaScript blockiert ist und keine Trackingscripte ausgeführt werden können. Auf vielen Webseiten findet man den Code von GoogleTagManager (*Google Universal Analytics tracking code*):

```
<noscript>
  <iframe src="//www.googletagmanager.com/ns.html?id=blabala..."
    height="0" width="0" style="display:none;visibility:hidden">
  </iframe>
</noscript>
```

Die Tracking Technik des *DoubleClick Bid Manager* wurde von Invite Media entwickelt und in DoubleClick integriert, nachdem Google die Firma Invite Media aufgekauft hatte. Auch dieses Tracking nutzt einen unsichtbaren iFrame, um Tracking Wanzen mit oder ohne JavaScript zu platzieren:

```
<script type="text/javascript">
...
 <document.write('
    <iframe src="http://nnnn.fls.doubleclick.net/activityi;src=xxxx;...."
```

[22] https://www.heise.de/security/meldung/Jetzt-patchen-Angreifer-attackieren-Firefox-4630850.html

```
    width="1" height="1" frameborder="0" style="display:none"></iframe>');
</script>
<noscript>
  <iframe src=""http://nnnn.fls.doubleclick.net/activityi;src=xxxxx;"
    width="1" height="1" frameborder="0" style="display:none">
  </iframe>
</noscript>
```

Embedded Youtube Videos

Viele Webseiten integrieren Youtube Videos. Die Integration erfolgt als iFrame:

```
<iframe src="https://www.youtube.com/embed/xyz........
```

Mit dem Aufruf der Webseite, welche das eingebettete Video enthält, wird auch der iFrame von Youtube geladen und der Surfer mit einem Cookie von Youtube markiert. Um mit europäischem Datenschutzrecht konform zu sein, bietet Youtube eine Adresse für die Einbettung von Videos in Webseiten an, die auf das Setzen von Tracking Cookies verzichtet:

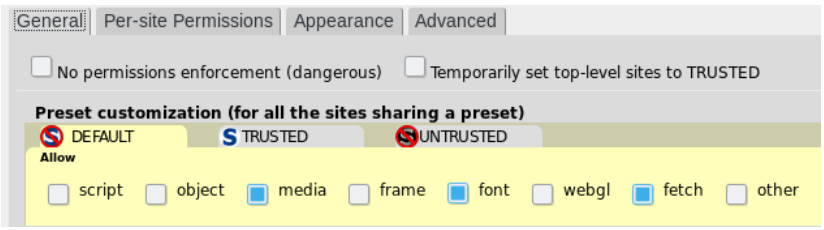
```
<iframe src="https://www.youtube-nocookie.com/embed/xyz........
```

Leider wählen nicht alle Webseitenbetreiber die privacy-freundlichere Youtube Variante. Man kann das Add-on *Privacy Enhanced Mode for Embedded Youtube*[23] installieren. Es schreibt die Adressen für embedded Youtube Videos auf die No-Cookie Adresse um.

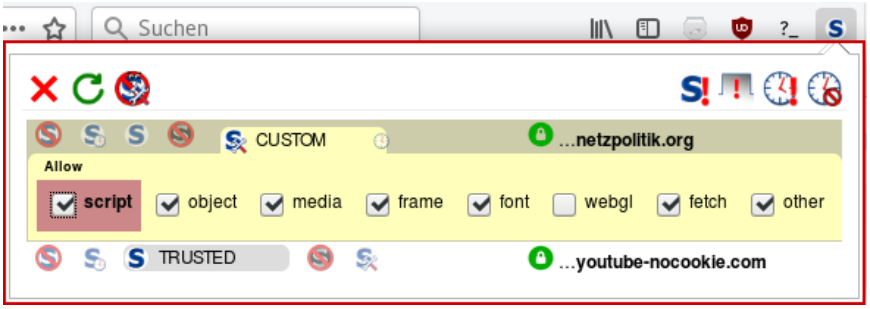
iFrames blockieren

Man kann iFrames generell mit den Add-ons *NoScript* oder *uBlock Origin* blockieren ohne wesentliche Einschränkungen beim Surfen. Bei Bedarf kann man Ausnahmen deklarieren und iFrames für einzelne Webseiten erlauben.

1. Mit dem Add-on **NoScript** blockiert man iFrames, indem man in allen Standardeinstellungen (auch *Trusted*!) die Option *frame* deaktiviert.



   Für vertrauenswürdige Webseiten, die Video-Player via iFrame einbinden, kann man *Custom* Settings definieren, um die Videos anschauen zu können.



2. Mit dem Add-on **uBlock Origin** blockiert man iFrames von Drittseiten, indem man in der ausgeklappten Übersicht die erste Spalte hinter der Option *Frames von Drittseiten* auf Rot setzt und die Einstellungen mit Klick auf das Schloss-Symbol speichert.

[23] https://addons.mozilla.org/de/firefox/addon/youtube-nocookie/

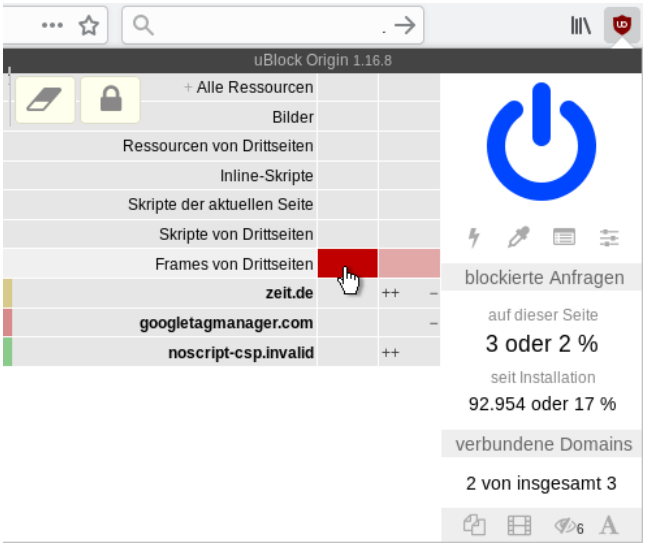


Abbildung 4.4: Blockieren der Frames von Drittseiten mit uBlock Origin

Wenn eine Webseite Frames von Drittseiten darf (z. B. weil Videos von Youtube oder Vimeo via iFrame eingebunden wurden), ann man in der zweiten Spalte eine lokale Ausnahme für die Drittseite definieren, indem man dieses Feld auf Grau setzt. Das Beispiel in Abb. 4.5 zeigt die Konfiguration, wenn man temporär bei Netzpolitik.org ein eingebettetes Video von Youtube anschauen möchte. Mit einem Klick auf das Schloss Symbol kann man die Einstellung dauerhaft speichern.

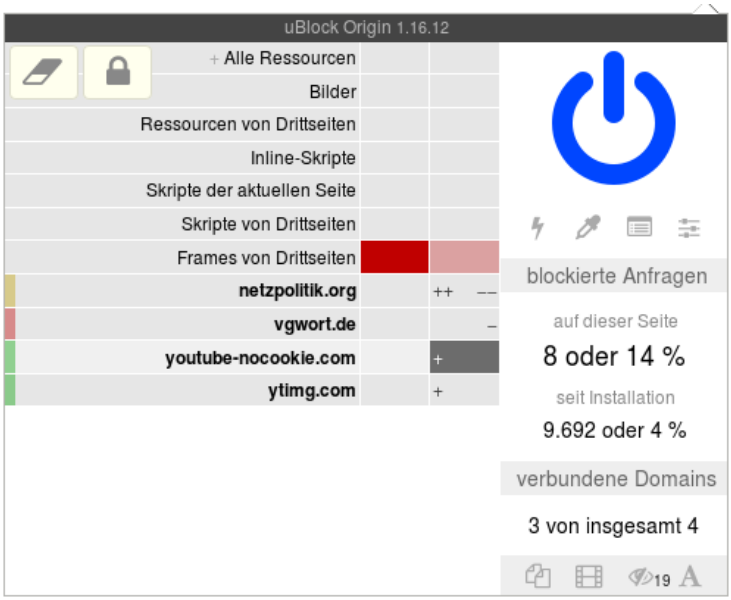


Abbildung 4.5: Freigeben von Frames für die Anzeige von embedded Youtube Videos auf Netzpolitik.org

3. Statt über das GUI von **uBlock Origin** kann man iFrames von Drittseiten auch in den Einstellungen blockieren. In der Konfiguration fügt man auf dem Reiter *Meine Regeln* folgen Regel hinzu:

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

Ausnahmen (z. B. für eingebettete Videos) definiert man nach folgendem Muster:

```
netzpolitik.org www.youtube-nocookie.com * noop
```

Auf der Webseite von Netzpolitk.org dürfen Framens, Scripte usw. von der Domain *www.youtube-nocookie.com* geladen werden. Die dynamische Filterung von Werbung und Trackingelementen bleibt dabei aktiv.

Für welche Variante man sich entscheidet, hängt von persönlichen Vorlieben ab.

4.8 Werbung, HTML-Wanzen und Social Media

Die auf vielen Websites eingeblendete **Werbung** wird von wenigen Servern bereitgestellt. Diese nutzen häufig (eigentlich immer) die damit gegebenen Möglichkeiten, das Surfverhalten über viele Websites hinweg zu erfassen. Dabei können direkt oder indirekt sehr private Informationen über den Surfer ermittelt werden.

- Der Blutspendendienst des Bayrischen Roten Kreuzes stellt auf seiner Webseite einen Vorcheck bereit. Durch ein eingebundenes Trackingscript von Facebook wurden die Antworten auf sensible Fragen zu Schwangerschaft, Drogenkonsum, Diabetes oder HIV-Infektion an Facebook gesendet, wie eine Analyse der Süddeutschen Zeitung ergab.[24]

- Eine Studie von Privacy International hat 136 Webseiten mit Gesundheitsinformationen untersucht. Dabei wurde klar, dass fast alle Webseiten mit Trackern verseucht waren und dass die Werbenetzwerke allein durch das Aufrufen einer Seite mit bestimmten Informationen zu Krankheiten interessante Einsichten gewinnen, ob man sich beispielsweise für Krankheitssympthome oder Heilung von Depressionen interessiert. Diese Informationen können in die Profilbildung einfließen und zu Schlussfolgerungen führen, die uns nicht gefallen werden. Bei zwei Websites wurde auch Antworten auf sensible, gesundheitliche Fragen zur Ferndiagnose an die Werbenetzwerke übertragen.[25]

Immer häufiger nutzen Kriminelle die große Werbenetzwerke, um mit ihre Schadsoftware möglichst vielen Rechnern anzugreifen. Nach Beobachtung von Trend Micro[26] kaufen Kriminelle zur Zielgruppe passende Werbeplätze, lassen bösartige Werbebanner ausliefern oder locken die Surfer mit Anzeigen auf Malware Webseiten. Diese Angriffe werden als Malvertising bezeichnet (abgeleitet von *malicious advertising*) und nehmen derzeit stark zu. Die Sicherheitexperten von Cyphort registrierten 2015 einen Anstieg von 325% und erwarteten eine Fortsetzung des Trends für 2016. Einige Beispiele für derartige Angriffe:

- Im Januar 2013 lieferten die Server des Werbenetzwerkes OpenX bösartige Scripte aus, die den Rechner über Sicherheitslücken im Java Plug-in und im Internet Explorer kompromittierten.[27]

- Zum Jahreswechsel 2014 wurden innerhalb von 4 Tagen 27.000 Surfer durch Werbung von Yahoo mit Malware infiziert.[28]

- Eine erfolgreiche, mehrwöchige Malvertising Kampagne konnte im Aug. 2015 mit Hilfe von Doubleclick einige Millionen Surfer infizieren.[29]

[24] https://www.sueddeutsche.de/dgital/blutspende-brk-facebook-patientendaten-1.4576563
[25] https://heise.de/-4513282
[26] http://heise.de/-2429990
[27] http://heise.de/-1787511
[28] http://www.zdnet.de/88180242/werbung-auf-yahoo-com-verteilte-malware-an-nutzer-in-europa
[29] https://blog.malwarebytes.org/malvertising-2/2015/09/large-malvertising-campaign-goes-almost-undetected/

- Im Nov. 2015 wurden die Server des Werbenetzwerkes Pagefair gehackt, um bösartigen JavaScript Code in der Werbung auszuliefern.[30]

Bei **HTML-Wanzen** (sogenannten Webbugs) handelt es sich um 1x1-Pixel große transparente Bildchen, welche in den HTML-Code einer Webseite oder einer E-Mail eingebettet werden. Sie sind für den Nutzer unsichtbar und werden beim Betrachten einer Webseite oder beim Öffnen der E-Mail von einem externen Server geladen und ermöglichen es dem Betreiber des Servers, das Surfverhalten websiteübergreifend zu verfolgen.

Die **Like Buttons** werden von Facebook und anderen Soziale Netzen verwendet, um Daten zu sammeln. Mit dem Aufruf einer Webseite mit Facebook Like Button werden Daten an Facebook übertragen und dort ausgewertet, auch wenn der Surfer selbst kein Mitglied bei Facebook ist. Die Verwendung der Like Buttons ist nach Ansicht von Thilo Weichert (ULD) nicht mit deutschen Datenschutzrecht vereinbar. Deutsche Webseitenbetreiber sind aufgefordert, die Facebook Buttons von ihren Seiten zu entfernen[31].

Forscher der Universität Cambridge (Großbritannien) konnten im Rahmen einer Untersuchung durch Auswertung der Klicks auf Facebook Like Buttons die sexuelle Orientierung und politische Einstellung der Teilnehmer vorhersagen[32]. Man verrät mit einem Klick auf einen Like Button möglicherweise Informationen, die man nicht im Netz veröffentlichen möchte.

4.8.1 Tracking-Filter für Firefox

Es gibt mehrere Add-ons für Firefox, die Werbung und Trackingelemente blockieren. Das Center for Internet and Society der Stanford Law School hat in einer Analyse vom September 2011 einige Lösungen verglichen [33]. Die Ergebnisse in Bild 4.6 zeigen: keine Lösung ist perfekt.

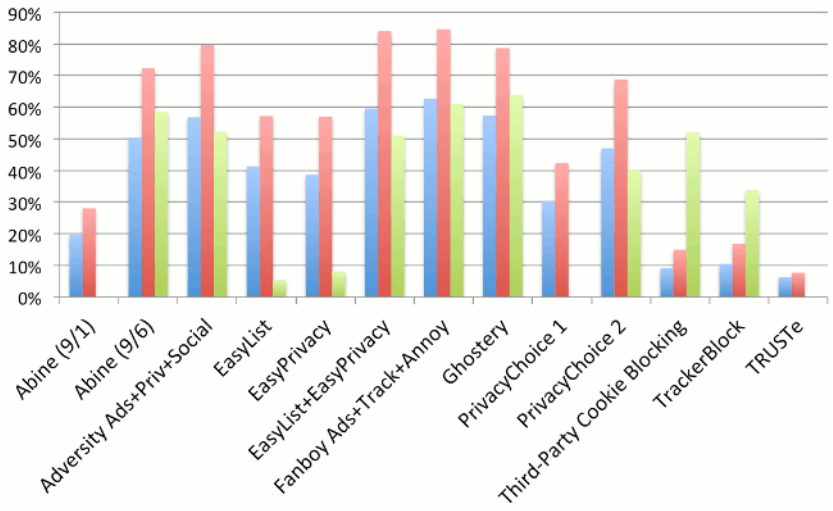


Abbildung 4.6: Effektivität verschiedener Tracking-Filter

Aufgrund der Flexibilität bei der Einbindung verschiedener Filterlisten und der langfristigen Stabilität in der Entwicklung sind
textituBlock Origin und textitAdBlock Plus empfehlenswert. Mit den Easylist Filterlisten erreichen die Add-ons die besten Ergebnisse. Die Listen werden ständig weiterentwickelt.

[30] http://www.golem.de/news/anti-adblocker-dienst-500-websites-ueber-pagefair-gehackt-1511-117262.html
[31] https://www.datenschutzzentrum.de/facebook
[32] http://heise.de/-1820638
[33] https://cyberlaw.stanford.edu/node/6730

Zusätzlich zur den Blocklisten gegen Werbung und Tracking gibt es auch Listen, die die Social Media Buttons blockieren. FanBoy arbeitet seit 2010 mit EasyList zusammen, daher die gleichfalls guten Ergebnisse.

Ghostery schneidet im Test auch gut ab und wird oft empfohlen. Insbesondere in der Diskussion um Acceptable Ads in AdBLock Plus wird Ghostery immer wieder als angeblich saubere Alternative genannt. Dabei wird übersehen, das Ghostery bei den Trackingdiensten Drawbridge[34] und Tapad[35] als Partner gelistet ist. Die Spezialität dieser Trackingdienste ist die Identifikation der unterschiedlichen Geräte (Smartphones, Computer auf der Arbeit und zuhause, Laptops, Tablets), die von einem User benutzt werden. Die Kooperation mit den Trackingdiensten ist auf der Ghostery Webseite[36] nicht klar beschrieben und nicht offengelegt. Möglicherweise handelt es sich dabei um die via Ghostrank von dem Browser Add-on gesammelten Daten? Da diese Zusammenarbeit mit der Werbeindustrie und die resultierenden Folgen wie *Ghostery Verified Domains* undurchsichtig sind, wird Ghostery hier NICHT empfohlen.

4.8.2 Tracking Protection in Firefox

Firefor enthält einen eingebauten Trackingschutz, den man in den Einstellungen in der Sektion *Datenschutz und Sicherheit* aktiviert. Es wird eine Blockliste von Disconnect genutzt, die von einem Mozilla-Server heruntergeladen wird. Diese Blockliste ist nicht dafür ausgelegt, möglichst viel Werbung auf allen Webseiten zu blockieren. Sie blockiert Trackingdienste und damit als Nebeneffekt Werbebanner, die für Tracking genutzt werden. Folgende Schutzlevel stehen dabei zur Auswahl:

Standard: In Firefox 69.0 ist der Schutz gegen Trackingscripte standardmäßig nur in privaten Fenstern aktiv, der Schutz gegen Trackingcookies und Krypto-Miner ist immer aktiv.

Streng: Im strengen Modus sollen Scripte zum Tracking in allen Fenstern blockiert werden, außerdem Trackingcookies, Krypto-Miner sowie Scripte zum Fingerprinting des Browsers.

Benutzerdefiniert: Außerdem gibt es die benutzerdefinierte Konfiguration, in der man selbst enscheiden kann, welche Schutzmechanismen aktiviert werden sollen. An dieser Stelle könnte man auch die allgm. Richtlinien zur Behandlung von Cookies konfigurieren.

Der Trackingschutz ist nur bedingt brauchbar, wie ein oberflächlicher Test zeigt. Für den kleinen Test wurde die strenge Tracking Protection von Firefox 69.0 aktiviert und dann wurden ein paar Webseiten aufgerufen. Dabei wurde vor allem beobachtet, welche Third-Party Cookies jetzt als Trackingcookies erkannt und blockiert wurden.

- Auf den Webseiten *Heise.de* und *Zeit.de* ist die Werbung verschwunden aber die Trackingcookies von WebTrekk werden nicht blockiert. Das ist evtl. nicht verwunderlich, da sich WebTrekk mit DNS-Aliases auf beiden Webseiten einen First-Party Status erschleicht und der in Firefox 69.0 implementierte Schutz gegen Trackingcookies nur Third-Party Cookies analysiert und in gute und böse Cookies einteilt.

  Trackingscripte von Google und OpenX werden auf Heise.de und Zeit.de blockiert, aber man wird auf beiden Webseiten mit Third-Party Cookies von EASYmedia beobachtet, die nicht von der Tracking Protection blockiert werden. In der Datenschutzpolicy von EASYmedia findet man folgenden Satz zum Austausch von Daten mit Dritten:

[34] http://drawbrid.ge
[35] http://www.tapad.com
[36] https://www.ghostery.com

> *- EASYmedia ist mit einer großen Anzahl von Partnern wie z. B. Google, OpenX, SmartAds und vielen anderen verbunden. Um die Bereitstellung unseres Dienstes im Cookie-basierten Advertising Ökosystem zu ermöglichen, tauscht EASYmedia automatisiert pseudonyme IDs mit solchen Partnern aus...*
>
> *- EASYmedia kann auch Informationen von Dritten erhalten, um gezielte und maßgeschneiderte Werbung auf Webseiten und mobilen Anwendungen zu ermöglichen.*

(Es gibt Tracking-Familien, die die Daten untereinander austauschen und damit eine große Reichweite bei der Beobachtung des Surfverhaltens erreichen... und das Google-Imperium ist die größte Familie.)

- Auf *YouTube.com* wird man trotz strengem Trackingschutz mit einem Cookie von DoubleClick.net markiert, das zur Auswahl von individuell optimierter Werbung verwendet wird, siehe IDE Cookie bei Googles Cookie-Arten:

  > *Wir verwenden Cookies auch für Werbung, die wir an verschiedenen Stellen im Web zeigen. Unser wichtigstes Cookie für Anzeigenvorgaben für Websites, die nicht zu Google gehören, heißt IDE. Es wird in Browsern unter der Domain doubleclick.net gespeichert. [...] Andere Google-Produkte wie YouTube nutzen dieses Cookie möglicherweise ebenfalls zur Auswahl relevanter Werbung.*

  (Also wenn das kein bekanntes Trackingcookie ist...)

- Auf *Bild.de* werden viele Trackingscripte blockiert, die Webseite ist offensichlich mit unterschiedlichsten Trackern überflutet. Allerdings ist der Schutz auch hier nicht umfassend. Es wurden keine Trackingcookies von der neuen Firefox Tracking Protection gefunden und blockiert, aber einige der akzeptierten Third-Party Cookies von WebTrekk, Dynamic Yield, TealiumIQ, Adserve.io usw. könnte man eindeutig als Tracking einsortieren.

Das sind nur Beispiele und ist keine wiss. Analyse. Es zeigt aber, dass der Trackingschutz von Firefox oft nur oberflächlich arbeitet und andere Lösungen mit optimierten Filterlisten für deutsche Surfer bessere Ergebnisse erreichen un dauch mehr Features bieten.

Bei Aktivierung der Tracking Protection werden aber nicht nur die Filter aktiviert sondern auch Do-Not-Track (DNT). Mit jedem HTTP Request wird ein DNT Header gesendet, der allen Webservern den Wunsch des Nutzers anzeigen soll, dass man nicht beschnüffelt werden möchte. Do-Not-Track ist politisch gescheitert, es wird von Trackingdiensten ignoriert. Die Aktivierung des DNT Headers schafft aber ein Differenzierungsmerkmal für das Browser Fingerprinting, wie auch die DNT Working Group des W3C in ihrer Spezifikation anmerkt. Deshalb ist es empfehlenswert, die Firefox Tracking Protection abschalten und statt dessen einen anderen AdBlocker verwenden:

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

Das gleiche gilt für den Private Browsing Mode (PBM). Im PBM wird die Tracking Protection standardmäßg aktiviert und es wird damit ein DNT Header gesendet, womit das Fingerprinting des Browsers erleichtert wird. Mit folgender Option deaktiviert man die Tracking Protection im Private Browsing Mode:

```
privacy.trackingprotection.pbmode.enabled = false
```

4.8.3 uBlock Origin für Firefox

uBlock Origin[37] ist ein effizienter und einfach installierberer Werbeblocker für Firefox. Zur Installation muss man nur auf den Downloadbutton auf der Webseite klicken.

[37] https://addons.mozilla.org/de/firefox/addon/ublock-origin

Nach der Installation findet man oben rechts in der Toolbar des Browsers das uBlock Symbol. Mit einem Klick auf des Symbol kann man die Filterung für die aktuelle Webseite anpassen oder ganz deaktivieren. Mit einem Klick auf das kleine Symbol für *Einstellungen* rechts unter dem dicken Schalter kann man die Konfiguration anpassen.

Um die Anpassungen zu vereinfachen, stellen wir die Config Datei *ublock-config-2.txt*[38] zum Download bereit, die man auf dem Reiter *Einstellungen* importieren kann. Diese Konfiguration aktiviert mehr Filterlisten (siehe unten), enthält die Filter für den Schutz gegen Zugriffe auf lokale URLs sowie eine kleine Whitelist und verhindert das Senden von CSP Reports, wobei für NoScript die notwendigen Ausnahmen definiert werden.

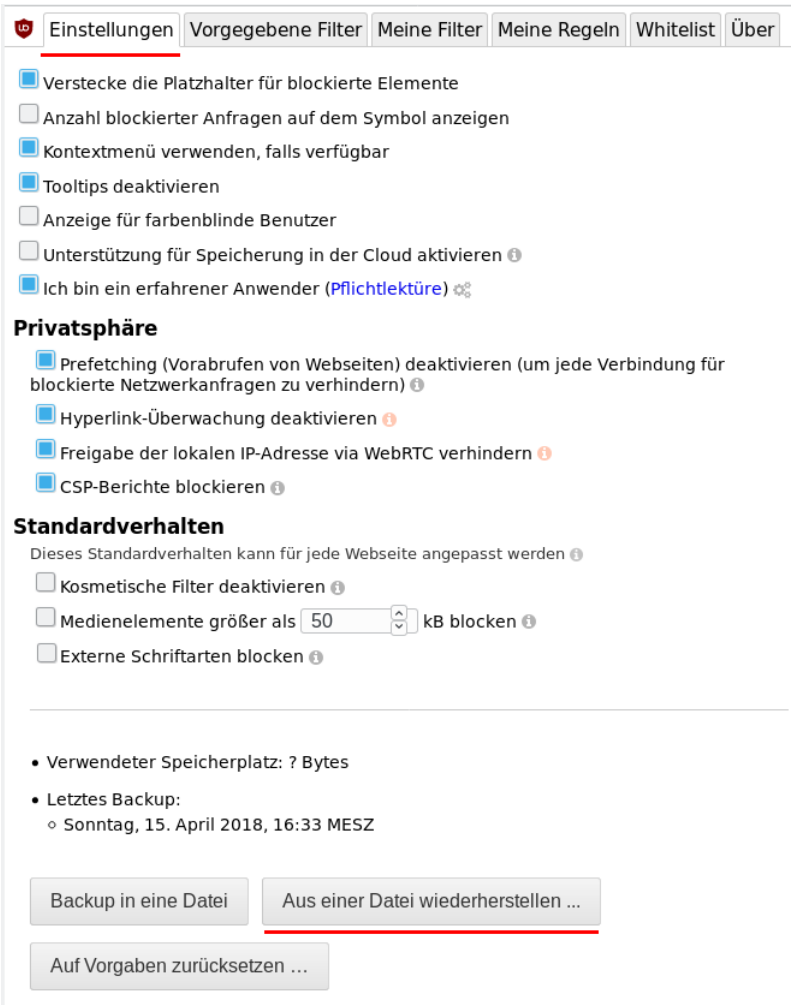


Abbildung 4.7: Dashboard von uBlock Origin

Die verwendeten Filterlisten werden auf dem Reiter *3rd-party filters* aktiviert, z. B. *Fanboy's Social Blocking List* oder *EasyList Germany* sowie die *Anti-AdBlock-Killer* Liste, die wieder das werbefreie Lesen von Bild.de und ähnlichen Webseiten ermöglicht. Aus Sicherheitsgründen würde ich keine Listen abonnieren, die über eine unverschlüsselt HTTP-Verbindung aktualisiert werden (erkennbar an dem roten Symbol *http*).

[38] https://www.privacy-handbuch.de/download/ublock-config-2.txt

Laden externer Schriftarten mit uBlock blockieren?

Das Blockieren von externen Schriftarten mit uBlock Origin empfehlen wir nicht. Einerseits werden die Zugriffe auf CSS Server wie *fonts.googleapis.com* damit nicht blockiert, da die Stylesheets trotzdem geholt werden. Außderem werde damit auch die via Fonts dargestellten Navigationssymbole blockiert, so dass viele Webseiten unbenutzbar werden.

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

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

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

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

uBlock Origin zusammen mit NoScript verwenden

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

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

4.9 Firefox activity-stream

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

- Das Suchfeld könnte man als praktisch aber überflüssig bezeichnen, da man in der Adressleiste bereits ein Suchfeld hat.
- Häufig besuchte Webseiten und zufällige Vorschläge aus der History sind überflüssig, wenn man diese Daten nicht speichert.
- Die individuell optimierten Vorschläge, die von Pocket aus einer handverlesenen Liste von 900+ Top Webseiten ausgewählt werden, sind privacy-relevant.

  Laut Datenschutz Statement verwendet Pocket Cookies und andere Technologien (EverCookies?) um einen optimalen Service basierend auf unseren Aktivtäten und Interessen(!) anzubieten. Klickt man auf einen der angebotenen Vorschläge, dann signalisiert man damit Interesse an dem Thema und der Klick wird von Pocket registriert. Außerdem sammelt Pocket Telemetriedaten über den Aufruf des activity-stream und Informationen darüber, ob der activity-stream vom User abgeschaltet wurde.

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

  Beim Test der Funktion wurden Webseiten wie Bild.de, Youtube.com und ähnliches vorgeschlagen. Ist Bild.de wirklich eine Webseite, die man an erster Stelle empfehlen muss? Oder hat der Springer Verlag dafür bezahlt? Durch den Aufruf der NewTab Page wurden auf einem nackten Firefox 57.0 mehrere Tracking Cookies für Bild.de reproduzierbar neu gesetzt (siehe Abb. 4.10: *wt3_eid* und *wt3_sid* sind Tracking Cookies von WebTrekk), obwohl www.Bild.de nie aufgerufen wurde.

  Wie konnte die Webseite Bild.de die Trackingcookies setzen? Um die NewTab Page darzustellen (seit Firefox 61 auch die Startseite), holt Firefox eine JSON Datei von

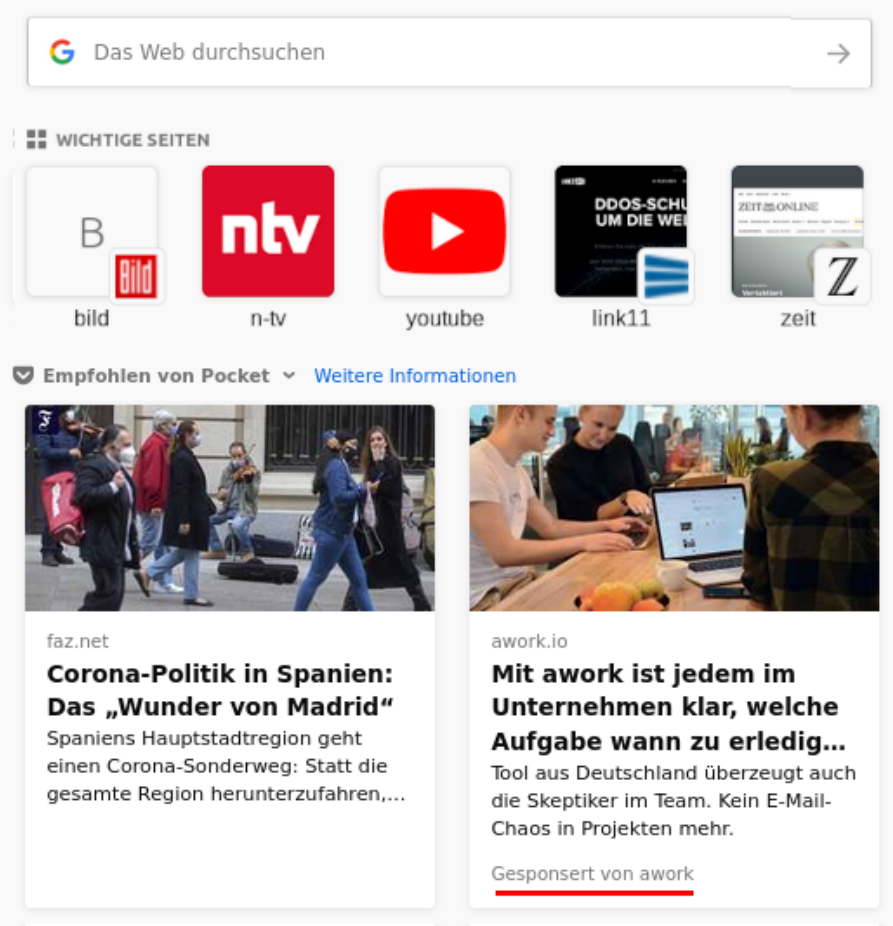


Abbildung 4.8: Gesponserte Empfehlungen auf der NewTab Seite und Startseite

Mozilla, die eine Liste mit den URLs für die darzustellenden Icons aller 900+ Top Webseiten enthält. Für Bild.de findet man folgenden Eintrag:

```
{
"domians": ["bild.de"]
"image_url": "https://bilder.bild.de/fotos/bild-de-..../3.bild.png"
}
```

Das Icon für Bild.de wird also von dem Webserver *bilder.bild.de* geholt und dieser nutzt die Möglichkeit, um einige Trackingcookies zu setzen. Das ist bei anderen Empfehlungen auch möglich.

activity-stream deaktivieren

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

Unter der Adresse *about:config* kann man Einstellungen ebenfalls vornehmen und den activity-stream für die Startseite und für neue Tabs abschalten:

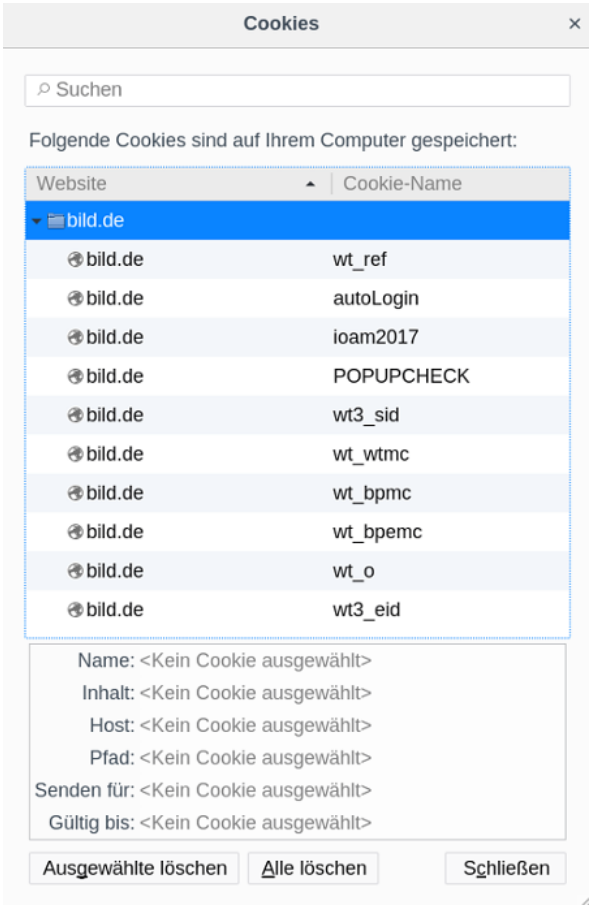


Abbildung 4.9: Cookies von Bild.de nach Aufruf eines neuen Tab

```
browser.startup.page       = 0
browser.newtabpage.enabled = false
```

Außerdem kann man die *Highlights* im Menü der Bibliothek abschalten:

```
browser.library.activity-stream.enabled = false
```

Firefox zeigt die handverlesenden *Topsites* außerdem in der Liste der Vorschlägen bei Eingabe einer Adresse in der URL Leiste an. Das deaktiviert man mit:

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

Bezahlte Werbeeinblendungen deaktiviert mit mit folgenden Einstellungen:

```
browser.newtabpage.activity-stream.showSponsored = false
browser.newtabpage.activity-stream.showSponsoredTopSites = false
```

Oberflächlich sieht damit alles ok aus, man hat eine Startseite sowie NewTab Page ohne überflüssigen Schnickschnack und wird nicht mit handverlesenen Empfehlungen belästigt. Beim Starten kontaktiert Firefox aber weiterhin die Server mit dem Empfehlungen und holt die aktuellen Dateien. Das kann man Firefox mit folgenden Optionen abgewöhnen:

```
browser.newtabpage.activity-stream.feeds.topsites = false
browser.newtabpage.activity-stream.feeds.snippets = false
browser.newtabpage.activity-stream.section.highlights.includePocket = false
browser.newtabpage.activity-stream.feeds.system.topsites = false
```

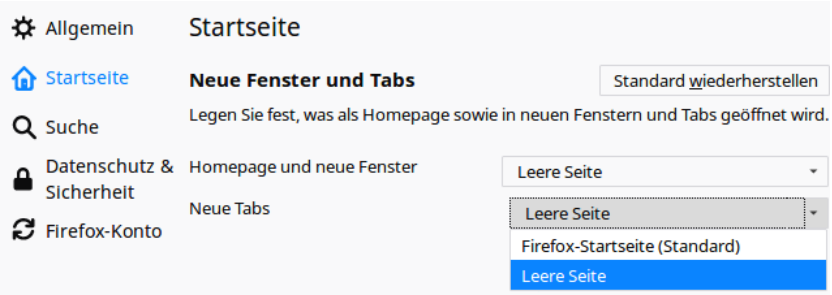


Abbildung 4.10: Leere Seite für Startseite und neue Tabs konfigurieren

Im Hintergrund werden außerdem Telemetrie Pings an den Pocket Server gesendet und Firefox teilt damit dem Pocket Server laufend mit, dass man *activity-stream feeds* deaktiviert hat. Um diese Telemetrie Pings ebenfalls zu deaktivieren, muss man noch einige weitere Werte unter äbout:configßetzen:

```
browser.newtabpage.activity-stream.telemetry       = false
browser.newtabpage.activity-stream.feeds.telemetry = false
```

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

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

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

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

4.10 Contextual Feature Recommender (CFR)

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

Mir ist unklar, nach welchen Richtlinien Mozilla die Empfehlungen für Add-ons auswählt. Mit der Empfehlung für das Web-Security Add-on hatte Mozilla schon gründlich daneben gegriffen und ein Tracking Add-on als Trackingschutz empfohlen (Bugzilla #1483995). Das Add-on *Web-of-Trust* konnte sich ebenfalls lange als angebliches Security Add-on verkaufen bevor man entdeckte, dass mit diesem Add-on massenweise Daten gesammelt wurden.[39]

Man sollte Add-ons nicht wahllos aufgrund irgendwelcher Empfehlungen installieren, die nicht nachvollziehbar sind. Konzeptloses Zusammenwürfeln von irgendwelchen Privacy Add-on, wie es Mozilla z. B. im Blogartikel *Make your Firefox browser a privacy superpower with these extensions*[40] empfiehlt, ist kein guter, sinnvoller Ansatz. Deshalb kann man den Contextual Feature Recommender abzuschalten, um nicht belästigt zu werden.

In den Einstellungen findet man die Option im Bereich *Allgemein* unter *Browsing* (Abb. 4.11). Unter *about:config* kann man folgende Variablen setzen:

[39] https://www.tagesschau.de/inland/tracker-online-103.html
[40] https://blog.mozilla.org/firefox/make-your-firefox-browser-a-privacy-superpower-with-these-extensions/

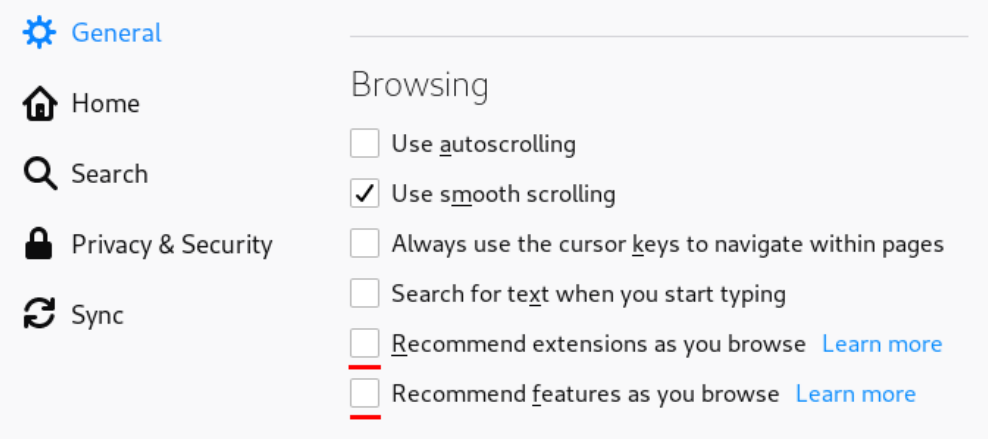


Abbildung 4.11: Contextual Feature Recommender (CFR) deaktivieren

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

Außerdem werden in der Add-on Verwaltung von Firefox Empfehlungen angezeigt, die den Nutzer zur Installation verführen sollen. Die Empfehlungen werden als iFrame von einem Mozilla Server geladen und als erstes beim Aufruf der Add-on Verwaltung angezeigt. Diese Empfehlungen kann man mit folgenden Einstellungen unter *about:config* abschalten und die Add-on Verwaltung von Firefox sieht dann wieder viel übersichtlicher aus:

```
extensions.htmlaboutaddons.recommendations.enabled  = false
extensions.htmlaboutaddons.discover.enabled         = false
extensions.ui.lastCategory                          = addons://list/extension
```

4.11 History Sniffing

Browser speichern Informationen über besuchte Webseiten in einer Surf-History. Eine empirische Untersuchung der University of California [41] zeigt, dass ca. 1% der Top 50.000 Websites versuchen, diese Daten über zuvor besuchte Websites auszulesen. Daneben gab es spezielle Anbieter wie Tealium oder Beencounter, die einem Webmaster in Echtzeit eine Liste der Websites liefern, die ein Surfer zuvor besucht hat. Die dabei übermittelten Informationen erlauben ein ähnlich detailliertes Interessenprofil zu erstellen, wie das Tracking über viele Websites. In der Regel werden die Informationen für die Auswahl passender Werbung genutzt.

Ein Experiment des Isec Forschungslabors für IT-Sicherheit [42] zeigt, dass diese History-Daten auch zur Deanonymisierung genutzt werden können. Anhand der Browser History wurde ermittelt, welche Gruppen bei Xing der Surfer bisher besucht hat. Da es kaum zwei Nutzer gibt, die zu den gleichen Gruppen gehören, konnte mit diesen Daten eine Deanonymiserung erfolgen. Die Realnamen sowie E-Mail Adressen konnten ohne Mithilfe der Surfer ermittelt werden.

In der Regel wurde der Besuch von Webseiten in der Vergangenheit durch Auswertung der Formatierung von Links ermittelt. Im Browser werden Links zu bereits besuchten Webseiten anders dargestellt, als unbekannte Webseiten. Deshalb wurde die folgende Option eingeführt, mit der man die abweichende Formatierung von besuchten Links verhindert:

```
layout.css.visited_links_enabled = false
```

[41] http://cseweb.ucsd.edu/users/lerner/papers/ccs10-jsc.pdf
[42] http://www.iseclab.org/papers/sonda-TR.pdf

Seit 2013 ist Firefox standardmäßig robust gegen diese Trackingmethode und verhindert das Auslesen der Formatierungen für die Darstellung besuchter Webseiten. Das Deaktivieren der Formatierung von besuchten Links ist daher als Verteidigung gegen Tracking nicht mehr nötig, kann aber Peinlichkeiten vor dem Bildschirm vermeiden.

Es wurde andere Angriffe auf die Surfhistory entwickelt (z. B. Timing Attacks). Die einzig wirksame Verteidigung besteht in der Deaktivierung der Surf-History.

```
privacy.history.custom = true
places.history.enabled = false
```

Außerdem können Webseiten in einem Tab die Anzahl der zuvor besucht Webseiten auslesen. Aufgrund eines Bug in Firefox 63+ kann man es nicht verhinden. Die Werte für die Variable *browser.sessionhistory.max_entries* werden ignoriert.[43]

4.12 Browsercache und Chronik

Mit jeder aufgerufenen Webseite wird ein ETag gesendet, welches der Browser zusammen mit den Daten der Webseite (HTML, Bilder, JS) im Cache speichert. Wird die Webseite erneut aufgerufen, sendet der Browser zuerst nur das ETag an den Webserver, um zu erfragen, ob sich die Webseite geändert hat. Wenn der Server antwortet, dass für dieses ETag keine Änderungen vorliegen, dann verwendet der Browser die Daten aus dem Cache um muss sie nicht neu laden.

Das ETag kann eine eindeutige User-ID enthalten, die zum Tracking verwendet werden kann. KISSmetrics verwendete diese Technik bereits 2011, um gelöschte Trackingcookies wieder herzustellen.[44]

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

Abbildung 4.12: Cache löschen beim Beenden

[43] https://bugzilla.mozilla.org/show_bug.cgi?id=1511813
[44] https://heise.de/-1288914

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

```
privacy.sanitize.sanitizeOnShutdown   = true
privacy.clearOnShutdown.cache         = true
privacy.clearOnShutdown.cookies       = true
privacy.clearOnShutdown.downloads     = true
privacy.clearOnShutdown.formdata      = true
privacy.clearOnShutdown.history       = true
privacy.clearOnShutdown.offlineApps   = true
privacy.clearOnShutdown.sessions      = true
privacy.clearOnShutdown.siteSettings  = true oder false
privacy.clearOnShutdown.openWindows   = false
```

Die erste Option aktiviert das Löschen der Chronik beim Schließen des Browsers. Die weiteren Parameter legen fest, welche Werte gelöscht werden sollen. *openWindows* sollte man auf FALSE setzen, da sonst evtl. immer zwei Instanzen des Browsers gestartet werden. Bei den *siteSettings* kann man überlegen, ob man alle Cookie Freigaben löschen möchte und gegen HSTS-Cookies geschützt sein möchte, oder ob man die Cookie Freigaben für ausgewählte Webseiten aus Bequemlichkeit lieber behält.

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

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

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

4.13 Referer

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

Die Studie *Privacy leakage vs. Protection measures* [45] zeigt, dass außerdem viele Webseiten private Informationen via Referer an Trackingdienste übertragen. Das folgende Beispiel zeigt den Aufruf eines Werbebanners nach dem Login auf der Webseite http://sports.com

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

Mit einer eindeutigen UserID (im Beispiel ein Tracking-Cookie) kann das Surfverhalten über viele Webseiten verfolgt werden. Durch zusätzliche Informationen (im Beispiel eine E-Mail Adresse) werden die gesammelten Datensätze personalisiert. Im Rahmen der Studie wurde 120 populäre Webseiten untersucht. 56% der Webseiten sendeten nach dem Login private Informationen wie E-Mail Adresse, Name oder Wohnort an Trackingdienste.

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

[45] http://w2spconf.com/2011/papers/privacyVsProtection.pdf

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

Mit dieser Einstellung werden Subdomains als Drittseiten behandelt und es wird auch an Subdomains kein Referer gesendet. Das schützt somit auch gegen Trackingdienste, die sich mit DNS-Aliases als Subdomains auf populären Webseiten einschleichen (z. B. WebTrekk bei Heise.de und Zeit.de). Allerdings bringt es möglicherweise vereinzelt Probleme bei einigen Websites mit sich. Wer diese Probleme minimieren möchte, kann folgende Option setzen:

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

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

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

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

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

4.14 Risiko Plugins

Für die Darstellung von Inhalten, die nicht im HTML-Standard definiert sind, kann Firefox Plug-ins nutzen. Sie werden in der Add-on Verwaltung in der Sektion PPluginsäktiviert. Um zu verhindern, das bei der Installation von irgendwelchen Softwarepaketen ungewollt Browser Plug-ins automatisch aktiviert werden, kann man folgende Variable unter *about:config* setzen:

```
plugin.default.state = 0
```

Um unter Windows das automatische Scannen der Registry nach neuen Plug-ins zu deaktivieren, ist unter *about:config* folgende Variable zu setzen:

```
plugin.scan.plid.all = false
```

4.14.1 Media Plug-ins für Video und Audio

Die Einstellungen zum Deaktivieren des automatischen Abspielens von Audio und Video hat Mozilla immer wieder geändert. Mit folgenden Einstellungen unter *about:config* deaktiviert man das automatische Abspielen von Videos und Audio:

```
media.autoplay.default         = 5
media.autoplay.blocking_policy = 2
```

Das Deaktivieren des automatischen Abspielens von Videos ist auch ein Sicherheitsfeature, das den Start eines bösartigen Videos im Hintergrund verhindert und die Angriffsfläche für Drive-by-Download Angriffe verringert.

Für einige Video- und Audioformate verwendet Firefox externe Plug-ins zum abspielen. Standardmäßig werden von Firefox zwei Media Plug-ins verwaltet:

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

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

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

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

Widevine Content Decryption Module von Google zur Wiedergabe von DRM geschützten Videos ist unter Windows standardmäßig aktiviert, bei den meisten Linux Distributionen aber standardmäßig deaktiviert. Man braucht es nicht notwendigerweise. Mit folgendem Wert unter *about:config* kann man es komplett deinstallieren:

```
media.eme.enabled = false
```

Damit es auch nicht in den Einstellungen als aktivierbare Option erscheint, kann man die Konfigurationsoption verstecken:

```
browser.eme.ui.enabled = false
```

4.14.2 Anzeige von PDF Dokumenten

Adobes Acrobat Plug-ins für die Anzeige von PDF-Dokumenten im Browser war über viele Jahre ein erhebliches Sicherheitsrisiko. 2008 gelang es dem *Ghostnet*, mit bösartigen PDF Dokumenten die Computernetze westlicher Regierungen, der US-Regierung und des Dalai Lama zu infizieren, dem Trojaner *MiniDuke* gelang es 2012, mit bösartigen PDFs in die Computer von Regierungsorganisationen in Deutschland, Israel, Russland, Belgien, Irland, Großbritannien, Portugal, Rumänien, Tschechien und der Ukraine einzudringen, und der Wurm *Win32/Auraax* wurde ebenfalls mit bösartigen PDF-Dokumenten verteilt.

Aktuelle Firefox Versionen verwenden die JavaScript Bibliothek **PDF.js** für die Anzeige von PDF-Dokumenten. Auch diese Bibliothek hatte schon kritische Sicherheitslücken, die von Angreifern aktiv ausgenutzt wurden (z. B. CVE-2015-0802, CVE-2015-0816 oder CVE-2015-4495). Für hohe Sicherheitsanforderungen kann man die Anzeige von PDF-Dokumenten im Browser deaktivieren und damit die Angriffsfläche für Drive-By-Download Angriffe verringern:

```
pdfjs.disabled = true
```

Statt funktionsüberladener Monster-Applikationen kann man einfache PDF-Reader nutzen, die sich auf die wesentliche Funktion des Anzeigens von PDF-Dokumenten beschränken. Die FSFE stellt auf PDFreaders.org[46] Open Source Alternativen vor.

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

Die Linux Distribution **QubesOS** bietet für potentielle *Landesverräter* und andere Risikogruppen, die als Target für den Einsatz der neuen Bundestrojaner in Frage kommen, einige besondere Sicherheitsfeatures. Dazu gehört die Anzeige von PDFs in einer Wegwerf-VM oder die Umwandlung von PDF Dokumenten aus unbekannten Quellen in Trusted PDFs, die man risikolos weitergeben kann. Die Funktionen kann man nach dem Download mit einem Rechtsklick auf ein PDF Dokument im Dateimanager aufrufen.

Für die Umwandlung in Trusted PDFs wird *qubes-app-linix-pdf-converter*[47] gestartet, das Rendering des (möglicherweise bösartigen) PDF Dokumentes erfolgt in einer Wegwerf-VM, die danach gelöscht wird. Die gerenderten Bitmaps werden zu einem neuen, ganz harmlosen PDF zusammengesetzt. Wie bei QubesOS üblich, dauert der Vorgang insbesondere bei großen PDF Dokumenten einige Zeit. (Eile ist ein Feind der Sicherheit!)

[46] http://www.pdfreaders.org/index.de.html
[47] https://github.com/QubesOS/qubes-app-linx-pdf-converter

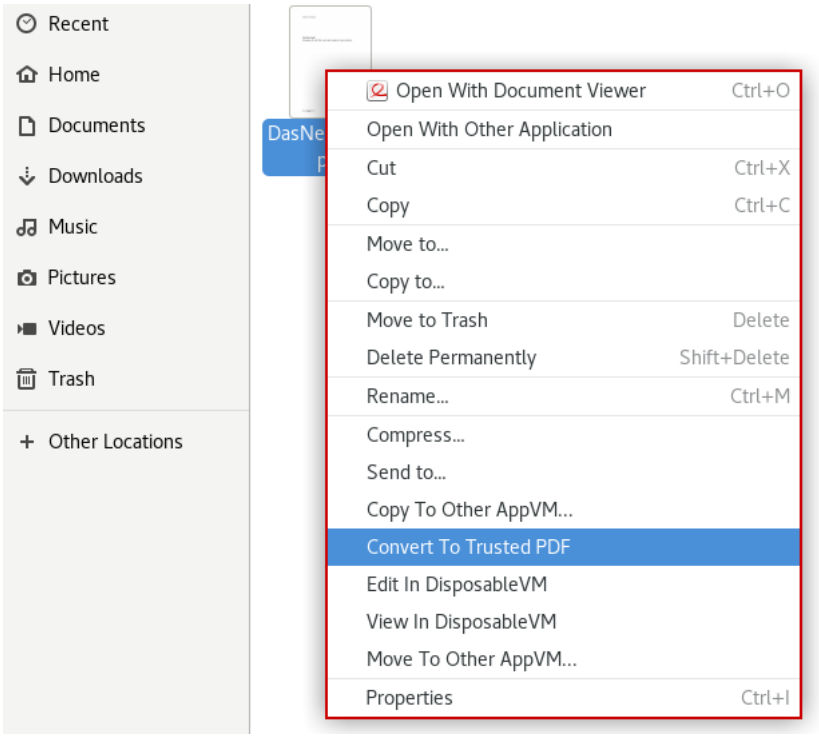


Abbildung 4.13: Konvertierung von PDFs im Dateimanager in QubesOS

4.15 HTTPS-Verschlüsselung erzwingen und härten

Viele Websites bieten inzwischen HTTPS-Verschlüsselung an. Diese sichere Datenübertragung wird häufig nicht genutzt, obwohl es möglich wäre. Mit wenig Aufwand lässt sich die Nutzung von HTTPS für Websites erzwingen, die diese Option anbieten.

Oft gibt man aus Faulheit in der URL Leiste des Browsers nur *www.privacy-handbuch.de* ein oder noch einfacher *privacy-handbuch.de*. Daraufhin sendet der Browser einen einfachen HTTP Request an den Webserver. Gut konfigurierte Webserver antworten mit einem 301 Status und schicken den Surfer auf die HTTPS verschlüsselte Webseite, aber das ist nicht immer der Fall. Außerdem ist der unverschlüsselte Request überflüssig.

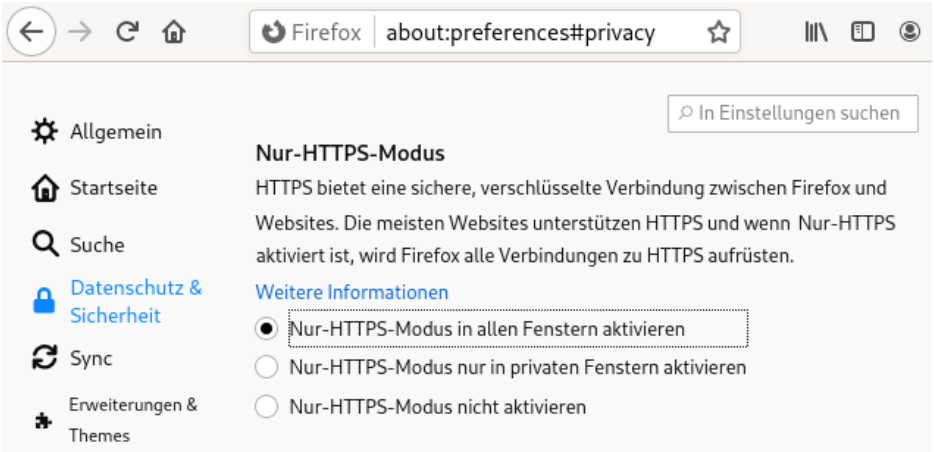


Abbildung 4.14: Nur-HTTPS-Mode in Firefox 83+ aktivieren

Firefox bietet den Nur-HTTPS-Modus, bei dem Webseiten immer via HTTPS aufgerufen werden. Firefox Release und ESR Version unterscheiden sich in der Konfiguration:

- Bei Firefox 83+ kann man den Nur-HTTPS-Modus (bzw. https-only-mode) in den Einstellungen in der Sektion *Datenschutz und Sicherheit* aktivieren (Abb: 4.14).
- Im Firefox 78.x ESR muss man unter *about:config* folgenden Wert setzen:

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

- Wenn keine HTTPS Verbindung möglich ist, dann wird eine Warnung angezeigt und man kann mit einem Klick die unverschlüsselte HTTP Seite aufrufen (Abb: 4.15).

  Die Konfiguration des Routers ist somit problemlos möglich, nur ein Klick mehr.

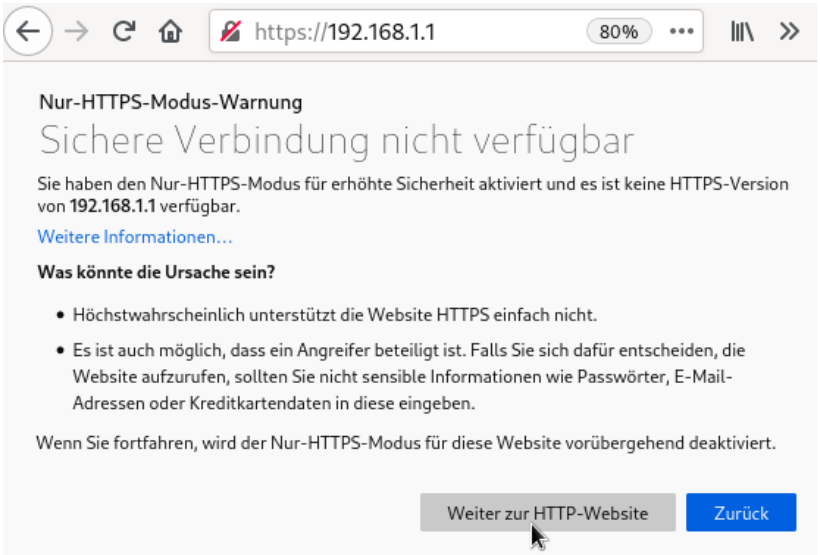


Abbildung 4.15: Warnung bei Aufruf einer unverschlüsselten HTTP Seite

- Für lokale Verbindungen zum eigenen Rechner wird kein HTTPS erzwungen. Man kann z. B. den Druckserver CUPS (Linux) wie gewohnt im Browser administrieren.

  Wenn man auch für http://localhost oder http://127.0.0.1 ein Upgrade auf HTTPS erzwingen möchte, könnte man folgenden Wert setzen (aber warum?):

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

- Neben HTTP unterstützt Firefox auch noch das FTP-Protokoll aus …Gründen. Für FTP erfolgt kein(!) Upgrade auf TLS im Nur-HTTPS-Modus. Um unsichere FTP Verbindungen auszuschließen, muss man es komplett deaktivieren:

  ```
  network.ftp.enabled = false
  ```

- Downloads über unsichere Verbindungen kann Firefox 80+ blockieren. Webseiten können via HTTP aufgerufen werden (im Nur-HTTPS-Modus nach Bestätigen der Warnung). Aber Downloads, die man auf der Festplatte speichert, sollten immer via HTTPS geladen werden. Unsichere Downloads blockiert man mit der Option:

  ```
  dom.block_download_insecure = true
  ```

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

- Mixed Content nennt man die Elemente in HTTPS Webseiten, welche über einen unverschlüsselten HTTP Link referenziert werde. Mit folgender Option erzwingt das Upgrade auf HTTPS auch für alle Inhalte der Webseite wie Bilder, Fonts, usw.

  ```
  security.mixed_content.upgrade_display_content = true
  ```

  Das Laden von aktiven Inhalten wie Javascript via unverschlüsseltem HTTP ist beim Aufruf von Webseiten via HTTPS standardmäßig verboten.

- Insecure Renegotiation wird seit 2009 als schwerwiegender Bug des SSL-Protokoll eingestuft. Tools zum Ausnutzen der Insecure Renegotiation gibt es auch als Open-Source (z. B. dsniff). Deshalb sollte man es verbieten:

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

- Certifikate Pinning schützt gegen Man-in-the-Middle Angriffe. Mit folgender Option wird für eine populäre Webseiten wie Google, Youtube, Twitter, TorProject, Dropbox u.a. ein TLS verschlüsselte Verbindung nur dann akzeptiert, wenn das Zertifikat des Servers von einer CA signiert wurde, die im Code von Firefox festgeschrieben ist:

  ```
  security.cert_pinning.enforcement_level  = 2
  ```

  Wenn einige Webseiten mit dieser Einstellung nicht aufrufbar sind, dann sitzt ein Man-in-the-Middle in der TLS-Verschlüsselung (das kann z. B. ein Virenscanner sein).

- Weitere Add-ons wie **HTTPSEverywhere** oder **HTTPZ** sind damit überflüssig.

4.15.1 Anzeige der HTTPS Verschlüsselung

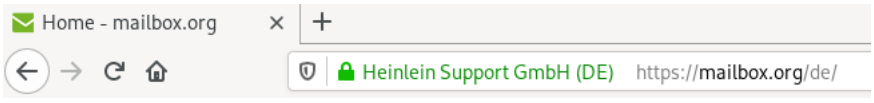
Standardmäßig zeigt Firefox 70+ einen HTTPS-verschlüsselten Transport der Daten nur mit einem kleinen, unscheinbar grauen Icon neben der Adresse an:

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

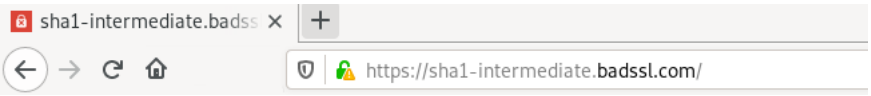
```
security.secure_connection_icon_color_gray = false
```

Neben einfachen SSL-Zertifikaten gibt *Extended Validation Certificates*, bei denen die Certification Authority (CA) die Identität des Inhabers aufwendiger prüft, bevor ein Zertifikat ausgestellt wird. Firefox 70+ zeigt keinen Hinweis mehr bei EV-Zertifikaten an. Wenn man die Sicherheitsinformation zum verifizierten Inhaber des SSL-Zertifikates wieder sehen möchte, muss man folgende Optionen unter *about:config* aktivieren:

```
security.identityblock.show_extended_validation  = true
security.OCSP.enabled                            = 1
```



Auf der Webseite https://badssl.com kann man sich anschauen, wie Firefox bei Problemen in der HTTPS Verschlüsselung reagiert. Wenn man eine unsichere Verschlüsselung aktzeptiert hat, zeigt Firefox ein kleines, gelbes Warndreick neben dem Schloss-Symbol. Diese Warnung sollte man nicht ignorieren:



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

```
security.insecure_connection_icon.enabled         = true
security.insecure_connection_icon.pbmode.enabled  = true
```

Die Anzeige eines Warn-Textes neben der URL aktiviert man mit:

```
security.insecure_connection_text.enabled         = true
security.insecure_connection_text.pbmode.enabled  = true
```

Beide Optionen können auch kombiniert werden, das sieht dann so aus:

4.15.2 Vertrauenswürdigkeit von HTTPS

IT-Sicherheitsforscher der EFF kamen breits 2009 in einer wiss. Arbeit zu dem Schluss, dass Geheimdienste mit gültigen SSL-Zertifikaten schwer erkennbare man-in-the-middle Angriffe durchführen können. Diese Angriffe können routiniert ausgeführt werden.[48]

> *Certificate-based attacks are a concern all over the world, including in the U.S., since governments everywhere are eagerly adopting spying technology to eavesdrop on the public. Vendors of this technology seem to suggest the attacks can be done routinely.*

Anbieter von fertige Appliances für diesen auch als *Lawful SSL Interception* bezeichneten Angriff findet man beim Stöbern in den SpyFiles von Wikileaks. Für staatliche Schnüffler gibt es mehrere Möglichkeiten, um diese Technik mit gültigen SSL-Zertifikate für schwer erkennbare man-in-the-middle Angriffe zu kombinieren:

1. Für einen großflächiger Angriff gegen iranische Internet Nutzer wurden im August 2011 mehrere CAs gehackt, um gültige SSL-Zertifikate zu erstellen (DigiNotar, Comodo, InstantSSL und zwei Sub-Registrare von Comodo). Bei DigiNotar wurden 531 Zertifikate kompromittiert. Neben den Webseiten von Google, Yahoo, Mozilla, Skype, TorProject.org u.a. waren auch die Webdienste von MI6, CIA und Mossad betroffen.

2. Certification Authorities könnten unter Druck gesetzt werden, um staatlichen Stellen SubCA-Zertifikate auszustellen, mit denen die Zertifikate für man-in-the-middle Angriffe signiert werden könnten. Ein Kommentar zum TürkTRUST Desaster:

   > *I think you will see more and more events like this, where a CA under pressure from a government will behave in strange ways. (A. Shamir)*

   Im Juni 2014 signierte die staatliche indische Certification Authority (NIC) gefälschte SSL-Zertifikate für Google Dienste und Yahoo!. 45 gefakte Zertifikate wurden nachgewiesen. Ob es um eine staatliche Überwachung, einen Hackerangriff oder einen Konfigurationsfehler(?) handelt, ist unklar.[49]

3. Die Anbieter von Webdiensten können zur Herausgabe der eigenen Zertifikate und Keys gezwungen werden, wie am Beispiel des E-Mail Providers Lavabit bekannt wurde. Die betroffenen Provider sind zum Stillschweigen verpflichtet. Der Angreifer kann mit diesen Zertifikate einen Angriff auf die SSL-Verschlüsselung durchführen, der nicht mehr erkennbar ist.

[48] https://eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl
[49] https://www.heise.de/-2255992

4. Verisign ist nicht nur die größte Certification Authority. Die Abteilung NetDiscovery von Verisign ist ein Global Player in der Überwachungstechnik und unterstützt die Behörden und westliche Geheimdienste seit 2002 bei der SSL Interception.

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

Die Software für einen man-in-the-middle Angriff mit den gefälschten Zertifikaten gibt es auch als Open Source, z. B. den *mitm-proxy*[50] der Stanford University oder *dsniff*[51].

4.15.3 SSL-Zertifikate via OCSP validieren

Das Online Certificate Status Protocol (OCSP) sollte eine Überprüfung der SSL-Zertifikate ermöglichen. Bevor der Browser eine SSL-Verbindung akzeptiert, fragt er bei der Certification Authority nach, ob das verwendete Zertifikat für diesen Server noch gültig ist. Um SSL-Zertifikate via OCSP zu verifizieren, wurden zwei Verfahren definiert:

OCSP Server sind eine veraltete Technik und leicht auszutricksen, wie Moxie Marlinspike in dem Paper *Defeating OCSP With The Character 3* (2009) gezeigt hat. Gängige Tools für Man-in-the-middle Angriffe wie *sslsniff*[52] können das automatisiert ausführen. Die Validierung via OCSP Server bringt kaum Sicherheitsgewinn.[53]

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

```
POST http://ocsp2.globalsign.com/gsorganizationvalg2 HTTP/1.1
Host: ocsp2.globalsign.com
User-Agent: Mozilla/5.0 (...) Gecko/20130626 Firefox/17.0 Iceweasel/17.0.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
Content-Length: 117
Content-Type: application/ocsp-request
Cookie: __cfduid=57a288498324f76b1d1373918358
```

Auch wenn aktuelle Firefox Versionen keine Cookies von OCSP.Get Antworten mehr akzeptieren, erhält die Certification Authority (CA) laufend Informationen, von welcher IP-Adresse die SSL-geschützten Webseiten bzw. Mailserver o.ä. kontaktiert wurden. Da die OCSP-Anfrage und Antworten unverschlüsselt übertragen werden, kann auch ein *Lauscher am Draht* diese Informationen abgreifen. Aus Privacy Gründen kann man die Validierung via OCSP Server deaktivieren

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

Wenn man die Validierung von SSL-Zertifikaten via OCSP-Server als Sicherheitsfeature nutzen möchte (damit beispielsweise Extended Validation Informationen der

[50] http://crypto.stanford.edu/ssl-mitm/
[51] http://www.monkey.org/ dugsong/dsniff/
[52] https://moxie.org/software/sslsniff
[53] https://www.thoughtcrime.org/papers/ocsp-attack.pdf

Zertifikate angezeigt werden), dann muss man auch darauf bestehen, dass das Ergebnis geliefert und ausgewertet wird. Anderenfalls ist es als Sicherheitsfeature unbrauchbar. Diese verschärfte OCSP Validierung aktiviert man unter *about:config* mit:

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

Da es keine klare Empfehlung für eine Abschaltung oder verschärfte Durchsetzung von OCSP gibt, enthalten unsere user.js Konfiguration in der Zusammenfassung keine Vorgaben. Der Anwender möge selbst entscheiden. Die Standardeinstellung von Firefox mit aktiviertem OCSP aber ohne eine Auswertung zu erzwingen, vereint aber die Nachteile von beiden Varianten.

OCSP.Stapling ist ein modernes Verfahren, dass die oben genannten Probleme vermeidet. Der Browser ruft ein Token vom Webserver ab, das die Gültigkeit des Zertifikates für einen kurzen Zeitraum bestätigt und von der CA signiert wurde.

Moderne Webserver und alle aktuellen Browser unterstützen es inzwischen. Der bekannte Test für Webserver Qualsys SSL Labs wird ab Jan. 2017 die Bestnote A+ nur vergeben, wenn der Webserver OCSP.Stapling anbietet. Die BSI Richtlinie TR-03116-4 (Kryptografische Vorgaben für TLS, S/MIME, OpenPGP und SAML) fordert ebenfalls Support für OCSP.Stapling.

Firefox ist sinnvoll vorkonfiguriert. Es wird standardmäßig OCSP.Stapling genutzt, wie man unter *about:config* überprüfen kann:

```
security.ssl.enable_ocsp_stapling     = true
security.ssl.enable_ocsp_must_staple  = true
```

4.15.4 Tracking via SSL Session

Beim Aufbau einer verschlüsselten HTTPS-Verbindung zwischen Browser und Webserver wird eine sogenannte Session initialisert. Diese Session kann für 48h genutzt werden. Das beschleunigt das Laden der Webseite bei erneutem Zugriff, da die Details der Verschlüsselung nicht jedes mal neu zwischen Browser und Webserver ausgehandelt werden müssen. Da diese Session eindeutig ist, kann sie für das Tracking genutzt werden. Das Verfahren ist im RFC 5077 [54] beschrieben.

Die SSL-Session-ID kann von nahezu allen Webserven für das Tracking der Zugriffe genutzt werden. IBM WebSphere, Apache und andere bieten eine API für den Zugriff auf die SSL Session-ID. Einige Webshops sind für das Tracking via SSL Session-ID vorbereitet (z. B. die *xtcModified eCommerce Shopsoftware*[55]). Dieses Tracking-Verfahren ist so gut wie nicht nachweisbar, da es vollständig durch den Webserver realisiert wird und keine Spuren im Browser hinterlässt.

In Firefox ist der SSL Session Cache in den Surf-Containern gekapselt. Unser Konzept aktiviert folgende Schutzmaßnahmen gegen das Tracking:

- FirstParty.Isolation verhindert das webseite-übergreifende Tracking.
- Löschen von Cache und SiteSettings beim Schließen des Browsers verhindert das langfristige Tracking über einen längeren Zeitraum.

Dieser Schutzlevel entspricht somit dem von uns angestrebten Schutz gegen Tracking mit Cookies/EverCookie ohne das Surfen durch ständig neues Aushandeln der SSL Sessions zu verlangsamen.

[54] https://tools.ietf.org/html/rfc5077
[55] http://www.modified-shop.org/wiki/SESSION_CHECK_SSL_SESSION_ID

4.15.5 Tracking via HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) wurde als Schutz gegen den *ssl-stripe* Angriff eingeführt, den Moxie Marlinspike auf der Black Hack 2009 vorstellte. Der Angriff wurde beispielsweise 2012 von mehreren Bad Tor Exit Nodes aktiv genutzt.

Als Schutz gegen *ssl-stripe* Angriffe sendet der Webserver beim Aufruf einer Webseite einen zusätzlichen HSTS-Header, um dem Browser mitzuteilen, dass diese Website für eine bestimmte Zeit immer via HTTPS aufgerufen werden soll. Außerdem enthält Firefox die *HSTS Preload List* mit mehr als 1.000 Webseiten, die nur via HTTPS aufgerufen werden dürfen. Das verhindert einen Downgrade auf unverschlüsselte HTTP-Verbindungen.

S. Greenhalgh hat ein Verfahren publiziert, wie man HSTS für das Tracking von Surfern verwenden kann[56]. Entwickler bei Apple haben im März 2018 beobachtet, dass dieses Verfahren in-the-wild eingesetzt wird, veröffentlichten aber keine Details. Sie schlagen eine Modifikation des Standards vor, um Tracking via HSTS Cookies zu verhindern.[57]

Ob man HSTS im Browser deaktiviert und sich nur auf die *HSTS Preload List* verlässt, um sich gegen ein Trackingverfahren zu schützen, oder ob man HSTS aktiviert, um sich gegen *ssl-stripe* Angriffe zu schützen (Standard im Firefox), ist also eine Wahl zwischen Skylla und Charybdis. Überlegungen dazu:

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

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

  Damit werden beim Schließen des Browsers alle gespeicherten HSTS-Werte gelöscht und ein langfristiges Tracking wird verhindert. Während einer Surf-Session ist der HSTS-Schutz aktiv.
- Innerhalb einer Surf-Session kann man HSTS-Cookies mit der Tastenkombination STRG-SHIFT-ENTF löschen. Zum Löschen der HSTS-Werte ist unter Details die Option *Website-Einstellungen* zu aktivieren.

4.15.6 SSL/TLS Konfiguration

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

1. Das Protokoll SSLv3 ist geknackt. Mozilla hat SSLv3 in Firefox 34 standardmäßig abgeschaltet.
2. Die RC4-Cipher sind schwach und genügen aktuellen Anforderungen nicht mehr. Laut Empfehlung der IETF (RFC 7465) darf RC4 nicht mehr für die Verschlüsselung genutzt werden und ist in Firefox seit Version 44 deaktiviert.
3. Für die 3DES-Verschlüsselung gibt es mit der Birthday Attack einen plausiblen Angriff der allerdings im Moment noch große Datenmengen > 32GB erfordert. Diese Cipher sollten aber ebenfalls deaktiviert werden. Krypto-Experten empfehlen, 3DES wie RC4 zu behandeln und in den Standards die Nutzung zu verbieten.

[56] http://heise.de/-2511258
[57] https://heise.de/-3998754

4. Beim Diffie-Hellman-Schlüsseltausch kann der Admin viele Fehler bei der Konfiguration des Webservers machen. Auf der Webseite https://badssl.com kann man ausprobieren, dass Firefox diese Schwächen nicht erkennt und schwache DH-Parameter für den Schlüsseltausch aktzeptiert. Außerdem muss man davon ausgehen, dass die NSA die Common DH Primes lt. RFC 2409 bis 1024 Bit geknackt hat.[58]

5. Insecure Renegotiation wird seit 2009 als schwiegender Bug des SSL-Protokoll eingestuft. Tools zum Ausnutzen der Insecure Renegotiation gibt es auch als Open-Source (z. B. dsniff). Ein Angreifer kann Login Credentials stehlen ohne die SSL-Verschlüsselung knacken zu müssen.

6. SHA sollte laut Empfehlung der IETF nicht mehr als Signaturalgorithmus für die Beglaubigung von Zertifikaten verwendet werden. Die CAs haben inzwischen fast alles umgestellt.

7. Eine SSL-verschlüsselte Webseite sollte nur SSL-verschlüsselte Inhalte darstellen. Unverschlüsselte Elemente sollten nicht geladen werden, um die Sicherheit nicht zu kompromittieren. Firefox blockiert unverschlüsselte aktive Inhalte, lässt Bilder aber zu.

8. FIPS-kompatible Cipher sind per Design schwach ausgelegt und in Firefox standardmäßig deaktiviert.

Tracking Risiko durch seltsame Auswahl der SSL/TLS Cipher

Wenn der Browser eine SSL-verschlüsselte Verbindung zu einem Webserver aufbauen will, dann sendet er Liste der unterstützten TLS-Features, Cipher und der nutzbaren elliptischen Kurven für EC-Crypto. Die Reihenfolge und der Inhalt der Listen ist unterschiedlich für verschiedene Browser und Browser Versionen.

- Firefox 53 sendet beispielsweise:

```
<e name='Firefox/53.0' protocol='771' extTypes='21 23 65281 10 11 16 5 18 40 43 13'
suites='4865 4867 4866 49195 49199 52393 52392 49196 49200 49171 49172 51 53'
curves='29 23 24 25 256 257' points='AA==' compress='AA=='/>
```

- Google Chrome sendet:

```
<e name='Chrome/57.0.2951.0' protocol='771' greateExt='1' extTypes='65281 0 23 35
13 5 18 16 30032 11 40 45 43 10 21' greaseSuite='1'
suites='4865 4866 4867 49195 49199 49196 49200 52393 52392 52244 52243 49171 49172
156 157 47 53 10' greaseCurves='1' curves='29 23 24' points='AA==' compress='AA=='/>
```

Das sieht etwas kryptisch aus, man kann sich auf verschiedenen Webseite aber auch anzeigen lassen, was es bedeutet.

Wenn man an den SSL-Ciphern rumspielt und schwache Cipher deaktiviert, kreiert man möglicherweise ein individuelles Erkennungsmerkmal anhand dessen man beim Aufruf einer verschlüsselten Webseite wiedererkennbar ist. Deshalb empfehlen wir keine Manipulationen an den verwendeten Ciphern. Besser ist es, einen aktuellen Firefox bzw. Firefox ESR zu verwenden und es bei den Einstellungen der Entwickler zu belassen.

4.16 Installierte Schriftarten verstecken

Informationen über installierte Schriftarten können mit JavaScript, Flash oder Java ausgelesen und zur Berechnung eines individuellen Fingerprint des Browsers genutzt werden. Viele Trackingdienste nutzen inzwischen diese Technik. Die Studie *Dusting the web for*

[58] https://freedom-to-tinker.com/blog/haldermanheninger/how-is-nsa-breaking-so-much-crypto

fingerprinters[59] der KU Leuven (2013) kommt zu den Schluss, dass mindestens 0,5 - 1,0% der Webseiten die installierten Schriftarten für Trackingzwecke auslesen.

Der Download von (exotischen) Schriftarten wird auch von Google zum Tracking genutzt. Viele Webdesigner nutzen Schriften vom Google Font Service. Für den Designer ist die Einbindung der Fonts einfach.

1. Der Webdesigner muss nur ein kleines CSS-Stylesheet importieren. Um die Schriftart OpenSans zu nutzen, reicht folgende Zeile:

```
<link href='https://fonts.googleapis.com/css?family=Open+Sans'
      rel='stylesheet' type='text/css'>
```

2. Beim Aufruf der Webseite lädt der Browser das Stylesheet vom Server *fonts.googleapis.com*. Das Stylesheet enthält die Links zum Download der Fonts.

3. Der Browser holt sich dann die Dateien mit Schriftarten vom Server *fonts.gstatic.com* und zeigt die Webseite an. Die Font Dateien werden für 24h im Cache gespeichert.

Für das Laden von Schriftarten vom Google Font Service gelten die Datenschutzbestimmung von Google[60]. Viele Webseiten weisen in Ihren Privacy Statements aber nicht darauf hin, dass beim Aufruf der Webseite Daten bei Google gespeichert und verarbeitet werden. Wenn man ein Smartphone nutzt, werden bei Google z. B. die Telefonnummer und andere eindeutige Geräte-IDs mit dem Aufruf der Webseite verknüpft.

Das Laden von Schriftarten aus dem Internet ist außerdem ein Sicherheitsrisiko, weil damit Angriffe direkt auf das Betriebssystem möglich werden. Bugs in den Font Rendering Bibliotheken, die Remote Code Execution auf Systemlevel durch Laden von bösartigen Schriften erlaubten, gab es für Windows (ms11-087, ms15-078), Linux (CVE-2010-3855) oder OpenBSD (CVE-2013-6462). Der Bug ms15-078 wurde von der Firma Hacking Team zur Installation eines Überwachungstrojaners genutzt. Das Google Security Team hat zwischen 2015 und 2017 mit der Code Fuzzing Software *BrokenType* weitere 40 Bugs im Windows Kernel und Font Rendering gefunden, die ein Angreifer nutzen konnte, um mit bösartigen Fonts den Rechner anzugreifen und Code mit Systemrechten auszuführen.[61]

Blockieren externer Schriftarten mit Add-ons?

Einige Firefox Add-ons wie uBlock Origin oder uMatrix können mit einer Option den Download von zusätzlichen Schriftarten blockieren. Dabei gibt es folgende Nachteile:

1. Es wird beim Google Fonts Service nur der zweite Schritt blockiert. Das Stylesheet wird trotzdem von Google geladen. Wenn man keine Fonts von Google verwenden möchte, dann sollte man *fonts.googleapis.com* mit einer Filterregel blockieren.

2. Die Add-ons können nicht zwischen Fonts für eine hübsche Schrift (entbehrlich) und notwendigen Fonts für die Darstellung von Icons für die Navigation unterscheiden. Viele Webseiten werden dadurch unbrauchbar.

3. Das Blockieren des Downloads externer Schriftarten schützt nicht gegen das Auslesen lokal installierter Fonts für das Fingerprinting des Browsers.

Deshalb ist die Nutzung des Features *externe Schriftarten blockieren* in uBlock Origin oder uMatrix suboptimal und wird hier nicht empfohlen.

[59] https://www.cosic.esat.kuleuven.be/publications/article-2334.pdf
[60] https://www.google.com/intl/de/policies/privacy
[61] https://www.heise.de/-4155012

Konfiguration der Schriftarten in Firefox

Um das Laden von externen Schriftarten zu blockieren, deaktiviert man in den Einstellungen die Optionen *Webseiten das verwenden von eigenen Schriften erlauben* und die CSS Font Loading API. Damit sehen einige Webseiten nicht mehr ganz so hübsch aus, die Einschränkungen sind aber gering:

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

Das Underline Handling sollte man deaktivieren, da es zum Fingerprinting der installierten Schriftarten und zur Erkennung des Betriebssystems verwendet werden kann:

```
font.blacklist.underline_offset = "" (leerer String)
```

Immer mehr Websites verwenden Webicon Fonts für die Darstellung von Symbolen. Häufig sieht man statt der Symbole seltsame Zeichen, weil der passende Font mit den Symbolen nicht aus dem Internet geladen wird. Das Web wird damit unbenutzbar.

Um diese Probleme zu vermeiden, empfehlen wir die Freigabe von downloadbaren Schriften für die Darstellung von Symbolen für weniger strenge Sicherheitsanforderungen. Damit werden Icons wieder korrekt dargestellt:

```
gfx.downloadable_fonts.enabled   = true
```

Für hohe Sicherheitsanforderungen kann man das Rendering von OpenType SVG Fonts und die Graphite Engine deaktivieren, um die Angriffsfläche zu reduzieren. Die Graphite Engine wird nur für die verbesserte Darstellung komplexer asiatischer Schriften benötigt:

```
gfx.font_rendering.opentype_svg.enabled   = false
gfx.font_rendering.graphite.enabled       = false
```

Um die Lesbarkeit von Webseiten zu verbessern, sollten man gut lesbare Standardschriften verwenden. Unter Windows eignet sich *Arial*, unter Linux eignet sich *Liberation Sans*. Man findet die Option in den Firefox *Einstellungen* auf dem Reiter *Inhalt*. Klicken Sie auf den Button *Erweitert*, um im folgenden Dialog die Standardschriftarten zu wählen.

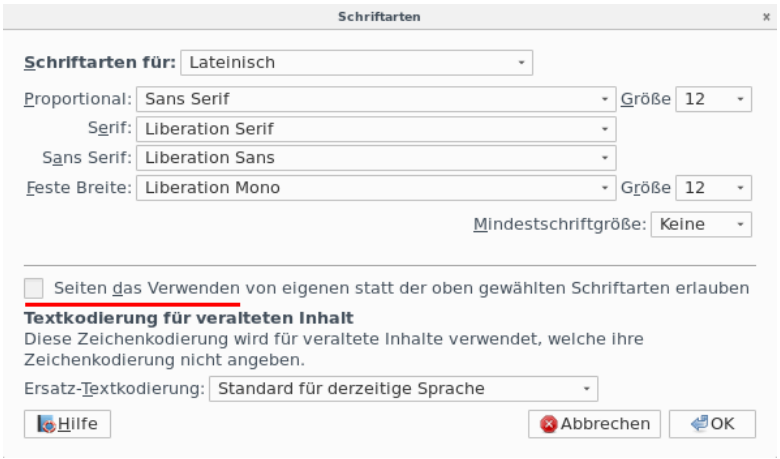


Abbildung 4.16: Schriftarten auswählen

4.17 HTML5 Canvas Elemente

Das HTML5 Canvas Element ist ein Grafikbereich auf der Webseite, in den der Browser mit JavaScript zeichnen kann. Ähnlich wie bei einem Zeichenprogramm kann man auch Text schreiben. Die Trackingbranche hat Methoden entwickelt, um diese Technologie für die Berechnung eines individuellen Fingerprinting des Browser zu nutzen.

1. Mit JavaScript kann ein Text in das Canvas Element geschrieben werden. Danach wird das Ergebnis als Grafik ausgelesen und ein Hashwert von der Grafik berechnet. Das Ergebnis unterscheidet sich von Browser zu Browser aufgrund installierter Schriften, Software für das Rendering usw. Diese Verfahren wurde 2012 in dem Paper *Perfect Pixel*[62] beschrieben und 2016 auf 14.371 Webseiten in-the-wild nachgewiesen.

   Der Canvastest auf Browsewrleaks.com[63] demonstriert das Verfahren und kann Schlussfolgerungen über den verwendeten Browser und das Betriebssystem ableiten (und damit einen User-Agent Fake enttarnen).

   Your Fingerprint :

Signature	1CC7FA60
Found in DB	✓ True
General Conclusion	**It is very likely that you are using [Firefox] on [Ubuntu]**

2. Canvas Font Fingerprinting wurde 2016 in dem *OpenWPM Paper* beschrieben. Dabei wird die Methode *measureText* des *CanvasRenderingContext2D* Objektes genutzt. Der Text wird nicht in das Canvas Element geschrieben sondern es wird nur die Größe ermittelt, die ein Text mit unterschiedlichen Schriftarten benötigen würde, wenn er geschrieben werden würde. Der ClientRects Test auf Browsewrleaks.com[64] demonstriert das Verfahren.

   Auch dieses Trackingverfahren wird in-the-wild für das Fingerprinting eingesetzt.

Schutz gegen Fingerprinting mit HTML5 Canvas

Das Add-on **CanvasBlocker**[65] kann Zugriffe auf Canvas-API faken (geringfügig modifizieren) oder faken. Daneben werden noch weitere Javascript-APIs modifiziert wie die Audio-API oder die Screen-API zum Auslesen der Fenster- und Bildschirmgröße, die als Informationen für Browserfingerprintig genutzt werden.

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

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

1. *Convenient Settings* (nur leichte Modifikationen der APIs)
2. *Stealth Settings* (meiner Meinung nach die besten Einstellungen, da sie einen umfangreichen Schutz bieten aber schwer als Fakes erkennbar sind)
3. *Maximum Protection* (maximaler Schutz aber mit kleinen Störungen auf einigen Websites, außerdem sind die Fakes teilweise durch Trackingscripte erkennbar)

Bei der Installation muss man einen der genannten Paramtersätze auswählen. Um nachträglich die Presets zu ändern, klickt man in den Einstellungen von CanvasBlocker auf dem Reiter *General* in der Sektion *Settings* auf den Button *Open* für die Presets (Abb: 4.17). Es öffnet sich ein neuer Tab, wo man einen der vorbereiteten Parametersätze auswählt.

[62] http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf
[63] https://www.browserleaks.com/canvas
[64] https://www.browserleaks.com/rects
[65] https://addons.mozilla.org/de/firefox/addon/canvasblocker/

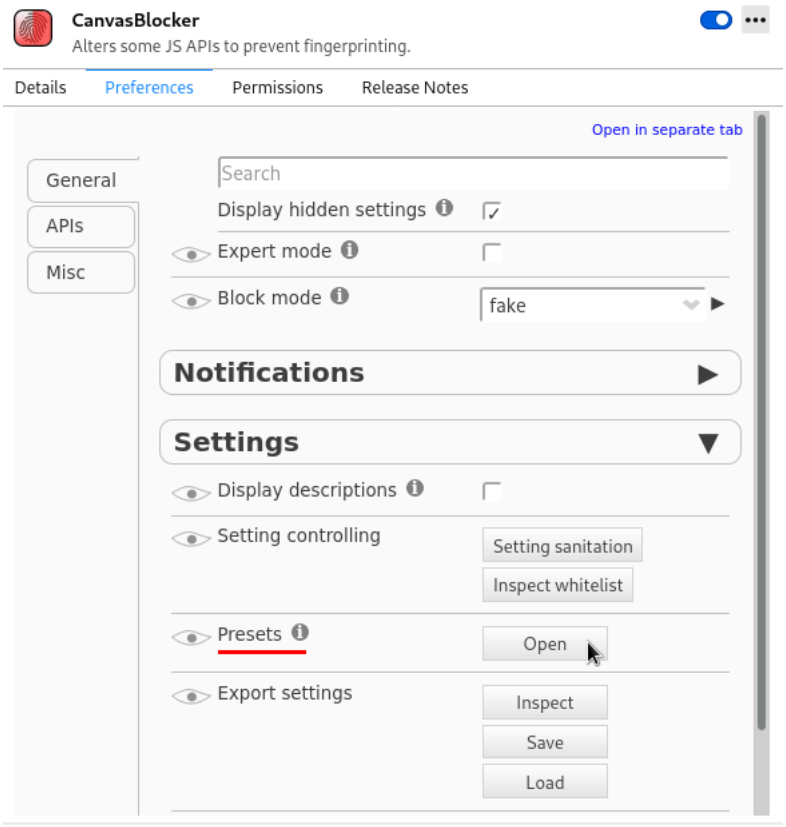
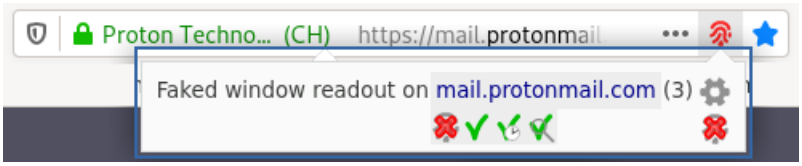


Abbildung 4.17: CanvasBlocker: Presets für die Konfigurationsparameter auswählen

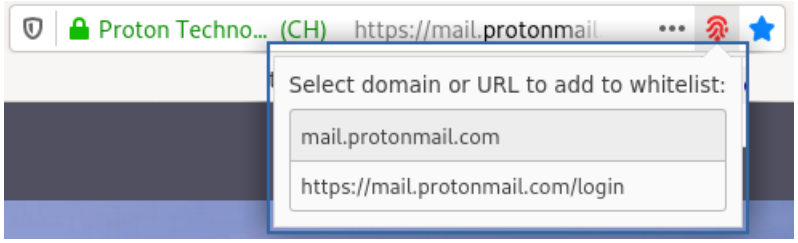
Whitelisting vertrauenswürdiger Webseiten

Die Canvas-API wird nicht nur für das Tracking verwendet. Viele Javascript-lastige Webseiten verwenden es auch, um die optimale die Darstellung der Webseiten zu berechnen. Vertauenswürdige Webseiten kann man deshalb in eine Whitelist aufnehmen.

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



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



4.18 Zugriff auf lokale URLs blockieren

Neugierige oder bösartige Webseiten könnten z. B. mit JavaScript über Adressen wie *http://localhost...* oder *http://192.168.1.1...* auf lokale Dienste auf dem eigenen Rechner, auf den Router oder auf andere Dienste im lokalen Netzwerk (LAN) zugreifen:

- Auf der [TAILS-Dev] Mailingliste wurde darauf hingewiesen, dass ein Angreifer oder Trackingdienst JavaScript Code in eine Webseite einbetten könnte, der das interne LAN nach Servern scannt oder versucht lokale Dienste wie den Druckerservice CUPS unter der Adresse http://localhost:631 zu kontaktieren und diese Informationen zum Fingerprinting nutzt, um den Surfer später wiederzuerkennen.[66]

- Bösartiger JavaScript Code könnte lokale Dienste wie CUPS oder andere Rechner im LAN angreifen. Im Mai 2015 wurde ein Exploit-Kit entdeckt, der als böses JavaScript auf Webseiten platziert wird und bei Aufruf der Webseite den Router angreift, um DNS Einstellungen zu ändern und den Internetzugriff beliebig zu manipulieren.[67]

- Die Firma ThreadMetrix hat 2015 für die Webseiten von Banken einen Sicherheitsmechanismus entwickelt, der unter anderem via Javascript bestimmte Ports auf dem lokalen Rechner scannt, die für einige Viren, Fernwartungssoftware und Remote Desktops wie VNC typisch sind. Seit Mai 2020 ist ein ähnliches Feature auch bei eBay aktiv, wenn eBay vermutet, dass der Anwender Windows nutzt. Dabei handelt sich um ein Sicherheitsfeature und keinen Angriff oder Tracking, aber trotzdem...

uBlock Origin

Nachdem eBay im Mai 2020 begonnen hatte, die lokalen Ports zu scannen, hat das uBlock Team reagiert und eine Filterliste erstellt. Diese Filterliste blockiert für Webseiten aus dem Internet den Zugriff auf lokale URLs, Adressen im LAN sowie häufige Router Adressen.

Zukünftig wird die LAN-Block-Filterliste (wahrscheinlich) in die Standardlisten von uBlock Origin aufgenommen werden aber bei Installation standardmäßig deaktiviert sein. Aktuell muss man die LAN-Block-Filterliste von *gwarser* noch selbst auf dem Reiter *Filterlisten* hinzufügen, indem man die Liste von folgender Adresse lädt:

`https://raw.githubusercontent.com/gwarser/filter-lists/master/lan-block.txt`

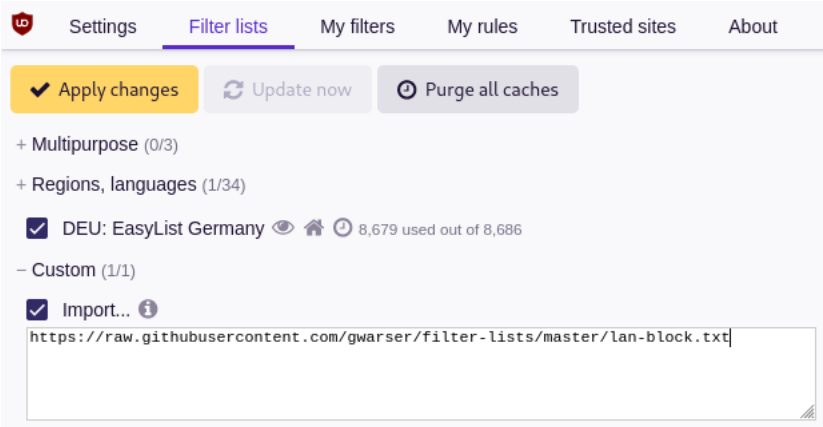


Abbildung 4.18: uBlock Origin: Filterliste hinzufügen

[66] https://mailman.boum.org/pipermail/tails-dev/2015-April/008607.html
[67] https://heise.de/-2665387

4.19 Der Unsinn vom Spoofen der User-Agent Kennung

Bei jedem Aufruf einer Webseite oder dem Laden von Bilder o.ä. sendet der Browser in den HTTP Request Headern Informationen wie die bevorzugten Dateitypen, die bevorzugte Sprache oder die User-Agent Kennung mit Informationen über den verwendeten Browser, die Version des Browsers und das Betriebssystem. Firefox 72 für Linux sendet zum Beispiel:

```
Mozilla/5.0 (X11; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
```

Aus unterschiedlichen Gründen wird immer wieder empfohlen, die User-Agent Kennung zu modifizieren (faken). Linuxer und MacOS Nutzer sollen als Fake die Kennung von Google Chrome für Windows verwenden, weil dieser Browser häufiger verwendet wird und man damit angeblich besser in der Masse untertaucht. Windows Nutzer sollen ein Linux spoofen, um sich gegen Drive-by-Downloads von Malware zu schützen. . . u.a.m.

Es ist nahezu unmöglich, die User-Agent Kennung eines Browsers plausibel zu faken. Eine unsachgemäße Änderung kann zu einem einzigartigen Gesamtbild führen, welches das Tracking enorm erleichtert und man erreicht das Gegenteil des Beabsichtigten. Der Anonymitätstest von JonDonym[68] entlarvt viele Fehler:

HTTP Header: Die einzelnen Browser sind durch individuelle Headerzeilen und -reihenfolge im HTTP-Request beim Aufruf einer Webseite unterscheidbar. Eine Tarnung mit dem User-Agent eines anderen Browsers ist oft leicht als Fake zu identifizieren. Viele Add-ons zum Spoofen der User Agent Kennung machen diesen Fehler.

Das Add-on *User-Agent-Overrider* (Version 0.2.5.1) sollte im Test einen Internet Explorer 9.0 für Win64 faken. Die Header Signatur entlarvt den Browser jedoch als einen Firefox, der sich als IE tarnen will.

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

Das Add-on *Random-Agent-Spoofer* (Version 0.9.5.2) sollte im Test einen Google Chrome Browser 41.0 für Win64 faken. Die Header Signatur entlarvt den Browser ebenfalls als Firefox, der sich tarnen will.

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

Firefox Release Versionen und Firefox ESR Versionen unterscheiden sich nicht nur in der Version in der User-Agent Kennung sondern auch in anderen Eigenschaften. Firefox 68.x ESR und Firefox 72+ unterscheiden sich im HTTP-Accept Header:

```
Firefox 68: ...application/xml;q=0.9,*/*;q=0.8
Firefox 72: ...application/xml;q=0.9, image/webp,*/*;q=0.8
```

Es ist deshalb nicht sinnvoll, ein User-Agent Fake für Firefox ESR zu aktivieren, wenn man eine Firefox Release Version verwendet. Die resultierende Kombination von Eigenschaften ist selten und erleichtert das Tracking via Fingerprinting. (Aus diesem Grund ist die Option *privacy.resistFingerprinting* nur für Firefox ESR sinnvoll nutzbar, da damit ein User-Agent Fake als Firefox ESR für Windows aktiviert wird.)

Javascript: Das Add-on User Agent Platform Spoofer macht aus einem Firefox für Windwos einen Firefox für Linux und umgekehrt, um die automatische Installation von Malware im Drive by Download zu erschwerden. Auch hier ist der Fake nicht vollständig, wie ein kurzer Test unter Linux zeigt. Mit Javascript kann der genutzte Browsertyp und Betriebssystem ermittelt werden:

[68] http://ip-check.info

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

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

CSS Attribute: Durch unterschiedliche Font Rendering Bibliotheken ergeben sich Abweichungen bei CSS Attributen, die mit Javascript ausgelesen werden können. Anhand des CSS-Attributes *line-height* kann man zum Beispiel bei Verwendung hoch- und tiefgestellter Zeichen Schlussfolgerungen über das Betriebssystem ziehen. Es ergeben sich unterschiedliche Werte bei gleichem HTML Code, beispielsweise 19px für Linux, 19.5167px für MacOS und 19.2px oder 20px für Windows.

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

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

Plug-ins: verraten in der Regel das verwendete Betriebssystem und können dafür keinen Fake konfigurieren. Wenn man auf Flash u.ä. nicht verzichten kann, dann sollte man keinen User-Agent Fake verwenden.

Schlussfolgerung

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

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

Eine kleine Ausnahme für Linuxer

Viele Linux Distributionen bauen einen Firefox, der in der User-Agent Kennung des Browser den Namen der Linux Distribution mit einfügt. Hier könnte man einen generischen Firefox für Linux vortäuschen, um die überflüssige Information der genutzten Linux Distribution aus der Kennung zu entfernen indem amn folgenden Wert für die Variable *general.useragent.override* einträgt:

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

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

4.20 Hardware Fingerprinting

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

Bildschirm: Informationen über die Größe des Monitors und des Browserfensters werden am häufigsten für das Hardwarefingerprinting genutzt. Es liegen keine wissenschaftlichen Analysen zur Verbreitung dieser Trackingmethode vor, aber grob geschätzt werden diese Informationen von 30-50% der Webseiten ausgewertet. Insbesondere auf größeren Portalen wie heise.de, spiegel.de, zeit.de oder google.com findet man fast immer Trackingscripte, die Bildschirmgröße und Größe des Browserfensters für das Fingerprinting des Browsers nutzen.

Das Add-on **CanvasBlocker** kann Zugriffe auf die Screen-API faken und verwendet die am besten passende Bildschirmgröße aus folgenden häufigen Werten: 1366x768, 1440x900, 1600x900, 1920x1080, 4096x2160 und 8192x4320.

Die Verwendung von CanvasBlocker ist empfehlenswert, da es für den Fake Bildschirmgrößen verwendet, die in-the-wild häufig vorkommen. Daneben gibt es noch die von TorProject.org entwickelte Option zum Faken der Bildschirmgröße, die mit den folgende Variablen unter *about:config* aktiviert wird:

```
privacy.resistFingerprinting              = true
privacy.resistFingerprinting.letterboxing = true
```

Wenn diese Variable gesetzt wurde, dann verhält sich Firefox 55.0+ wie der TorBrowser. Das Browserfenster wird in einer Größe von 1000 Pixeln Breite und eine Höhe von n*100 Pixeln geöffnet. Bei Vergrößerung des Fensters wird der genutzte Ausschnitt um ein Vielfaches von 100 Pixeln vergrößert, möglicherweise sieht man rund um den Bereich der Webseite weiße Ränder. Die Fenstergröße des Browser wird auch als Bildschirmgröße verwendet und die reale Größe ist nicht mehr auslesbar. Die Größen sind allerdings willkürlich gewählt. Für die Definition einer Anonymitätsgruppe des TorBrowsers ist es sinnvoll aber in-the-wild sind diese Werte sehr selten.

Außerdem werden noch folgende Features mit dieser Option aktiviert:

- Als User-Agent wird die Kennung eines Firefox ESR für Windows verwendet. Der unvollständiger Fake des User-Agent ist eher kontraproduktiv und erleichtert Fingerprinting, wenn man keinen Firefox ESR für Windows verwendet!
- Zeitzone des Browsers wird auf UTC gesetzt (anhand der IP-Adresse ist trotzdem erkennbar, in welcher Zeitzone der Nutzer sich befindet).
- Die Option *Öffnen mit...* wird im Download Dialog deaktiviert. Downloads müssen gespeichert werden und können nicht aus dem Browser heraus mit anderen Anwendungen geöffnet werden.
- navigator.plugins and navigator.mimeTypes sind nicht auslesbar.
- Auslesen der Screen Rotation liefert immer Querformat.
- Die Genauigkeit von Timiming Events wird auf min. 100ms reduziert.

Hinweis: Aufgrund der Änderung an der User-Agent Kennung ist diese Option nur für Firefox ESR (Windows) empfehlenswert! Beim Firefox 72+ wurde der HTTP-Accept-Header geändert. Damit ist der Fake nicht plausibel und es ist einfach zu erkennen, dass ein Release Firefox sich als Firefox ESR tarnen möchte. Diese Kombination ist selten und erleichtert das Tracking via Browser Fingerprinting statt es zu erschweren.

AudioContext: Mit der Audio-API kann Javascript unhörbare Soundschnipsel im Audiobuffer generieren, manipulieren und die Ergebnisse wieder auslesen. Dabei unterscheiden sich die Ergebnisse in Abhängigkeit von der Audiohardware und -software. Die Daten können für das Fingerprinting genutzt werden, wie die *AudioContext Fingerprint Test Page*[69] zeigt.

Das Add-on **CanvasBlocker** kann Zugriffe auf die Audio-API faken (geringfügig modifizieren) und damit ein Fingerprinting des Browsers verhindern. Das Ergebnis ist zwar *unique* aber immer wieder anders.

[69] https://audiofingerprint.openwpm.com

Alternativ kann die Audio-API mit folgender Option deaktiviert werden:

```
dom.webaudio.enabled = false
```

Das Faken der Audio-API mit dem Add-on CanvasBlocker ist unauffälliger und schwerer erkennbar als das Blockieren der API und deshalb empfohlen.

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

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

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

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

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

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

4.21 WebRTC mit Firefox

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

Neben der Internettelefonie wird WebRTC auch auch bei browserbasierten Videokonferenzsystemen wie Jitsi Meet eingesetzt. Bei der direkten 1:1 Kommunikation ist für den Datenstrom eine Ende-zu-Ende Verschlüsselung vorgesehen. Bei Konferenzsystemen ist es häufig so, dass der Konferenzserver als Endpunkt agiert, die Daten entschlüsselt und für jeden Teilnehmer neu verschlüsselt. (Verbesserte Lösung mit durchgehende Ende-zu-Ende Verschlüsselung für Konferenzsysteme sind in der Entwicklung.)

OpenH264 Videocodecs

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

Mit folgende Einstellungen unter *about:config* wird das OpenH264 Plugin aktiviert:

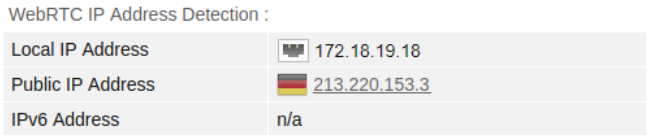
```
media.gmp-gmpopenh264.enabled          = true
media.gmp-gmpopenh264.autoupdate       = true
media.gmp-gmpopenh264.provider.enabled = true
```

Bei einigen sicherheitsoptimierten Linux Distributionen wie RHEL, CentOS oder Fedora ist das Plugin standardmäßig deaktiviert. Oft sind Probleme mit browserbasierten Videokonferenzen darauf zurück zu führen, dass das Plugin nicht aktiviert wurde.

Internet Connectivity Establishment (ICE)

Der Datenstrom soll bei WebRTC möglichst direkt zwischen den Teilnehmern ausgetauscht werden. Es wird der ICE Standard (Internet Connectivity Establishment) verwendet, um eine direkte Verbindung zwischen den Clients aufzubauen. ICE versucht im Hintergrund sehr aggressiv, die direkte Verbindung irgendwie herzustellen. Es werden Proxy Einstellungen umgangen, via UPnP wird versucht, ein Loch in Router und Firewalls zu bohren, VPNs werden teilweise ausgetrickst... Dabei kommt ein STUN Server zum Einsatz, der die verschiedene Möglichkeiten ausprobiert. Wenn wirklich keine direkte Verbindung möglich ist, wird ein TURN Server als Proxy für den Datenstrom verwendet.

Aufgrund dieser aggressiven Strategie zum Verbindungsaufbau können der Gegenseite folgende Informationen bekannt werden, wie der WebRTC Test von Browserleaks[70] zeigt:



- Alle IP-Adressen und Interfaces des Rechners oder der VM im lokalen LAN. (Ein Angreifer oder Trackingservice könnte das verwenden, um mehrere Rechner innerhalb eines Firmennetzwerkes oder in einem Haushalt zu unterscheiden.)
- Externe Adresse des Routers/Gateways zum Internet. (Diese Adresse sollte eigentlich geheim bleiben, wenn man einen Proxy wie Tor Onion Router oder ein VPN verwendet. Aber alle Proxys und einige VPN Techniken können von ICE ausgetrickst werden und damit den Nutzer deanonymisieren.)
- Externe Adresse des Proxy oder VPN Endpunktes. (Diese Information lässt sich natürlich nicht geheim halten.)

Firefox bietet einige Möglichkeiten, die Privacy Probleme von ICE zu reduzieren:

1. Bei privater Nutzung kann man davon ausgehen, dass man innerhalb der Wohnung mündlich kommuniziert und nicht via WebRTC. Die internen Adressen aus dem LAN müssen nicht publiziert werden. Mit folgenden Optionen man es abschalten:

   ```
   media.peerconnection.ice.default_address_only = true
   media.peerconnection.ice.no_host              = true
   ```

2. Wenn man verhindern möchte, dass die Gegenseite die externe IP-Adresse des Routers erfährt und damit Schlussfolgerungen über den Standort via Geolocation ziehen könnte, kann man direkte Verbindungen generell ausschließen und immer eine Verbindung über einen TURN Proxy Server erzwingen:

   ```
   media.peerconnection.ice.relay_only = true
   ```

3. Wenn man den STUN/TURN Servern des Videokonferenzanbieters nicht vertraut, kann man eigene Server verwenden:

   ```
   media.peerconnection.use_document_iceservers = false
   ```

   Die eigenen Server muss man in der folgenden Variable definieren:

   ```
   media.peerconnection.default_iceservers = <Serverliste>
   ```

4. Wenn man WebRTC nur via VPN verwenden möchte aber nicht, wenn man ohne VPN surft, dann kann man die zulässigen Netzwerkinterfaces definieren:

[70] https://browserleaks.com/webrtc

```
media.peerconnection.ice.force_interface = tun1
media.peerconnection.ice.no_host         = true
```

Wenn das VPN nicht aktiviert wurde und damit das virtuelle VPN Interface *tun1* nicht vorhanden ist, kann man ganz normal surfen aber eine WebRTC Verbindung wird nicht akzeptiert. Nur wenn das VPN aktiv ist, ist eine WebRTC Verbindung möglich, deren Daten immer durch das VPN geschickt werden.

5. Änlich wie bei der VPNs kann man auch die Verwendung eines Proxy erzwingen und WebRTC nur via Proxy zulassen:

   ```
   media.peerconnection.ice.proxy_only = true
   ```

   In den meisten Fällen wird WebRTC mit dieser Einstellung nicht funktionieren, da HTTP- oder SOCKS-Proxy wie Tor Onion Router nicht UDP-fähig sind.

Mit dem **WebRTC Test**[71] kann man prüfen, ob die Einstellungen korrekt funktionieren.

Media Device Enumeration

Um WebRTC nutzen zu können, muss Firefox wissen, welche Media Input Devices vorhanden sind und nach Zustimmung durch den Nutzer Zugriff darauf erlangen können:

```
media.navigator.enabled       = true
media.navigator.video.enabled = true
```

Trackingdienste können die Media Device Enumaration von WebRTC ausnutzen, um Daten über Kamera und Mikrofon zu sammeln und für das Hardware Fingerprinting zu verwenden. Der Surfer wird dabei nicht um Zustimmung für einem Zugriff auf Kamera oder Mikrofon gebeten. Der WebRTC Test von Browserleaks demonstriert es.

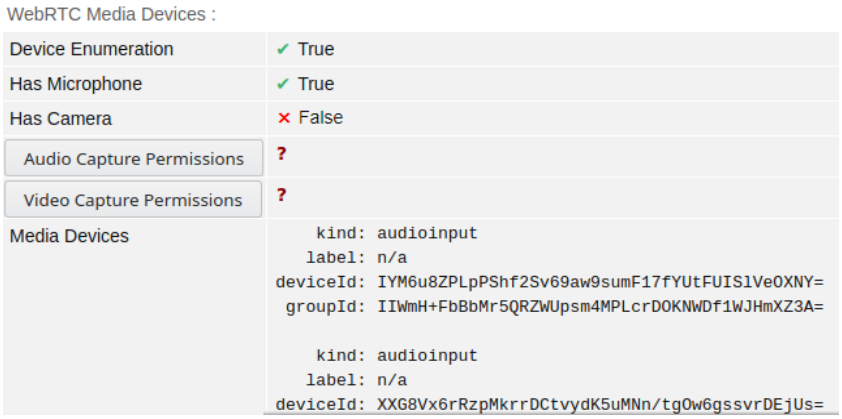


Abbildung 4.19: Media Device Enumeration via WebRTC

Firefox verwendet als Device-IDs einen gesalzenen Hash. Der Salt für die Berechnung des Hashes wird beim ersten Start festgelegt und immer erneuert, wenn Cookies und Cache Daten gelöscht werden. Außerdem ist der Salt in Surfcontainern unterschiedlich. Damit ist die Device-ID in gleicher Weise wie langlebige Cookies für das Tracking geeigent oder nicht geeignet wie Cookies und als Schutz gegen Tracking anhand der Device-IDs kann man die Empfehlungen für Cookies umsetzen.

[71] https://test.webrtc.org/

WebRTC und OpenH264 Plugin deaktivieren

Wenn man den Browser nur zum Surfen verwendet und nicht für Videokonferenzen mit Jitsi Meet oder ähnlichen Systemen, kann man WebRTC, Media Device Enumeration und das OpenH264 Plugin deaktivieren, um Trackingfeatures und Angriffsfläche zu minimieren:

```
media.peerconnection.enabled           = false

media.navigator.enabled                = false
media.navigator.video.enabled          = false

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

4.22 DNS-over-HTTPS mit Firefox

DNS (Domain Name Service) ist das Telefonbuch des Internet. Es übersetzt lesbare URLs wie *www.privacy-handbuch.de* in die IP-Adresse des Servers, der diese Webseite zur Verfügung stellt. Eine ausführliche Anleitung zu diesem zentralen Internetdienst findet man im Kapitel *DNS und DNSSEC*.

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

Da DNS ein zentraler Dienst für alle Internet Anwendungen ist, ist eine zentrale Konfiguration der DNS-Server sinnvoller als die Konfiguration einzelner Webbrowser.

Kein ESNI ohne DNS-over-HTTPS

Firefox unterstützt *Encrypted Server Name Indication* (ESNI) für TLS 1.3 verschlüsselte Verbindungen nur, wenn DNS-over-HTTPS aktiviert ist! Um ESNI zu verwenden, muss der Browser einen TXT Record der Webseite aus dem DNS abrufen. Das geht nur mit dem eingebauten Trusted Recursive Resolver. Außerdem muss folgender Wert aktiviert werden:

```
network.security.esni.enabled = true
```

Auf der Testseite[72] von Cloudflare kann man prüfen, ob es funktioniert.

ESNI könnte ein Grund sein, DNS-over-HTTPS im Browser zusätzlich zu aktivieren, auch wenn man eine sichere DNS Namensauflösung auf Systemebene konfiguriert hat.

Browserfingerprinting mittels DNS Server

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

1. Der Webserver sendet im HTML Code ein kleines, überflüssiges Element, dass von einer zufällig generierten Subdomain des Trackingservice geladen werden soll.

[72] https://www.cloudflare.com/ssl/encrypted-sni/

2. Der Browser versucht die IP-Adresse für diese Subdomain zu ermitteln. Der konfigurierte Upstream DNS-Server hat die Information nicht im Cache und muss deshalb den authorativen Server des Trackingdienstes anfragen.

3. Der authorative DNS-Server des Trackingdienstes registriert die DNS Anfrage und die IP-Adresse des anfragenden DNS-Servers und sendet beides an den Trackingservice, wo die Information mit dem Aufruf der Webseite korrelliert werden kann.

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

Konfiguration in den Netzwerk Einstellungen

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

Wenn man eine der user.js Konfiguration installiert hat, dann kann man einen privacy-freundlichen Provider direkt auswählen, der HTPPS-over-DNS anbietet (Abb 4.20).

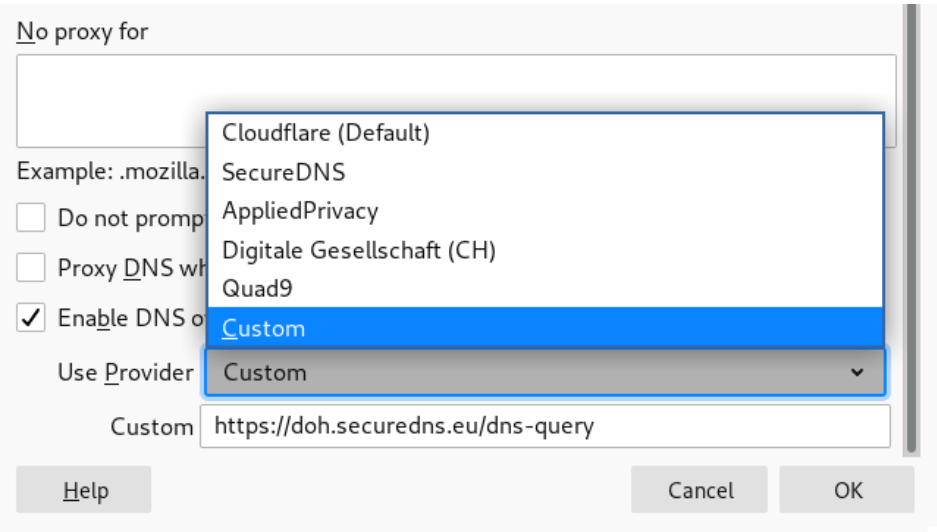


Abbildung 4.20: Konfiguration der DNS-over-HTTPS

Konfiguration für Experten

Mit folgende Werten könnte man TRR in Firefox unter *about:config* konfigurieren:

- Mit dem TRR-Mode kann man auswählen, wie DNS-over-HTTPS verwendet wird:

```
network.trr.mode = 0 (Abgeschaltet aufgrund der Default Einstellung.)
network.trr.mode = 1 (Frage System DNS und TRR und verwendet erstes Ergebnis.)
network.trr.mode = 2 (Verwende TRR und System DNS nur als Fallback.)
network.trr.mode = 3 (Verwende ausschließlich TRR nach dem Start.)
network.trr.mode = 4 (TRR parallel zum System DNS aber nicht verwenden.)
network.trr.mode = 5 (Abgeschaltet aufgrund der Entscheidung des Nutzers. FF61+)
```

Firefox für Windows deaktiviert DNS-over-HTTPS unabhängig von den Einstellungen für network.trr.mode, wenn ein VPN genutzt wird, wenn ein Proxy in den Windows Systemeinstellungen konfiguriert wurde oder wenn mittels NRPT spezielle DNS Server für einzelne Domains festgelegt wurden. Wenn man mit Firefox für Windows trotz VPN, Proxy oder NRPT einen DNS-over-HTTPS Server verwenden möchte, muss man folgende Einstellungen aktivieren:

```
network.trr.enable_when_vpn_detected   = true
network.trr.enable_when_proxy_detected = true
network.trr.enable_when_nrpt_detected  = true
```

- Wenn man TRR-Mode 1-3 verwenden möchte, dann muss man die zwingend notwendige Validierung von SSL-Zertifikaten via OCSP-Server abschalten. Ansonsten beißt sich die Katze in den Schwanz. Firefox will das SSL-Zertifikat des DNS-over-HTTPS Server prüfen und braucht dafür die IP-Adresse des OCSP Servers vom DNS-over-HTTPS Server... Also entweder OCSP komplett deaktivieren:

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

  Oder nicht zwanghaft auf eine OCSP Antwort bestehen:

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

- Konfiguration für den DNS-over-HTTPS Server von Freifunk München:

  ```
  network.trr.uri = https://doh.ffmuc.net
  network.trr.bootstrapAddress = 5.1.66.255
  ```

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

  ```
  network.trr.uri = https://dns.digitale-gesellschaft.ch/dns-query
  network.trr.bootstrapAddress = 185.95.218.42
  ```

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

  ```
  network.trr.uri = https://dnsforge.de/dns-query
  network.trr.bootstrapAddress = 176.9.1.117
  ```

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

  ```
  network.trr.uri = https://doh-de.blahdns.com/dns-query
  network.trr.bootstrapAddress = 159.69.198.101
  ```

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

  ```
  network.trr.uri = https://doh-fi.blahdns.com/dns-query
  network.trr.bootstrapAddress = 95.216.212.177
  ```

- Konfiguration für Quad9 DNS-over-HTTPS Server:

  ```
  network.trr.uri = https://dns.quad9.net/dns-query
  network.trr.bootstrapAddress = 9.9.9.9
  ```

- Konfiguration für Standard Cloudflare DNS-over-HTTPS Server:

  ```
  network.trr.uri = https://cloudflare-dns.com/dns-query
  network.trr.bootstrapAddress = 1.1.1.1
  ```

- Für Googles DNS-over-HTTPS Server gilt die Datensch(m)utz Policy von Google:

```
network.trr.uri = https://dns.google.com/resolve
network.trr.bootstrapAddress = 216.58.214.110
```

- Unter der Adresse *about:networking* kann man sich auf dem Reiter *DNS* anschauen, ob der Trusted Recursive Resolver funktioniert und verwendet wird.

- Road-Warrior, die häufig an Wi-Fi Hotspots unterwegs sind, können nach dem Login im Portal des Hotspot automatisch auf DNS-over-HTTPS umschalten:

```
network.trr.wait-for-portal = true
network.captive-portal-service.enabled = true
```

  (Die Wi-Fi Hotspot Portalerkennung ist in unserer Firefox Config deaktiviert.)

4.23 Sonstige Maßnahmen

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

Überflüssige Cloud-Dienste deaktivieren

Firefox bietet mehrere Dienste, die die *User Experience* verbessern sollen und dafür irgendwelche Daten auf irgendwelche Cloud Server hochladen:

Pocket-API ist eine Erweiterung, mit der man Webseiten komplett in einem sogenannten Pocket speichern und später lesen kann. In der Praxis kann man natürlich auch Lesezeichen dafür nutzen oder die Download Funktion, wenn man eine Webseite später in genau diesem Zustand lesen möchte. Die Pocket-API ist überflüssig, kann man unter *about:config* deaktivieren:

```
extensions.pocket.enabled = false
```

Screenshots ist eine Erweiterung, mit der man Bildschirmfotos erstellen kann, die automatisch auf den Cloud-Server *screenshots.mozilla.com* hochgeladen werden und von dort ganz einfach mit einem Klick auf Social Media Webseiten verbreitet werden könnten.

In den Datenschutzhinweisen[73] weist Mozilla darauf hin, dass nicht nur der Upload der Screenshots protokolliert wird, sondern auch jeder Abruf durch Dritte, die die Screenshot auf irgendwelchen Social Media Webseiten betrachten, wo sie veröffentlicht wurden. Den Upload von Screenshots kann man unter *about:config* mit folgendem Parameter deaktivieren:

```
extensions.screenshots.upload-disabled = true
```

Wenn ich einen Screenshot haben möchte, dann gibt es dafür genügend Tools, die Screenshots erstellen können und ich entscheide dann, wie ich sie publiziere. Die Screenshot Extension kann man auch unter *about:config* komplett deaktivieren:

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

[73] https://www.mozilla.org/de/privacy/firefox

Keine Daten beim Ausfüllen von Formularen speichern

Firefox bietet die Möglichkeit, Daten aus Formularen zu speichern und später ähnliche Formulare automatisch auszufüllen. Seit Version 55 können Adressdaten erkannt und gespeichert werden, Firefox 58+ kann Kreditkartennummern erkennen und speichern. Damit soll vor allem Power-Shoppern das Einkaufen im Internet etwas erleichtert werden.

Firefox bietet einige Schutzfunktionen gegen Phishing Angriffe auf automatisch ausgefüllte Formulardaten. Trotzdem ist es nicht auszuschließen, dass raffinierte Angreifer Wege finden werden, um unsichtbare Formulare automatisch ausfüllen zu lassen und die Daten auslesen. Unter *about:config* kann man das Speichern von Formulardaten abschalten:

```
browser.formfill.enable = false
```

Zusätzlich kann man folgende Features deaktivieren:

```
extensions.formautofill.addresses.enabled    = false
extensions.formautofill.creditCards.enabled  = false
extensions.formautofill.heuristics.enabled   = false
```

WebGL konfigurieren oder deaktivieren

WebGL stellt eine JavaScript-API für das Rendering von 3D-Objekten bereit. Wenn die Debug Informationen vie Javascript auslesbar sind, können Informationen über den Hersteller das Modell der Grafikkarte ausgelesen werden. Diese Informationen sind gut für das Fingerprinting geeignet. Deshalb sollten die WebGL Debug Informationen in jedem Fall abgeschaltet werden:

```
webgl.enable-debug-renderer-info = false
```

WebGL kann die Performance der Grafikhardware und OpenGL Software für das Fingerprinting verwenden, wie die Studie *Perfect Pixel: Fingerprinting Canvas in HTML5* [74] zeigte. Das Fingerprinting via WebGL kann mit folgenden Einstellungen reduziert werden:

```
webgl.min_capability_mode                      = true
webgl.disable-fail-if-major-performance-caveat = true
```

Außerdem ist WebGL ein (unnötiges) Sicherheitsrisiko, weil damit Angriffe auf das Betriebssystem möglich werden. Durch nachgeladene Schriften können Bugs in den Font Rendering Bibliotheken ausgenutzt werden, das gab es für Windows (ms11-087), Linux (CVE-2010-3855) oder OpenBSD (CVE-2013-6462). Die WebGL Shader Engines haben auch gelegentlich Bugs, wie z. B. MFSA 2016-53. Man kann WebGL komplett deaktivieren, um dieses Risiko zu reduzieren:

```
webgl.disabled      = true
webgl.enable-webgl2 = false
```

Timing APIs deaktivieren

Die hochgenauen Timing APIs können von Webanwendungen zur Analyse des Ladens von Resourcen oder des Nutzerverhaltens missbraucht werde, siehe: *Timing Attacks on Web Privacy*[75]. Wenn man seinen Browser zum Lesen von Webseiten und nicht vorrangig für Games verwendet, sollte man die APIs deaktivieren:

```
dom.enable_resource_timing                = false
dom.enable_performance                    = false
dom.enable_performance_navigation_timing = false
```

[74] http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf
[75] http://sip.cs.princeton.edu/pub/webtiming.pdf

Clipboard Events deaktivieren

Mit den Clipboard Events informiert Firefox eine Webseite, dass der Surfer einen Ausschnitt in die Zwischenablage kopiert hat oder den Inhalt der Zwischenablage in ein Formularfeld eingefügt hat. Es werden die Events *oncopy, oncut* and *onpaste* ausgelöst, auf die die Webseite reagieren kann. Man kann diese Events unter *about:config* deaktivieren:

```
dom.event.clipboardevents.enabled = false
```

Außer bei Google Docs und ähnliche JavaScript-lastigen GUIs zur Dokumentenbearbeitung in der Cloud ist mir keine sinnvolle Anwendung dieses Features bekannt.

Spekulatives Laden von Webseiten

Firefox beginnt in einigen Situationen bereits mit dem Laden von Webseiten, wenn sich der Mauszeiger über einem Link befindet, also bevor man wirklich klickt. Damit soll das Laden von Webseiten einige Millisekunden beschleunigt werden. Wenn man Verbindungen mit unerwünschten Webservern vermeiden möchte, kann man das Feature unter *about:config* abschalten:

```
network.http.speculative-parallel-limit = 0
```

Kill Switch für Add-ons abschalten

Die Extension blocklist[76] kann Mozilla nutzen, um einzelne Add-ons im Browser zu deaktivieren. Es ist praktisch ein kill switch für Firefox Add-ons und Plug-ins. Beim Aktualisieren der Blockliste werden detaillierte Informationen zum realen Browser und Betriebssystem an Mozilla übertragen.

```
https://addons.mozilla.org/blocklist/3/%7Bec8030f7-c20a
-464f-9b0e-13a3a9e97384%7D/10.0.5/Firefox/20120608001639
/Linux_x86-gcc3/en-US/default/Linux%202.6.37.6-smp%20
(GTK%202.24.4)/default/default/20/20/3/
```

Ich mag es nicht, wenn jemand remote irgendetwas auf meinem Rechner deaktiviert oder deaktivieren könnte. Unter *about:config* kann man dieses Feature abschalten:

```
extensions.blocklist.enabled = false
```

Update der Metadaten für Add-ons deaktivieren

Seit Firefox 4.0 kontaktiert der Browser täglich den AMO-Server von Mozilla und sendet eine genaue Liste der installierten Add-ons und die Zeit, die Firefox zum Start braucht. Als Antwort sendet der Server Statusupdates für die installierten Add-ons. Diese Funktion ist unabhägig vom Update Check für Add-ons, es ist nur eine zusätzliche Datensammlung von Mozilla. Unter *about:config* kann man diese Funktion abschalten:

```
extensions.getAddons.cache.enabled = false
```

HTML5 Beacons deaktivieren

Mit Beacons kann ein Browser beim Verlassen/Schließen einer Webseite Daten zur Analyse an den Webserver senden, die via JavaScript gesammelte wurden. Unter *about:config* kann man dieses Feature abschalten:

```
beacon.enabled = false
```

Wenn man HTML5 Beacons abschaltet, kann es vorkommen, dass eine Webseite nach einem Klick nicht aktualisiert wird. eBay.com ist ein Beispiel dafür. Man muss oft den Reload Button klicken, um eine wirklich aktuelle Seite zu sehen. Deshalb ist dieses Feature nur in der strengen user.js Konfiguration deaktiviert.

[76] https://addons.mozilla.org/en-US/firefox/blocked

Safebrowsing deaktivieren

Wenn die Safebrowsing Funktion aktiv ist, dann holt Firefox alle 30min aktualisierte Blocklisten von den Safebrowsing Providern. Alle Seitenaufrufe werden lokal mit den Listen abgeglichen. Bei einem Treffer sendet Firefox einen Hash der URL an den Safebrowsing Provider, um zu prüfen, ob die Seite noch auf der Liste steht.

Unter Windows werden außerdem alle Downloads von ausführbaren Anwendungen geprüft. Firefox sendet Informationen zur heruntergeladenen Datei (Name, Herkunft, Größe, Hash) an den *Google Safe Browsing Service*. Dafür gilt Googles Datensch(m)utz Policy.

Unter *about:config* kann man Safebrowsing deaktivieren:

```
browser.safebrowsing.phishing.enabled                                = false
browser.safebrowsing.malware.enabled                                 = false
browser.safebrowsing.blockedURIs.enabled                             = false
browser.safebrowsing.downloads.enabled                               = false
browser.safebrowsing.downloads.remote.enabled                        = false
browser.safebrowsing.downloads.remote.block_dangerous                = false
browser.safebrowsing.downloads.remote.block_dangerous_host           = false
browser.safebrowsing.downloads.remote.block_potentially_unwanted     = false
browser.safebrowsing.downloads.remote.block_uncommon                 = false
browser.safebrowsing.downloads.remote.url                            =       (leerer String)
browser.safebrowsing.provider.*.gethashURL                           =       (leerer String)
browser.safebrowsing.provider.*.updateURL                            =       (leerer String)
```

Gegen Phishing Angriffe schützen keine technische Maßnahmen vollständig sondern in erster Linie das eigene Verhalten. Und gegen Malware schützen regelmäßige Updates des Systems besser als Virenscanner und schnell veraltende URL-Listen.

Healthreport und Übertragung von Telemetriedaten deaktivieren

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

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

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

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

Zur Deaktivierung des Telemetrie Toolkit setzt man folgenden Wert:

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

Einzelne Aktionen zur Telemetrie kann man mit folgenden Optionen deaktivieren:

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

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

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

Im August 2018 hat Mozilla festgestellt, dass es keine Daten darüber gibt, wie viele Nutzer die Übertragung der Telemetriedaten abgeschaltet haben. Deshalb hat Mozilla im September 2018 das Add-on Telemetrie Coverage eingebaut und an 1% der Nutzer verteilt. Das Add-on ignoriert die Einstellungen zu Telemetrie und sendet folgende Daten an Mozilla: Firefox Version, Update Channel, Betriebssystem und -version sowie die Information, ob die Übertragung von Telemetriedaten deaktiviert wurde. Um diese Datenübertragung an Mozilla zu deaktivieren, muss man unter *about:config* folgende Variablen neu anlegen:

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

Firefox Location Tracking

Seit Firefox 80 trackt Firefox den Standort der Nutzer. Bei jedem Start wird der Server location.services.mozilla.com angepingt und anhand der IP-Adresse das Land ermittelt, in dem der Nutzer sich aufhält. Die Daten werden in zwei Varibalen gespeichert:

```
Region.current  (das aktuelle Land, in dem der Nutzer sich aufhält)
Region.home     (das vermutete Heimatland des Nutzers)
```

Laut Dokumentation verwendet Mozilla diese Daten, um irgendwelchen relevanten Content auszuwählen und die Standardsuchmaschine zu definieren (in Abhängigkeit von den Verträgen, die Mozilla mit unterschiedlichen Suchdiensten abgeschlossen hat).

Das Aktualisieren des Standortes verhindert man mit folgendem Schalter:

```
browser.region.update.enabled = false
```

Mozillas Werbung nach einem Update

Nach jedem Update von Firefox wird eine andere Startseite aufgerufen, die Mozilla für Werbung sowie statistische Auswertungen nutzt und die ein bisschen nervt. Unter der Adresse *about:config* kann man diese Einblendung abschalten:

```
browser.startup.homepage_override.mstone = ignore
```

Mozillas Bewertungsfeature

Im Rahmen von Stichproben bittet Mozilla die Nutzer, ihre Erfahrungen mit Firefox zu bewerten. Die Bewertungsfunktion baut bei jedem Start von Firefox eine Verbindung zum Mozilla Server auf. Mit folgender Option unter *about:config* deaktiviert man die Bewertungsfunktion und die Verbindungsaufbau:

```
app.normandy.enabled = ignore
```

Deaktivierung der Add-ons auf Mozillas Webseiten

Standardmäßig werden Add-ons auf folgenden Webseiten deaktiviert, um die Funktionalität sicherzustellen, da sie auch für interne Funktionen von Firefox genutzt werden:

```
accounts-static.cdn.mozilla.net
accounts.firefox.com
addons.cdn.mozilla.net
addons.mozilla.org
api.accounts.firefox.com
content.cdn.mozilla.net
discovery.addons.mozilla.org
install.mozilla.org
oauth.accounts.firefox.com
```

```
profile.accounts.firefox.com
support.mozilla.org
sync.services.mozilla.com
```

Damit gibt es auf diese Webseiten zum Beispiel praktisch keinen Trackingschutz mehr, obwohl die Webseiten teilweise Trackingcode einbinden, den uBlock blockieren würde.

Man kann die Deaktivierung der Add-ons auf diesen Webseiten verhindern, wenn man folgende Variable unter *about:config* auf einen leeren String setzt:

```
extensions.webextensions.restrictedDomains =
```

Diese Einstellung kann aber in Abhängigkeit von den installierten Add-ons auch zu Problemen bei einigen internen Funktionen von Firefox führen, die diese Webdienste nutzen.

Systemfarben der Desktop Umgebung

Die CSS Attribute für Farbe und Hintergrund von HTML Elementen können die Systemfarben der Desktop Umgebung verwenden. Damit sieht die Webseite einer nativen Desktop Anwendung ähnlich. Diese individuellen Farben können via Javascript ausgelesen werden und für das Fingerprinting des Browsers verwendet werden. Gleiches gilt für den Darkmode.

Um das Auslesen der Desktop Einstellungen zu verhindern, kann man die eingebauten Standardwerte für die Systemfarben verwenden und den Darkmode deaktivieren:

```
ui.use_standins_for_native_colors = true
ui.systemUsesDarkTheme            = 0
```

In der Empfehlung *CSS Color Module Level 3*[77] ist die Verwendung von Systemfarben als *veraltet* markiert.

Wi-Fi Hotspot Portalerkennung deaktivieren

Firefox 52 erkennt die Portalseiten von Wi-Fi Hotspots und öffnet sie in einem neuen Tab. Für die Wi-Fi Hotspot Portal Erkennung ruft Firefox beim Start und bei einigen weiteren Ereignissen die Adresse *http://detectportal.firefox.com/success.txt* mit einem XMLHttpRequest ab. Wenn dabei ein Redirect gefunden wird statt der erwarteten Antwort, öffnet Firefox den Hinweis zum notwendigen Login auf einer Portal Seite.

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

  ```
  network.captive-portal-service.enabled = false
  ```

  (Wenn man gelegentlich (selten) einen Wi-Fi Hotspot nutzt, kann man die Variable kurzzeitig per Hand auf *true* setzen, damit es funktioniert.)

- Wenn man häufig mit dem Laptop unterwegs ist, kann die Wi-Fi Portal Erkennung ganz nützlich sein. In diesem Fall könnte man die Adresse für den XMLHttpRequest anpassen und einen eigenen Server für den Test verwenden, um nicht ständig den Mozilla Server zu kontaktieren.

  Am einfachsten lädt man die Datei *success.txt* herunter und speichert sie auf dem eigenen Webserver. Unter *about:config* passt die URL an:

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

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

[77] https://drafts.csswg.org/css-color-3

Microsoft Family Safety deaktivieren

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

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

Browser Slow Startup Notifications abschalten

Bei jedem Start prüft Firefox die Zeit, die der Browser zum Starten benötigt. Falls Firefox der Meinung ist, dass er zu langsam startet, wird die Deinstallation von Add-ons empfohlen. Da man sich überlegt, welche Add-ons man braucht und gern verwenden möchte und überflüssige Add-ons natürlich nicht installieren würde, ist dieses Feature überflüssig. Man kann es unter *about:config* deaktivieren:

```
browser.slowStartup.notificationDisabled  = true
browser.slowStartup.maxSamples            = 0
```

4.24 Zusammenfassung der Einstellungen

Um die Werte nicht alle per Hand anpassen zu müssen, haben wir Beispielkonfigurationen für Firefox 60+ vorbereitet, die man herunter laden und im Firefox-Profil speichern kann. Man kann nicht alle Wünsche mit einer Konfiguration abdecken, deshalb gibt es mehrere Vorschläge, die man von der Webseite des Privacy-Handbuches herunterladen kann: https://www.privacy-handbuch.de/handbuch_21u.htm

Die Vorschläge sind Teil eines Gesamtkonzeptes und es wird davon ausgegangen, das die Add-ons *uBlock Origin* und *CanvasBlocker* mit den empfohlenen Konfigurationen installiert wurden. Daraus ergeben sich einige Unterschiede zu vergleichbaren Projekten.

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

- Deaktivierung von Spielereien, die Mozilla eingebaut hat (Activity Stream, Pocket, Telemetrie, Datareporting, Ping-Centre, Captive Portal Check, Safebrowsing, Family Safety, die bunte NewTabPage und Startseite...).
- Löschen von Cache, Cookies usw. beim Beenden des Browsers sowie Aktivierung der Surfcontainer *FirstParty.Isolate* und *userContext* (Trackingschutz).
- Es wird kein Referrer an Drittseiten und beim Wechsel der Domain gesendet.
- Außerdem werden einige allgm. Sicherheitsfeatures aktiviert (AutoFill für Formulare deaktiviert, Anzeige von unsicheren Verbindungen als Text+Icon...)

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

- WebGL steht nur mit dem minimalen Featureset zur Verfügung.
- Deaktivierung einiger JavaScript APIs, die für das Fingerprinting des Browsers aber nur selten beim Surfen verwendet werden (Sensors, Gamepad, Media Navigator, WebRTC, Timing APIs...)
- Da installierte Schriftarten häufig für das Fingerprinting verwendet werden, ist die Verwendung von individuellen Schriften für HTML Dokumente deaktiviert. Man sollte deshalb gut lesbare Standardschriften konfigurieren. Einbindung externer Webicon Fonts für Navigationselemente ist zulässig.

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

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

- Javascript Just-in-Time-Compiler sind aus Sicherheitsgründen deaktiviert, was die ausführung von Javascript auf einige Webseiten verlangsamt.
- Anzeige von PDF Dokumenten im Browser ist deaktiviert.
- SVG, Flash, WebGL und WebGL2 sind komplett deaktiviert.
- Auto-Play und Hardware Video Decoding sind deaktiviert.
- Closed Source Video Codecs werden nicht verwendet.
- Favicons werden nicht geladen und nicht gespeichert.
- Es werden keine Login Credentials gespeichert.
- Push Services sind deaktiviert.
- Der Download von externen Schriftarten ist auch für Navigationssymbole deaktiviert. Um die resultierenden Einschränkungen etwas abzumildern, kann man häufig genutzte Webicon Fonts wie den Awesome Webicon Font installieren. Linux enthält passende Pakete, für Debian/Ubuntu funktioniert:

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

Hotspot Login: Die *Hotspot user.js* ist eine strenge user.js mit aktiviertem Captive Portal Service. Sie könnte in einem Profil eingesetzt werden, dass man nur für den Login bei Wi-Fi Hotspots nutzt. Die Startseite ist *about:profiles*, so dass man nach dem Hotspot Login schnell das gewünschte Profil zum Surfen starten kann.

Die gewählten Datei *user.js* ist im Firefox-Profil zu speichern und wird beim Start von Firefox eingelesen. Die Werte überschreiben die Einstellungen in *prefs.js*. Damit ist sichergestellt, dass man beim Start die gewünschten Einstellungen hat.

Das Firefox-Profil ist ein Unterverzeichnis mit seltsamen Buchstaben, das man in folgenden Verzeichnissen findet:

- Windows: %APPDATA% -> Mozilla -> Firefox -> Profiles -> ...
- MacOS: Library -> Application Support -> Firefox -> Profiles -> ...
- Linux: $HOME/.mozilla/firefox/...

Hinweis: Wenn man feststellt, das die gewählte Variante zu restriktiv ist und man auf eine weniger restriktive Variante wechseln möchte, dann muss man im Profilverzeichnis die Dateien *user.js* und *prefs.js* löschen. Wenn man etwas dazwischen will, kann man man die weniger restriktive Variante wählen und die Einstellungen unter *about:config* ergänzen.

4.25 Snakeoil für Firefox (überflüssiges)

Auf der Website für Firefox Add-ons findet man tausende Erweiterungen. Man kann nicht alle vorstellen. Es kommen immer wieder Hinweise auf dieses oder jenes privacyfreundliche Add-on. Deshalb gibt es an dieser Stelle ein paar Dinge zusammengestellt, die nicht empfehlenswert sind.

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

Do-Not-Track ist am Lobbyismus gescheitert

Do-Not-Track (DNT) wurde 2009 von der EEF.org vorgeschlagen. Mit einem zusätzlichen HTTP-Header sollte der Browser den grundsätzlichen Wunsch des Nutzers übermitteln, nicht getrackt zu werden. Im Dezember 2010 erklärte die FTC die Unterstützung für DNT und 2012 begann das W3C mit der Standardisierung des Features.

Der eindeutige Wunsch der Nutzer, der mit Aktivierung von DNT im Browser zum Ausdruck gebracht wurde, wurde von der Trackingbranche ignoriert. Empirische Studien zeigten, dass sich das Tracking beim Surfen damit um weniger als 2% verringerte.

Es war ein genialer Schachzug von Microsoft, DNT im IE10 standardmäßig ohne Interaktion des Nutzers zu aktivieren. Das widersprach eindeutig den Intentionen des W3C Standard, der ausdrücklich definierte, das ein DNT-Header nur vom Browser gesendet werden darf, wenn der Nutzer damit einen Wunsch aktiv zum Ausdruck bringen möchte:

> *The basic principle is that a tracking preference expression is only transmitted when it reflects a deliberate choice by the user. In the absence of user choice, there is no tracking preference expressed.*
> ...
> *A user agent MUST have a default tracking prefernce of* ***unset*** *unless a specific tracking preference is implied by the user decision...*

Diese Aktivierung *by Default* gab der Trackingbranche den Vorwand, DNT offiziell zu ignorieren, da man nicht mehr davon ausgehen könne, das ein Nutzer sich aktiv dafür entschieden habe. Yahoo erklärte im Mai 2014, dass alle Dienste des Konzerns DNT ignorieren werden, es folgten Google und Facebook im Juni und Twitter zwei Jahre später.

Beim Start der Diskussion zu einer neuen, europäischen ePrivacy Verordnung im Jan. 2017 sollte ursprünglich die Respektierung von "Do-Not-Trackäls verpflichtend definiert werden. In dem 2019 vorgelegten Diskussionspapier zur ePrivacy Verordnung wurde dieser Punkt gestrichen. Gleichzeitig konnten Lobbyorganisationen erreichen, dass durch Werbung finanzierte journalistische Angebote zukünftig die Daten der Nutzer ohne Zustimmung verarbeiten dürfen. Damit werden die Regelungen der DSVGO ausgehebelt.

Die DNT-Arbeitsgruppe beim W3C hat 2019 die finale Spezifikation für DNT vorgelegt und die Arbeit beendet. In der Spezifikation wird unter 10.2 darauf ingewiesen, das eine Umsetzung der DNT Spezifikation und Nutzung der Möglichkeiten neue Ansätze für das Fingerprinting des Browsers bieten könnte. Aber *Do-Not-Track* ist bereits politisch gescheitert.

Laut Bloomberg haben nur 12% der Nutzer weltweit DNT aktiviert. Da DNT nicht nennenswert gegen Tracking schützt, schafft man mit der Aktivierung von DNT nur ein Differenzierungsmerkmal für das Fingerprinting des Browsers. Apple hat DNT deshalb aus dem Browser Safari entfernt. In Firefox deaktiviert man DNT unter *about:config* mit folgender Option:

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

Statt der Trackingprotection von Firefox ist uBlock Origin empfehlenswert.

Web of Trust (WOT)

WOT war ein Add-on, das den Surfer über die Reputation der besuchten Webseite informierte und häufig empfohlen wurde. Während des Surfens sammelt WOT Daten über den Besuch jeder Webseite und überträgt die Daten an die Betreiber des Dienstes. Die Daten werden mit schwacher Anonymisierung zu Profilen verknüpft und auch an die

Werbeindustrie verkauft, wie Reporter des NDR zeigten[78]. Die Daten konnten relativ einfach deanonymisiert werden und lieferten umfangreiche Informationen zu Krankheiten, sexuellen Vorlieben und Drogenkonsum einzeln identifizierbarer Personen.

Unschön, wenn über einen Richter bekannt wird, dass er eine Vorliebe für Sado-Maso-Praktiken hat oder wenn sich Valerie Wilms, Bundestagsabgeordnete der Grünen, aufgrund der Daten erpressbar fühlt.

Google Analytics Opt-Out

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

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

GoogleSharing

Das Add-on 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 meiner Meinung verbessert man seine Privatsphäre nicht, indem die Daten einem weiteren Dienst zur Verfügung stellt. Dass der eigene Rechner dabei auch unkontrolliert Daten von anderen Nutzern stellvertretend an Google weiterleitet, ist ein unnötiges Risiko. Google speichert diese Informationen und gibt sie bereitwillig an Behörden und als PRISM-Partner auch an Geheimdienste weiter. So kann man unschuldig in Verwicklungen geraten, die man lieber vermeiden möchte. 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 datenschutzfreundliche Alternativen nutzen: die Suchmaschine Ixquick.com oder Startingpage.com, für E-Mails einen Provider nutzen, der den Inhalt der Nachrichten nicht indexiert, openstreetmap.org statt Google-Maps verwenden…

Zweite Verteidigungslinie?

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

- *FlashBlock* blockiert Flash-Animationen. Das erledigt auch NoScript.
- *ForceHTTPS* kann für bestimmte Webseiten die Nutzung von HTTPS erzwingen, auch diese Funktion bietet NoScript.
- *Targeted Advertising Cookie Opt-Out* und *Ghostery* blockieren Surftracker. Es werden nur Tracker blockiert, die der oben genannten Kombination auch bekannt sind.

[78] https://www.tagesschau.de/inland/tracker-online-103.html

- *No FB Tracking* blockiert die Facebook Like Buttons, das können uBlock Origin oder AdBlock aber besser. Die SocialMediaBlock Listen für diese Werbeblocker blockieren nicht nur Facebook Like Buttons, sondern auch die Wanzen von anderen Social Networks.
- ....

Wer meint, es nutzen zu müssen - Ok.

Kapitel 5

Passwörter und 2-Faktor-Authentifizierung

Wenn man sich bei einem Webdienst anmeldet, um personalisierte Angebote zu nutzen (z. B. bei einem E-Mail Dienst, bei Twitter, Facebook oder einem Webshop) muss man sich als berechtigter User authentifizieren.

Für diese Authentifizierung gibt es mehrere Methoden, die man grob in folgende Gruppen einteilen kann:

Authentifizierung durch Wissen: Man muss nachweisen, dass man Kenntnis von einem Geheimnis hat, das Dritten nicht bekannt sein sollte (z. B. Passwort oder die Antwort auf eine Sicherheitsfrage). Ein Angreifer sollte dieses Geheimnis nicht von einem Zettel ablesen, es nicht erraten oder durch Ausprobieren knacken können.

Unter den Bedingungen der zunehmenden Videoüberwachung öffentlicher Plätze muss man auch damit rechnen, dass die Passworteingabe bei Nutzung von Smartphones durch Dritte beobachtet werden kann.

Risiko-basierte Authentifizierung (RBA) soll die Sicherheit von Accounts verbessern, die nur mit einem Passwort geschützt sind. Bei einem Loginversuch wird anhand von Merkmalen ein Risikolevel berechnet, ob möglicherweise ein missbräuchlicher Login erfolgt. Übersteigt der Risikolevel einen Grenzwert, wird eine zusätzliche Verifikation gefordert. In der Regel muss der Nutzer ein zusätzliches Token einzugeben, das per E-Mail, SMS o.ä. an eine vorher verifizierte Adresse gesendet wird.

Zur Berechnung des Risikolevels könnten die Zeit seit dem letzten Login, der Standort im Vergleich zum letzten Login, Uhrzeit, IP-Adresse, Browserversion, Tippverhalten bei der Eingabe des Passwortes oder andere Merkmale verwendet werden.

Die Akzeptanz von RBA ist bei den Nutzern wesentlich höher als eine 2-Faktor-Authentifizierung, da sie im Normalfall nur das Passwort eingeben müssen. 2-Faktor-Auth. wird in der Regel nur bei hohen Sicherheitsanforderungen akzeptiert.

RBA ist bei vielen großen Plattformen (Google, Amazon, PayPal, LinkedIn...) und auch bei Projekt wie Mastodon im Hintergrund aktiv, wenn man eine Adresse für die Verifikation angibt. Implikationen für die Privatsphäre muss man gegen den Sicherheitsgewinn abwägen. Wenn man 2-Faktor-Auth. verwendet, wird RBA meist deaktiviert.

RBA wird häufig *ein Art 2-Faktor-Authentifizierung* genannt, was aber nicht ganz korrekt ist. Man muss nicht den physischen Besitz eines Gerätes nachweisen, wie bei 2FA üblicherweise gefordert, sondern nur lesenden Zugriff auf eine Zieladresse, an die das Token gesendet wird. Die Sicherheit ist also geringer als bei 2FA.

Authentifizierung durch Besitz: Man muss nachweisen, dass man ein besonderes bzw. individuell konfiguriertes *Token* besitzt, das ein Angreifer nicht besitzen kann. Dabei unterscheidet man zwischen:

- *Harter Besitz* ist ein physisch vorhandenes, individuell konfiguriertes *Token*, welches nicht kopierbar ist (Yubikey, U2F-Stick, ePA, NitroKey...)
- *Weicher Besitz* ist eine Anhäufung speziell konfigurierter Bits und Bytes, die evtl. auf einem anderen Gerät gespeichert sind aber prinzipiell kopierbar sind (z. B. OTP-Apps oder X509 Zertifikate).

Im Consumer Bereich wird am häufigsten OTP (One-Time-Passwörter) mit Smartphone Apps oder Hardware Token angeboten. OTP schützt gegen Keylogger und gegen Mitleser unter den Bedingungen der Videoüberwachung. Es schützt nicht(!) bei Einbrüchen auf dem Server. Da bei OTP-Server und Client den gleichen Algorithmus ausführen, könnte ein Angreifer bei erfolgreichem Einbruch auf dem Server die Parameter auslesen und clonen.

Die modernere Variante ist U2F mit Public-Key Kryptografie. Es wird nur ein Public Key für die Authentifizierung auf dem Server gespeichert. Damit sind die Daten auch für einen Einbrecher wertlos. Allerdings wird U2F nur von wenigen Anbietern und bisher nur vom Browser Google Chrome unterstützt. Die breite Einführung dauert noch etwas.

Die Verwendung von Zertifikaten gibt es eher bei Business Anwendungen, Serveradministration (SSH) oder für hoheitliche Aufgaben (ePA).

Biometrische Merkmale: (Fingerabdruck, Iris) sind für starke Authentifizierung eher ungeeignet, weil man sie bei einer Kompromittierung nicht ändern kann.

Im privaten Bereich bieten viele moderne Smartphones inzwischen die Freigabe des Sperrbildschirm via Fingerabdruck Scan. In diesem Fall würde ich die Verwendung des Fingerabdruck gegenüber der oft üblichen Wischgeste bevorzugen, da man die Wischgeste leicht beobachten und kann, während der Fingerabdruck sehr viel komplizierter zu faken ist.

Prinzipiell ist es aber möglich, einen Fingerabdruck zu fälschen, wenn sich der Aufwand für ein *High Value Target* lohnt. Auf dem 31C3 demonstrierte Starbug, wie er den Fingerabdruck von Frau v.d. Leyen und den Iris Scan von Bundeskanzlerin Merkel mit einem hochauflösenden Kameraobjektiv während einer Pressekonferenz kompromittierte. Der Fingerabdruck von W. Schäuble wurde vom CCC ebenfalls kompromittiert und in einer PR Aktion publiziert, um die Schwächen biometrischer Merkmale für die Authentifizierung zu zeigen.

5.1 Hinweise für Passwörter

Jeder kennt das Problem mit den Passwörtern. Es sollen starke Passwörter sein, sie sollen für jede Site unterschiedlich sein und außerdem soll man sich das alles auch noch merken und auf keinen Fall auf einen Zettel "speichern".

- Was ist ein starkes Passwort? Diese Frage muss man unter Beachtung des aktuellen Stand der Technik beantworten. Wörterbuchangriffe sind ein alter Hut. Das Passwort darf kein Wort aus einem Wörterbuch wie z. B. dem Duden sein, das ist einfach zu knacken. Für zufällige Kombinationen aus Buchstaben, Zahlen und Sonderzeichen kann man Cloud Computing für Brute Force Angriffe nutzen. Dabei werden alle möglichen Kombinationen durchprobiert. Ein 6-stelliges Passwort zu knacken, kostet 0,16 Euro. Eine 8-stellige Kombination hat man mit 400 Euro wahrscheinlich und mit

850 Euro sicher geknackt. (Stand: 2011, Passwort Hashing mit SHA)

Man sollte mindestens 12 Zeichen verwenden, wenn das Passwort neben Groß- und Kleinbuchstaben auch Zahlen und Sonderzeichen enthält, und mindestens 16 Zeichen, wenn das Passwort keine Sonderzeichen enthält. Außerdem sollte es kein Wort sein, dass man in einem Wörterbuch finden könnte.

Um sich komplizierte, wechselnde Passwörter leichter zu merken, könnte man einen Basisteil von einem leicht merkbaren Satz ableiten und den variablen Anteil (vorn, hinten mittig?) aus dem verwendeten Dienst. Ein kleines Beispiel:

- Merksatz: *Die Sonne schien am ganzen Sonntag nur für uns.*
- Passwort für die Webseite Heise.de: *DSsagSn4u-HEIS*
- Passwort für den Jabber Account: *DSsgaSn4u-XMPP*
- ...

Der Vorteil eines memorierbaren Passwort Systems ist, dass man die Passwörter nie irgendwo speichern muss und sie auch bei einem Crash des PC nicht verlieren kann, weil man das Backup vergessen hat.

- Warum sollte man nicht das gleiche Passwort für viele Logins verwenden? Diese Frage beantwortet der Hack von Anonymous gegen HBGary. Den Aktivisten von Anonymous gelang es, Zugang zur User-Datenbank des Content Management Systems der Website zu erlangen. Die Passwörter konnten geknackt werden. Die Passwörter wurden vom Führungspersonal für weiterer Dienste genutzt: E-Mail, Twitter und Linked-In. Die veröffentlichten 60.000 E-Mails waren sehr peinlich für HBGary [1].
- Im Sommer 2018 kursierten mehrere tausend Logindaten (Benutzername, Passwort) für den Dienst MEGA in den einschlägigen Darknet Foren. Die Login Credential stammten nicht aus einem Hack von MEGA sondern wurden durch automatisiertes Ausprobieren von Benutzername + Passwort Kombinationen aus anderen erfolgreichen Hacks ermittelt. Gegen dieses **Credential Stuffing** kann man sich nur schützen, indem man unterschiedliche Passwörter für verschiedene Dienste verwendet.

Firefox build-in Passwortspeicher

Wie alle anderen Browser hat auch Firefox einen Login Manager. Wenn man auf einer Webseite Login Credentials eingibt, fragt Firefox standardmäßig, ob er die Zugangsdaten für diese Webseite speichern soll. Zukünftig wird dann beim nächsten Aufruf der Webseite das Login Formular automatisch mit den passenden Daten ausgefüllt.

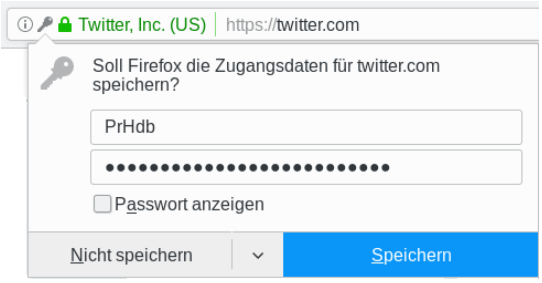


Abbildung 5.1: Login Credentials für eine Webseite in Firefox speichern

Wenn man in der Konfiguration ein Masterpasswort setzt, werden die Passwörter (nur die Passwörter, nicht die Usernamen) mit 3DES verschlüsselt. Der 3DES-Cipher ist

[1] https://www.heise.de/ct/artikel/Ausgelacht-1195082.html

zwar nicht State-of-the-Art und hat Schwächen, bei kleinen Datenmengen ist es aber hinreichend sicher.

Risiken bei der Nutzung des Firefox build-in Passwortspeichers:

1. Einige Trackingdienste exploiten die build-in Passwortspeicher von Browsern, indem ihre Trackingscripte ein verdecktes Login Formular generieren. Wenn der Surfer einen Account bei der Webseite hat, werden die Formulare vom Browser automatisch ausgefüllt. Die Trackingscripte interessieren sich für den Usernamen, der oft eine E-Mail Adresse ist. Ein MD5-Hash des Usernamen wird dann als nicht löschbare, eindeutige Tracking-ID genutzt.

   Die Studie *Web trackers exploit browser login managers* hat 1.110 Webseiten gefunden, bei denen diese Trackingtechnik in-the-wild eingesetzt wird.[2]

2. Mit XSS-Angriffen können ebenfalls verdeckte Login Formulare generiert werden, die vom Browser automatisch ausgefüllt werden, wenn man einen Account für diese Webseite hat. Das Konzept ist das gleiche wie bei den Trackingdiensten. Allerdings muss der Angreifer sein Script ohne Unterstützung des Webmasters in die Webseite hinein manipulieren. Außerdem wollen die Angreifer nicht nur den Usernamen als eindeutige ID verwenden sondern auch das Passwort abgreifen.

3. Es gibt seit Jahren immer wieder Viren und Trojaner, die es gezielt auf die Passwortdatenbank von Firefox abgesehen haben und diese Datenbank zu ihrem Master of Control senden. Deshalb sollten die Passwörter unbedingt mit einem Masterpasswort gesichert werden. Das schützt die Passwörterr, der Angreifer erhält aber trotzdem die Informationen, welche Accounts das Opfer auf welchen Webseiten nutzt.

Schutz gegen die Risiken:

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

  ```
  signon.rememberSignons = false
  ```

  Wenn man den *Private Browsing Mode* aktiviert, werden ebenfalls keine Login Credentials gespeichert.

- Wer es lieber etwas moderater bevorzugt und den built-in Passwortspeicher verwenden möchte, kann das Risiko verringern, indem man das automatische Ausfüllen von Formularen deaktiviert. Dann muss man die ersten Buchstaben des Usernamens in das Formular schreiben und kann in dem sich öffnenden Drop-Down Menü mit einem Mausklick den Usernamen und Passwort übernehmen.

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

Passwortspeicher

Passwortspeicher sind kleine Tools, die Username/Passwort Kombinationen und weitere Informationen zu verschiedenen Accounts in einer verschlüsselten Datenbank verwalten. Es gibt mehrere Gründe, die für die Verwendung eines Passwortspeichers sprechen:

[2] https://freedom-to-tinker.com/2017/12/27/no-boundaries-for-user-identities-web-trackers-exploit-browser-login-managers/

- Viele Programme (z. B. Pidgin) speichern Passwörter unverschlüsselt auf der Festplatte, wenn man die Option zur Speicherung der Passwörter nutzt (nicht empfohlen!). Andere Programme bieten keine Möglichkeit zur Speicherung von Passwörtern, fordern aber die Nutzung einer möglichst langen, sicheren Passphrase (z. B LUKS oder Veracrypt).

- Bei vielen Accounts muss man sich neben Unsername und Passwort weitere Informationen merken wie z. B. die Antwort auf eine Security Frage oder PINs bei Bezahldienstleistern.

- In der Regel enthalten Passwortspeicher eine Passwortgenerator, der wirklich zufällige und starke Passwörter generieren kann.

- Das Backup wird deutlich vereinfacht. Man muss nur die verschlüsselte Datenbank auf ein externes Backupmedium kopieren.

- Im Gegensatz zum Firefox Build-in Speicher werden alle Informationen verschlüsselt gespeichert, nicht nur die Passwörter.

Mir gefallen **KeePassX2** (für ältere Linux Distributionen) oder **KeePassXC** (Windows, MacOS, Ubuntu 18.04+, Fedora 28+) sehr gut. KeePassXC ist eine Weiterentwicklung der Community, für die es auch das Add-on *KeePassXC-Browser*[3] zur Integration in Firefox gibt. Bei Verwendung dieses Add-on entfallen die Risiken bei der Übergabe von Passwörter via Zwischenablage (siehe unten). Die Konfiguration für das Add-on ist in der Dokumentation von KeePassXC beschrieben.[4]

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

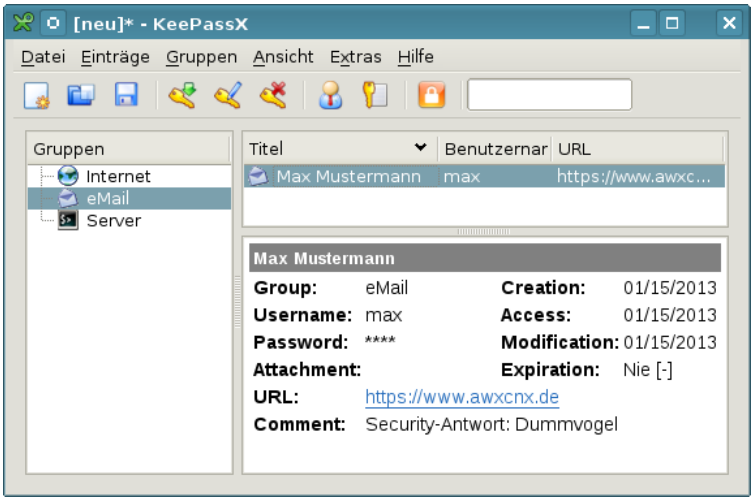


Abbildung 5.2: KeepassX Hauptfenster

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

[3] https://addons.mozilla.org/de/firefox/addon/keepassxc-browser
[4] https://keepassxc.org/docs/keepassxc-browser-migration

Warnung: Zwischenablage für Linux Desktops

Die Linux Desktops wie KDE, Gnome oder XFCE enthalten Tools zur Verwaltung der Zwischenablage. Diese Tools speichern die letzten (n) Einträge, die in die Zwischenablage kopiert wurden und schreiben diese Einträge in der Standardkonfiguration meist unverschlüsselt auf die Festlatte.

- Klipper (KDE Desktop) speichert die Daten in *$HOME/.kde/share/apps/klipper/history2.lst*
- Clipman (XFCE Desktop) speichert die Daten *$HOME/.cache/xfce4/clipman/textsrc*

Wenn man Passwortmanager wie KeepassX verwendet und die Passwörter wie vorgesehen via Zwischenablage kopiert, dann landen auch diese sensiblen Informationen unter Umständen unverschlüsselt auf der Festplatte und die verschlüsselte Speicherung in der Passwortdatenbank wird sinnlos. Um diese Lücke zu vermeiden, müssen die Tools zur Verwaltung der Zwischenablage vernünftig konfiguriert werden. Sie sollten nur wenige Einträge speichern und auf keinen Fall Daten unverschlüsselt auf die Festplatte schreiben oder nicht automatisch gestartet werden, wenn die Speicherung nicht deaktivierbar ist.

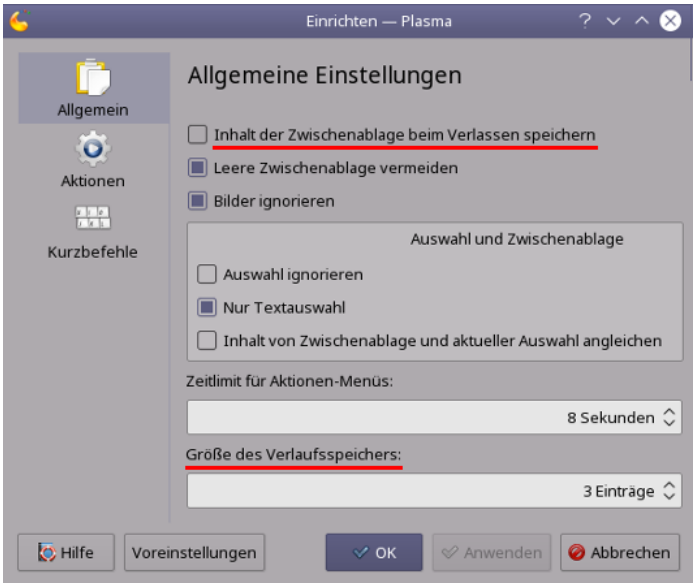


Abbildung 5.3: Konfiguration der KDE Zwischenablage Klipper

Als Beispiel zeigt Bild 5.3 die Konfiguration für die KDE Zwischenablage Klipper und Bild 5.4 zeigt, wie man den automatischen Start der Verwaltung der Zwischenablage Clipman in den XFCE Einstellungen für Sitzung und Startverhalten deaktiviert.

5.2 Zwei-Faktor-Authentifizierung

Einige Webdienste bieten Zwei-Faktor-Authentifizierung (2FA) als Alternative zum einfachen Login mit Username/Passwort an. Die Webseite http://www.dongleauth.info bietet eine Übersicht zu Webdiensten, die OTP oder U2F für den sicheren Login unterstützen.

Bei der Zwei-Faktor-Authentifizierung muss man als ersten Faktor in der Regel ein Wissen nachweisen (Passwort, PIN) und als zweiten Faktor den Besitz eines kleinen Gerätes (OTP-Generator o.ä.) oder einer Chipkarte wie bei Bankaccounts. Das Verfahren ist durch

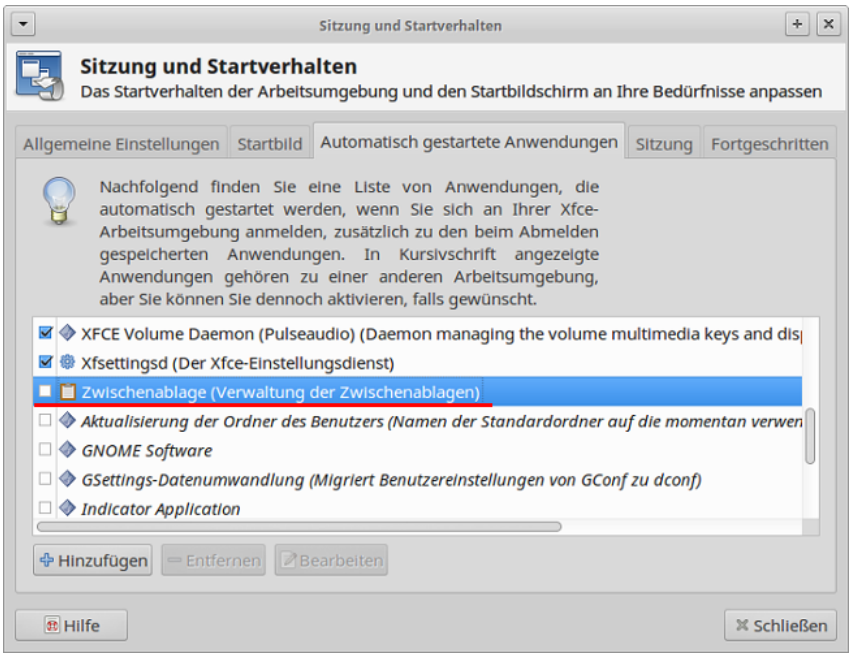


Abbildung 5.4: Starten von Clipman deaktivieren (XFCE Desktop)

Nutzung von EC- und Kreditkarten jedem bekannt. Internet verwendet man statt Chipkarte meist One-Time-Passwort Generatoren oder SecuritySticks (U2F, WebAuthn).

Wenn ein Angreifer durch Phishing, Videoüberwachung oder mit einem Keylogger den Usernamen und das Passwort für einen Account erbeutet, dann sollte es ohne den zweiten Faktor wertlos und nicht nutzbar sein. Das Passwort wird damit nicht überflüssig, es muss aber kein hochkomplexes, sicheres Passwort mehr sein. Eine 6-stellige Zahlenkombination ist nach NIST Special Publication 800-63B ausreichend.

2-Faktor-Authentifizierung für das Online Banking

Mit der europäischen Zahlungsrichtlinie PSD2 wird für die Online-Abwicklung von Bankgeschäften die 2-Faktor-Auth. auch für den Login bei Webseiten zur Zahlungsabwicklung zwingend vorgeschrieben. Banken haben unterschiedliche Lösungen entwickelt, die sich von den üblichen Lösungen für 2-Faktor-Auth. bei anderen Webdiensten unterscheiden. Banken verwenden in der Regel einen TAN-Generator als 2. Faktor und definieren den Geschäftsfall *Login*, da die Technk für Authorisierung von Transaktionen vorhanden ist.

chipTAN, Sm@rt-TAN verwenden Hardware TAN-Generatoren, welche die EC-Chipkarte der Bank für die Generierung einer TAN verwenden. Sie sind für hohe Sicherheitsanforderungen geeignet, da sie ein seperates Gerät verwenden, das nicht mit dem Internet verbunden ist. Die Daten für die Generierung einer TAN können entweder optisch zwischen PC und TAN-Generator übertragen werden (durch Scannen eines Code, der auf dem Bildschirm angezeigt wird) oder manuelle Eingabe.

photoTAN, SecureGo verwenden Smartphone Apps für die Generierung einer TAN. Die Verfahren sind für den Kunden billiger, da er kein zusätzliches Gerät kaufen muss. Sie sind aber weniger sicher, da ein Smartphone leichter kompromittiert werden kann.

Außerdem enthalten Smartphone Apps immer wieder unterschiedliche Tracker, die das Nutzungsverhalten verfolgen. Die *SecureGo App* der Fiducica & GAT IT AG enthält zwei Tracker, unter anderem Google Firebase Analytics. Ein positives Beispiel ist die *photoTAN App* der Commerzbank, die keine Tracker enthält.

Welche Optionen man hat, muss man bei Kundensupport der Bank erfragen. Auch wenn es etwas umständlicher ist, würde ich beim Umgang mit Geld immer die sichers-

te Lösung bevorzugen und Hardware TAN-Generatoren in Kombination mit meiner EC-Chipkarte nutzen.

2-Faktor-Authentifizierung für Webdienste

Für den Login bei Webdiensten werden für die 2-Faktor-Authentifizierung andere Verfahren genutzt, als beim Online Banking:

OTP: Bei der Zwei-Faktor-Authentifizierung mit zusätzlichem One-Time-Passwort besteht das Passwort aus zwei Komponenten, die nacheinander oder manchmal auch zusammen in das gleiche Passwortfeld eingegeben werden. Der erste Teil ist üblicherweise ein n-stellige PIN, die man wissen muss. Der zweite Teil ist das One-Time-Passwort. Es wird von einem kleinen Spielzeug (Tokengenerator) geliefert und ist nur einmalig verwendbar.

Es gibt mehrere Verfahren für die Zwei-Faktor-Auth. mit OTP:

- **HOTP** (HMAC-based OTP) nutzt One-Time-Passwörter, die aus einem HMAC-SHA1 Hashwert abgeleitet werden, der aus einem Zähler und einem gemeinsam Secret berechnet wurde. Sie sind beliebig lange gültig aber die Verwendung eines Token mit größerem Zählerwert erklärt auch alle Token mit niedrigerem Counter für ungültig.

  Tipp: Wenn man seinen OTP-Generator nicht in den Urlaub o.ä. mitnehmen möchte, kann man sich eine Liste von HOTP-Token generieren lassen und diese Zahlenkombinationen nacheinander zum Login unterwegs verwenden. Außerdem ist es schwieriger, ein HOTP Token zu klonen ohne entdeckt zu werden.

- **TOTP** (Time-based OTP) nutzt One-Time-Passwörter, die auf Basis der aktuellen Uhrzeit berechnet werden und nur innerhalb einer kurze Zeitspanne einmalig verwendet werden können.

  Die HOTP oder TOTP Passwörter können von einem Hardware Token (z. B. *Nitrokey Pro* mit der Nitrokey-App) generiert werden oder mit einer Smartphone App (*FreeOTP* für Android oder *OTP Auth App* für iPhone). Wenn ein Smartphone genutzt wird muss man die angezeigte Zahlenkombination per Hand in das Login Formular abtippen. Bei der Verwendung von TOTP hat man dafür 30sec bzw. 60 sec Zeit.

  Zwei-Faktor-Authentifizierung mit One-Time Passwörtern (OTP) erschwert Phishing Angriffe. Das ist das Angreifermodell, und nur dagegen bietet OTP verbesserten Schutz. OTP macht Phishing Angriffe aber nicht unmöglich. Bruce Schneier hat in der Theorie bereits 2009 darauf hingwiesen. 2018 haben potente Hacker begonnen, 2-Faktor-Auth mit OTP in größerem Umfang auszutricksen.

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

  - Die Sicherheitsfirma CERTFA berichtete Dez. 2018 in dem Blogartikel von einer Spear-Phishing Kampagne iranischer Hacker gegen Google und Yahoo! Accounts, welche die 2-Faktor Auth. austricksen konnte.[5]
  - Amnesty International berichtete ebenfalls von einer Phishing Angriffswelle aus Nahost gegen die Accounts von Aktivisten, welche die 2-Faktor-Auth von ProtonMail, Tutanota, Google und Yahoo! austricksen konnte.[6]
  - Im Januar 2019 wurde auf Github die Software Muraena und NecroBrowser[7] als Open Source veröffentlicht, die Phishing Angriffe auf 2-Faktor-Auth mit OTP automatisiert ausführen kann. Der Angreifer lockt das Opfer mit Phishing E-Mails o.ä. zum Login auf seine Webseite. Dort arbeitet Muraena als Reverse-Proxy, der sich unbemerkt zwischen Nutzer und Webdienst einschleicht und die Authentifizierung an den richtigen Server weiterleitet. Nachdem die Session aufgebaut wurde, extrahiert Muraena die Session

[5] https://blog.certfa.com/posts/the-return-of-the-charming-kitten/
[6] https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/
[7] https://github.com/muraenateam

Cookies oder Session-IDs und reicht sie an eine Instanz des NecroBrowsers weiter. Das Schließen der Session (Logout) wird von Muraena blockiert und dem Nutzer wird vorgegaukelt, er hätte sich abgemeldet. Danach kann der Angreifer mit dem NecroBrowser unbemerkt den Account übernehmen.

– Wenn es einem Angreifer gelingt, zwei oder mehr TOTP Token abzugreifen und den Zeitpunkt der Verwendung zu protokollieren, kann er mit dem Tool *hashcat* versuchen, die Secret Keys ermitteln und dann selbst gültige TOTP Token erzeugen.

  1. Die abgeschorchelten Token schreibt man zusammen mit den Zeitstempel im Format in eine Textdatei (in diesem Beispiel: *totp-inputs.txt*):

     ```
     833060:1263384780
     549115:1528848780
     ```

  2. Mit dieser Datei füttert man *hashcat* und protokolliert die Ergebnisse:

     ```
     > hashcat -m17300 -a3 -o totp.potfile totp-inputs.txt ?l?l?l?l?l?l?l
     ```

  3. Nach einigen Stunden oder Tagen Rechenzeit (abhängig von Rechenleistung und Qualität der Keys) schaut man sich die Ergebnisse an:

     ```
     > cut -d: -f3 totp.potfile | sort | uniq -c | sort -nr | head
     ```

     Die Ergebnisliste kann man von oben beginnend ausprobieren. Nach weiteren 5min hat man einen TOTP Secret Key, der die Generierung gültiger Token ermöglicht, und man kann den Account übernehmen:

     ```
     > oauthtool --base32 --totp "Secret Key" -d 6
     ```

  OTP schützt nicht bei Einbrüchen auf dem Server. Da bei OTP der Server und Client den gleichen Algorithmus zur Berechnung und Verifizierung des One-Time-Passworts ausführen, kann ein Angreifer bei einem erfolgreichem Einbruch auf dem Server die OTP Parameter auslesen und somit gültige OTP Token berechnen, insbesondere für TOTP ist es einfach, dabei unendeckt zu bleiben:

  ```
  > oauthtool --base32 --totp <Secret Key> -d 6
  ```

  Aus dem gleichen Grund schützt 2-Faktor-Auth mit OTP nicht beim Zugriff staatlicher Behörden auf Passwort Hashes, wie es in dem Feb. 2020 von der Regierung beschlossenen *Gesetzes zur Bekämpfung von Rechtsterrorismus* und Hasskriminilatät[8] vorgesehen ist. Und das schließt die Parameter zur Berechnung der OTP ein. Gegen diesen Angriff ist auschließlich die Stärke des ersten Faktors (Passwort) relevant und das Hashverfahren, welches der Provider zum Schutz des gespeicherten Passwortes einsetzt.

- **YubicoOTP:** ist ein properitäres Protokoll der Firma Yubico. Es wird ein USB-Stick genutzt, der sich wie eine Tastatur verhält. Man aktiviert das Passwortfeld und drückt dann eine Taste auf dem USB-Stick. Damit wird das One-Time-Passwort in das Eingabefeld geschrieben und man kann das Formular abschicken. Neben dem einfachen Yubico Stick gibt es den Yubico NEO, der auch als OpenPGP Smartcard genutzt werden kann und auch als U2F SecurityStick.

  Der Webdienst, bei dem man sich anmeldet, sendet das Einmalpasswort in der Regel über eine API an die YubiCloud und lässt es dort verifizieren. Nur wenige Webdienste bieten gebrandete Yubikeys und betreiben einen eigenen Server zur Validierung. Bezüglich Schutz gegen Phishing gilt das Gleiche wie für TOTP/HOTP.

FIDO-U2F: ist ein kryptografisches Privat/Public Key Verfahren zur Authentifizierung mit einem kleinen SecurityStick (z. B. *Nitrokey U2F*[9] oder verschiedene *Yubikeys*[10]), das im Okt. 2014 standardisiert wurde.

Das Verfahren läuft im Hintergrund automatisch ab, man muss nur den U2F-Stick vor dem Login anschließen. Der Server sendet ein zufälliges Challenge an den Client

[8] https://www.golem.de/news/hasskriminalitaet-regierung-will-passwortverschluesselung-nicht-aushebeln-2002-146727.html
[9] https://www.nitrokey.com/de
[10] https://www.yubico.com/products/yubikey-hardware/

(Browser), der Browser gibt diesen Input zusammen mit der Login URL, die er sieht, an den U2F-Stick weiter, der mit einem geheimen Schlüssel eine Signatur über diese Daten berechnet. Diese Signatur wird als Response an den Server zurück geschickt und kann dort mit dem passenden public Key verifiziert werden. Dabei wird für jeden Web-Account ein anderer Key verwendet.

Vorteile von FIDO-U2F gegenüber One-Time-Passwörtern:

1. Da asymmetrische Kryptografie genutzt wird, kennt der Server nur einen public Key. Wenn ein Angreifer den Server kompromittiert, kann er die U2F Auth. nicht aushebeln.
2. Da die Login URL, die der Browser sieht, in die Berechnung der Signatur einfließt, schützt U2F auch gegen alle Angriffe mit Phishing Webseiten. Um Software wie Muraena + NecroBrowser gegen FIOD-U2F Auth. einzusetzen, müsste der Angreifer die TLS-Verschlüsselung knacken und sich als *Man-in-the-Middle* in die TLS-verschlüsselte Kommunikation zwischen Browser und Webdienst einklinken.

FIDO-U2F muss vom Browser und vom Webdienst unterstützt werden. Bisher bietet Google Chrome nativen Support für U2F. Mozilla arbeitet an einer Implementierung für Firefox (Bug: #1065729). Bisher ist die Umsetzung noch nicht ganz vollständig. Man kann U2F in Firefox aktivieren, indem man folgende Variable unter *about:config* setzt:

```
security.webauth.u2f = true
```

Auf der Testseite von Yubico[11] kann man prüfen, ob man mit U2F einen Account erstellen den U2F-Stick für einen Dummy Login nutzen kann. Außerdem soll die Firefox Implementierung mit Google Accounts und Github problemlos funktionieren.

(Für Firefox Nutzer: Man sollte sich aber auch überlegen, ob man für sicherheitsrelevante Aufgaben wirklich Implementierungen im Beta Status verwenden möchte.)

WebAuthn/FIDO2 ist ein Standard des W3C, der im März 2019 verabschiedet wurde und von den Großen der IT-Branche unterstützt wird. WebAuthn ist eine Weiterentwicklung von FIDO-U2F und soll den Login mit Username / Passwort Kombinationen komplett ersetzen können.

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

WebAuthn/FIDO2 erweitert FIDO-U2F um folgende Punkte:

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

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

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

[11] https://demo.yubico.com/u2f

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

SMS: SMS-basierte Verfahren zur Authentifizierung gelten als nicht mehr sicher. Es gibt mehrere Publikationen zu dem Thema. Das NIST, BSI u.a. empfiehlen, SMS nicht mehr für die Authentifizierung zu nutzen.[12]

SMS-basierte Verfahren können mit SIM-Swap Angriffen oder SS7-Hijacking ausgehebelt werden. Das musste Twitter-CEO Jack Dorsey lernen, als sein Twitter Account trotz aktivierter 2-Faktor-Auth kompromittiert wurde. Ein Fehler beim Mobilfunkanbieter sei schuld gewesen, erklärte Twitter später, was auf einen erfolgreichen SIM-Swap hindeuten könnte.

ePerso: In Auswertung des US-Wahlkampfes 2016 und dem erheblichen Einfluss von gehackten E-Mail Accounts auf das Wahlverhalten der amerikanischen Bevölkerung hat die Bundesregierung die Cyber-Sicherheitsstrategien überarbeitet. Nach Ansicht der Bundesregierung ist die Sicherheit mit dem klassischen Benutzername/Passwort-Verfahren nicht mehr gegeben. Im Rahmen Cyber-Sicherheitsstrategien will die Regierung die Bürger stärker zur Nutzung der Onlineausweisfunktion des Personalausweises animieren.

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

5.3 Phishing Angriffe

Phishing ist eine der Plagen im Internet. Der Lagebericht des BSI zur IT-Sicherheit 2017 nennt diese Angriffe als zweitgrößte Gefahr nach den Erpressungstrojanern. Es gibt dabei ganz unterschiedliche Intentionen der Angreifer, um die Kontrolle über einen Account des anvisierten Opfers zu erlangen:

- Geheimdienste versuchen, die Accounts von politischen Oppositionellen zu hacken, um das Kontakt Netzwerk zu analysieren und die Kommunikation zu beobachten. Mit diesem Hintergrund wurden die Twitter Accounts von Erdogan-Kritikern von türkischen Hackern angegriffen.[13]

- Der *CEO-Hack* ist eine spezielle Version von Phishing Angriffen, bei dem gezielt die E-Mail Accounts von Führungspersonen in Firmen angegriffen werden. Dabei werden die Phishing Mails optimal auf die Zielperson zugeschnitten. Ziel ist es, die E-Mail Kommunikation zu beobachten und gezielt einzelne E-Mails wie z. B. Rechnungen zu manipulieren um Zahlung auf andere Konten umzuleiten. B. Schneier beschreibt in seinem Blog ein Beispiel für einen erfolgreichen *CEO-Hack* gegen eine Galerie.[14]

  > Criminals hack into an art dealer's email account and monitor incoming and outgoing correspondence. When the gallery sends a PDF invoice to a client following a sale, the conversation is hijacked. Posing as the gallery, hackers send a duplicate, fraudulent invoice from the same gallery email address, with an accompanying message instructing the client to disregard the first invoice and instead wire payment to the account listed in the fraudulent document.
  >
  > Once money has been transferred to the criminals' account, the hackers move the money to avoid detection and then disappear. The same technique is used to intercept payments made by galleries to their artists and others.

[12] https://pages.nist.gov/800-63-3/sp800-63b.html
[13] https://netzpolitik.org/2017/angriffe-gegen-twitter-accounts-von-erdogan-kritikern
[14] https://www.schneier.com/blog/archives/2017/11/cybercriminals_.html

- Auch ganz normale, nicht exponierte Internetnutzer werden mit Phishing Angriffen konfrontiert. Für Kriminelle ist dabei alles interessant, was mit Geld zu tun hat (z. B. PayPal.com, Amazon Konten o.ä.) Spammer versuchen, verifizierte E-Mail Accounts zu kapern und das Adressbuch des Opfers zu nutzen, um dann bei Empfängern der Spam Nachrichten das Vertrauen in den bekannten Absender auzunutzen. Dabei kann es manchmal zu kuriosen Missverständnissen kommen:

  My religious aunt asked why I was trying to sell her viagra!

  In der Regel werden normale Internetnutzer mit Bulk-Phishing attackiert. Die Angreifer versenden eine E-Mail mit alarmierendem Inhalt an tausende Empfänger in der Hoffnung, dass ein kleiner Teil der Empfänger so naiv ist und auf den Link-Button in der Mail klickt, um die Login Credentials auf der Phishing Webseite einzugeben.

  Beispiele für den Inhalt von ganz normalen Phishing E-Mails:

  - *Das Passwort für Ihren Account wurde kompromittiert! Bitte loggen Sie sich sofort ein und ändern Sie ihr Passwort.*
  - *Ihr PayPal Account muss neu verifiziert werden, bitte loggen Sie sich hier ein und...*
  - *Ihr Amazon Konto wurde deaktiviert, bitte loggen Sie sich ein und...*
  - *Ihre Lieferung wurde storniert, weitere Informationen finden Sie hier.*

  Professionelle Phishing Mails sind dem Design der originalen E-Mails sehr gut nachgemacht und für Laien schwer erkennbar. IT-Profis könnten sich die Header der Mails anschauen oder die Links genauer prüfen, aber das möchte man auch nicht für jede E-Mail ständig machen. Deshalb gibt es keine weitere Ratschläge für diesen Ansatz.

Abbildung 5.5: Beispiel für eine Phishing Mail

Schutz gegen Phishing Angriffe

Als Schutz gegen Phishing Angriffe empfehlen wir, Webseiten mit Formularen zur Eingabe von Login Credentials IMMER über Lesezeichen oder durch Eingabe der URL per Hand zu öffnen. Man sollte NIE auf die Link Buttons in irgendwelchen E-Mails klicken, um Login-Seiten für Accounts auszurufen. Dabei ist es egal, wie vertrauenswürdig eine Mail aussieht.

Es ist verführerisch einfach, schnell mal auf den Button oder Link zu klicken, wenn die Phishing Mail gut gemacht ist. Aber es ist auch nicht viel komplizierter, ein Lesezeichen oder die URL aus einem Passwortmanager wie KeePassXC aufzurufen.

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

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

Kapitel 6

Bezahlen im Netz

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

Die Nutzung von PayPal.com ist das Gegenteil von anonym. Bei jedem Zahlungsvorgang wird eine Verknüpfung von persönlichen Daten (E-Mail Adresse, Kontoverbindung) und gekauften Waren hergestellt. Die Daten werden an mehr als 100 Firmen übertragen zum Monitoring der Überweisung.

PayPal.com nutzt seine Marktposition für die Durchsetzung politischer Interessen der USA. Gemäß der Embargo-Politik der USA werden Internetnutzer in über 60 Ländern ausgesperrt. Internationales Aufsehen erregte die Sperrung der Konten von Wikileaks. Daneben gibt es viele weitere Fälle. Mehr als 30 deutschen Online-Händlern wurden die Konten gesperrt [1], weil sie kubanische Produkte (Zigarren, Rum, Aschenbecher) in Deutschland anboten. Die Sperre wurde mit einem amerikanischen Handelsembargo gegen Kuba begründet, das für Europäer belanglos ist.

Aufgrund dieser politischen Instrumentalisierung hat *Anonymous* zum Boykott von PayPal.com aufgerufen und an Nutzer appelliert, ihre Accounts bei diesem Bezahldienst zu kündigen.

Zukünftig möchte PayPal.com auch in der realen Welt präsent sein. Das Bezahlsystem soll die Geldbörse in zwei Jahren ersetzen, wie Ebay-Chef John Donahoe sagte, natürlich mit den üblichen Schnüffeleien:

> *Beim Einsatz von PayPal in den Geschäften könnten die Einzelhändler mehr über Vorlieben ihrer Kunden erfahren und sie entsprechend besser bedienen.*

Rechnung oder **Überweisung** (Vorkasse) sind privacy-freundliche Bezahlmethoden, da nur die beiden Kreditinstitute von Käufer und Verkäufer in den Bezahlprozess eingebunden sind. Außerdem sind es sichere Bezahlmethoden, die nicht durch (unzulässige) Speicherung von Daten kompromittiert werden können. Via Online Banking ist es auch am PC nutzbar. Leider werden diese Methoden nicht überall angeboten.

Kreditkarten werden von einer Bank ausgegeben. Die Abwicklung des Bezahlvorgangs wird bei Visa und Mastercard aber von sogenannten Payment Processoren übernommen. Teilweise sammeln diese Payment Processoren Daten über online und offline Einkäufe und verkaufen die Daten an große Datensammler wie Acxiom oder BlueKai, wo sie mit anderen persönlichen Daten zusammengeführt werden.

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

[1] http://heise.de/-1320630

In dem Patent wird beschrieben, wie die Kreditkartenfirmen aus den Einkäufen anhand der Konfektions- und die Schuhgrößen die Größe und das Gewicht des Karteninhabers ermittlen können. Diese Daten könnten an Fluggesellschaften verkauft werden, die damit die Sitzverteilung für die Passagiere optimieren könnten.

Die Sicherheit von Kreditkarten als Zahlungsmittel wird öfters durch unsachgemäße Datenspeicherung beim Verkäufer oder einem Partner des Verkäufers kompromittiert. Eine dreistellige Prüfziffer soll den Missbrauch von Kreditkartennummern für unberechtigte Einkäufe zu Lasten des Karteninhabers verhindern. Wenn aber der Payment Processor oder sein Sub-Kontraktor die Prüfziffer zusammen mit der Kartennummer dauerhaft speichert und die Datenbank unzureichend gesichert ist. . . - dann haben Kunden möglicherweise ein Problem, z. B. Millionen Hotelgäste, die via Booking.com oder Expedia gebucht hatten.[2]

Virtuelle Kreditkarten werden inzwischen von vielen Geldinstituten angeboten. Wenn man bereits einen verifizierten Account bei dem Kreditinstitut hat, ist die Erstellung einer virtuellen Kreditkarte online mit wenigen Klicks erledigt. Man bekommt die Kartennummer, Ablaufdatum und Prüfziffer sofort digital zugestellt aber keine Plastikkarte. In der Regel handelt es sich dabei um Debit Karten, die man vor der ersten Verwendung erstmal aufladen muss.

Die Kosten für virtuelle Kreditkarten sind meist geringer als vergleichbare echte Kreditkarten vom gleichen Anbieter aber sehr unterschiedlich. Bei KREDU kosten sie 149,- Euro pro Jahr + Zinsen für den Kredit, bei der Sparkasse 12,- Euro pro Jahr. . .

Virtuelle Kreditkarten könnte man regelmäßig wechseln (z. B. jährlich) und damit einige Sicherheitsprobleme bei der Nutzung von Kreditkarten im Internet reduzieren. Außerdem erschwert man Datensammlern die Verknüpfung von Online- und Offline Aktivitäten, wenn man verschiedene Kreditkarten Online und Offline nutzt.

Disposable Virtual Cards werden von besonders innovativen Kreditinstitute angeboten. Bei diesen Kreditkarten ändert sich die Kartennummern automatisch. Nach jeder Transaktion wird eine neue Kartennummer generiert. Falls die Datenbanken der Online-Händler später von Hackern kompromittiert werden, sind alte Kreditkartennummern wertlos. Außerdem wird die Auswertung für Datensammler erschwert, da Einkäufe nicht anhand von Kreditkarten verknüpft werden können.

Die Schweizer Revolut bietet Disposable Virtual Cards für ihre Premiumkunden, ecoPayz bietet dieses Feature ab Silver Level, Eno von Capital One. . . u.a.m.

Disposable Virtual Cards sind sicherer und privacy-freundlicher aber nicht anonym.

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

> *Bei jeder Transaktion über Google Pay können wir Informationen zur Transaktion erheben. Hierzu zählen: Datum, Uhrzeit und Betrag der Transaktion, Händlerstandort und -beschreibung, eine vom Verkäufer bereitgestellte Beschreibung der gekauften Waren oder Dienste, Fotos, die Sie der Transaktion beigefügt haben, der Name und die E-Mail-Adresse des Verkäufers und Käufers bzw. des Absenders und Empfängers, die verwendete Zahlungsmethode, [. . .]*

Kein weiterer Kommentar nötig - ist ein ganz normaler Google Service.

SOFORT Überweisung ist ein Online-Zahlungssystem zur bargeldlosen Zahlung im Internet. Bei dem Bezahlvorgang stellt der Kunde dem Zahlungsdienstleister Sofort GmbH die notwendigen Credentials für den Online Zugriff (PIN usw.) auf sein Konto zur Verfügung. Die Sofort GmbH nutzt diese Informationen, um sich Daten über Kontostand u.ä. zu holen und danach die Transaktion auszuführen.

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

Würde man das Verfahren in die Offline-Welt übertragen, könnte man die Dienstleistung der SOFORT Überweisung wie folgt beschreiben: Weil man selbst zu faul ist, gibt man einem Fremden auf der Straße die EC-Karte und PIN, damit er zum Bankautomaten geht, sich über den Kontostand und die letzten Transaktionen informiert um danach die gewünschte Überweisung auszuführen.

In den AGBs verbieten es alle Banken und Sparkassen den Kunden, die Credentials für den Online Zugriff Dritten zur Verfügung zu stellen. Mit der Nutzung von SOFORT Überweisung verstößt man also gegen die AGBs der Finanzinstitute.

Das Landgericht Frankfurt am Main hat es in einem Urteil klar formuliert, das die Nutzung des Dienstes unzumutbar ist, egal welche Sicherheitsgarantien von der Sofort GmbH versprochen werden:

> *Die Nutzung des Dienstes Sofortüberweisung ist unabhängig von seiner Bewertung durch Kreditinstitute für den Verbraucher unzumutbar, da er hierzu nicht nur mit einem Dritten in vertragliche Beziehungen treten muss, sondern diesem Dritten auch noch Kontozugangsdaten mitteilen muss und in den Abruf von Kontodaten einwilligen muss. Hierdurch erhält ein Dritter umfassenden Einblick in die Kunden-Kontoinformationen. Hierbei handelt es sich um besonders sensible Finanzdaten, die auch zur Erstellung von Persönlichkeitsprofilen genutzt werden könnten. Daneben muss der Kunde dem Zahlungsdienstleister seine personalisierten Sicherheitsmerkmale (zum Beispiel PIN und TAN) mitteilen. Dies birgt erhebliche Risiken für die Datensicherheit und eröffnet erhebliche Missbrauchsmöglichkeiten. Dabei kommt es im Ergebnis nicht auf die konkrete Sicherheit des Dienstes Sofortüberweisung an, sondern auf die grundsätzliche Erwägung, dass der Verbraucher nicht gezwungen werden kann, seine Daten diesem erhöhten Risiko auszusetzen.*

Der Bundesgerichtshof hat in dem Urteil Az.: KZR 39/16 diese Rechtsauffassung letztinstanzlich bestätigt.

Paysafecard entstand aus einem Forschungsprojekt der EU. In vielen Geschäften oder Tankstellen kann man Gutscheincodes kaufen. Die Webseite von Paysafecard bietet eine Umkreis-Suche nach Verkaufsstellen. Diese Codes kann man ähnlich anonym wie Bargeld im Web zur Bezahlung verwenden (wenn der Händler PSC akzeptiert).

Bei der Bezahlung wird man von der Webseite des Händlers zur Webseite von Paysafecard weiter geleitet. Dort gibt man den gekauften Code ein und der Händler erhält die Information, dass die Bezahlung erfolgt ist.

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

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

Durch Verschärfung der Sicherheitsvorkehrungen kommt es häufig zu gesperrten Gutscheinen, wenn die Gutscheine von verschiedenen IP-Adressen genutzt oder abgefragt werden. Nachfragen beim Support von Paysafecard, wie man die Sperrung der Gutscheincodes vermeiden kann, wurden bisher nicht beantwortet. Wenn ein Gutschein gesperrt wurde, muss man sich an den Support von Paysafecard wenden. Restbeträge kann man sich unter Angabe der eigenen Kontonummer erstatten lassen.

Aufgrund des Gesetzes gegen Geldwäsche ist Paysafecard gezwungen, die Anonymität des Zahlungsmittels einzuschränken. Deutsche Nutzer sollen (aber müssen nicht) auf der Website unter *"My PaySafaCard"* einen Account erstellen und können diesen Account mit Gutscheincodes aufladen. Wer mehr als 100,- Euro pro Monat nutzen

möchte, muss sich mit Ausweisdokumenten identifizieren. Probleme mit gesperrten Gutscheinen soll es dann nicht geben.

Eine Nutzung von mehreren Gutscheinen mit Restbeträgen für einen Bezahlvorgang ist seit Sept. 2012 NICHT mehr möglich! Restbeträge kann man sich unter Angabe der Kontonummer erstatten lassen. Damit wird die Anonymität des Zahungsmittels leider ausgehebelt. Passende Paysafecards gibt es nicht immer, es gibt nur Gutscheine für 10, 15, 20, 25, 30, 50 oder 100 Euro.

Seit Ende Oktober 2014 sperrt paysafecard Anonymisierungsdienste. Will man bei der Bezahlung anonym bleiben und nutzt einen Anonymisierungsdienst wie Tor, dann erhält man eine Fehlermeldung. Der Gutschein Code wird bei 1-2 Versuchen nicht gesperrt, man kann ihn ohne Anonymisierungsdienst weiter verwenden.

6.1 Anonyme Online-Zahlungen vor dem Aus?

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

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

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

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

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

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

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

> *So begrüßenswert es ist, dass der anonyme Erwerb von E-Geld damit nicht generell abgeschafft wird, so kritisch sehe ich die nach wie vor bestehende Tendenz, individuelles Handeln in immer stärkerem Maße zu registrieren...*
>
> *Die Diskussion über Identifikationspflichten - vor allem bei der Inanspruchnahme des Internets - ist damit aber sicherlich noch nicht beendet.*

[3] http://heise.de/-1269409

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

6.2 Bargeld

Man kann im Internet nicht mit Bargeld bezahlen, trotzdem soll es kurz erwähnt werden, weil das anonyme Bezahlen mit Bargeld schrittweise immer weiter eingeschränkt wird. Angesichts der ungebremsten Schuldenentwicklung und unzureichenden Wachstums wird die Politik immer radikalere Maßnahmen ergreifen. Ein Bargeldverbot passt durchaus ins Konzept.

In Italien, Spanien, Frankreich, Griechenland und Zypern wurden Bargeldzahlung über einen Höchstsatz von 1.000-3.000 Euro bereits verboten, in Frankreich wird ab August 2015 die Höchstgrenze für Bezahlung mit Bargeld auf 2.000 Euro abgesenkt (das Gesetz wurde nach dem Charlie-Hebbo-Attentat verabschiedet). In Dänemark wurde ein Gesetz aufgehoben, das Läden im Einzelhandel zwingt Bargeld akzeptieren müssen, außerdem wird die dänische Notenbank ab 2016 keine Geldscheine mehr drucken.

Der Wirtschaftsweise Bofinger und der US-Ökonom Rogoff haben im Mai 2015 nachdrücklich die Abschaffung des Bargelds gefordert. Sie appellierten an Bundeskanzlerin Merkel, dass Sie sich auf dem G7-Gipfel in Elmau für eine weltweite Abschaffung des Bargeld einsetzen soll. Dafür wurden folgende Gründe genannt: [5], die ich nur kurz kommentieren will:

Stärkung der Nationalbanken: Wollen wir wirklich irgendwelche Banken stärken? Wir sollten lieber über die Einführung von Vollgeld diskutieren (wie in Island oder in der Schweiz), um die Macht der Banken zu brechen und Banken auf ihren eigentliche Funktion zurück zu führen.

Austrocknung des Schwarzmarktes: Schwarzmarkt == BÖSE (Drogen, Kipo werden genannt - klar)

Der Schwarzmarkt ist aber auch ein Regulativ zwischen der Gesetzgebung und den Bürgern. Wenn eine Regierung die Wünsche der Bürger konsequent missachtet, dann haben Bürger die Möglichkeit, auf den Schwarzmarnkt auszuweichen (natürlich unter Androhung von Strafen). Je drakonischer und unbeliebter die Finanzgesetze werden, desto stärker wird der Schwarzmarkt wachsen.

Die Austrocknung des Schwarzmarktes wird also auch die Macht der Regierenden und Banken gegenüber der Bevölkerung stärken. Wollen wir diese Entwicklung?

Negativzinsen durchsetzen: *Die Zentralbanken könnten auf diese Weise leichter Negativzinsen durchsetzen. Papiergeld ist das entscheidende Hindernis, die Zentralbank-Zinsen weiter zu senken. Seine Beseitigung wäre eine sehr einfache und elegante Lösung für dieses Problem.* (US-Ökonom Rogoff)

Das würde bedeuten, dass sich die Sparer gegen diese Enteignung nicht mehr wehren könnten, indem sie das Geld einfach abheben. Einen sogenannter Bankenrun (wenn Kunden massenweise ihr Geld abheben) will keine Bank riskieren.

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

[5] http://www.manager-magazin.de/finanzen/artikel/bofinger-und-rogoff-fordern-abschaffung-des-bargelds-a-1034135.html

Kommentare zu den Vorschlägen von Bofinger/Rogoff

> *Um diese beiden Argumente ernsthaft als Vorteile durchgehen zu lassen, muss man ein Technokrat sein, der einen lückenlos organisierten Ameisenhaufen für die beste aller Gesellschaften hält. Wer Freiheit, Bürgerrechte und eine lebendige Demokratie bewahren will, den muss es schütteln, wenn jemand, der als Weiser gilt, solche Ansichten verbreitet.*[6]

Noch etwas deutlicher:

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

Forderungen deutscher Politiker

- Der NRW-Finanzminister Walter-Borjans (SPD) beteiligt sich an der Kampagne gegen Bargeld und forderte im Juli 2015 eine Obergrenze bei Barzahlung. Bezahlungen mit Bargeld sollten in Deutschland nur bis 2.000 - 3.000 Euro erlaubt sein. Ein höherer Betrag würde ihn skeptisch machen. (Warum eigentlich?)

- Der NRW Landeschef des Bundes Deutscher Kriminalbeamter (BDK), Sebastian Fiedler, unterstützt. Fiedler behauptet, wenn man 70.000 Euro für ein Auto oder 200.000 Euro für eine Immobilie bar bezahlt, dann handelt es sich um Geld aus Steuerhinterziehung oder Straftaten. (Kann man ein Auto anonym zulassen oder eine Immobilie anonym ins Grundbuch eintragen lassen und die Verwendung illegaler Einnahmen damit geheim halten? Wer findet den Denkfehler?)

- Im Januar 2016 wurde ein Plan der Bundesregierung bekannt, europaweit die Obergrenze für Barzahlungen auf max. 5.000 Euro festzulegen, um die Finanzierung von Terrorismus zu unterbinden. Da diese Forderung in Deutschland nur schwer durchsetzbar ist und auch von Finanz- und Datenschutzexperten abgelehnt wird, versucht die Bundesregierung wieder einmal den Weg über die EU.

- Außerdem fordert W. Schäuble zentrale Bankkontenregister in allen Mitgliedsstaaten der EU und die bessere Kontrolle von anonymen Prepaid-Zahlungsmittel und Kryptowährungen wie Bitcoin und Ripple zur *Terrorbekämpfung*.

Kommentare zu den Forderungen deutscher Politiker

- Wer etwas gegen die Finanzierung von Terrorismus tun will, der sollte die Beziehungen zu den Staaten wie Saudi Arabien, Katar oder USA überdenken, die als weltweit als die größten Finanzgeber von Terroristen bekannt sind. Man könnte auch Druck auf die Türkei ausüben, um die Verkaufswege von Erdöl aus den von der ISIS besetzten Gebieten zu unterbinden und damit eine wesentliche Geldquelle des ISIS treffen.

- Sicher kommt es vor, dass gelegentlich ein Köfferchen mit Bargeld den Besitzer wechselt. Der Waffenschieber Schreiber hat beispielsweise im Namen von Thyssen-Krupp der CDU eine Spende von 1,3 Mio. D-Mark in einem Köfferchen übergeben, dass die CDU nicht ordnungsgemäß versteuerte. Er hat W. Schäuble 100.000 D-Mark in Bar geschenkt, die ebenfalls nicht korrekt verbucht und versteuert wurden. Deshalb trat unser jetziger Finazminister vom CDU Parteivorsitz zurück und musste Merkel den Vortritt lassen. Derartige Praktiken wird man durch eine 5.000 Grenze für Barzahlungen aber nicht wirklich verhindern können.

[6] http://bitcoinblog.de/2015/05/18/bargeld-ist-macht
[7] http://www.heise.de/tp/artikel/45/45089/1.html

- Die Steuerfahndung hat in Deutschland aber ganz andere Probleme. Der Fall Zumwinkel ist schönes Beispiel. Der Steuerfahnder wurde von seinen Vorgesetzten ausdrücklich angewiesen, den Fall Zumwinkel nicht weiter zu verfolgen. Er tat es trotzdem und wurde dafür mit einem psychologischen Gutachten vom Dienst suspendiert. Die Staatsanwältin, die den Fall mit über 1 Mio Euro Steuerbetrug vor Gericht brachte, wurde strafversetzt. Die Anklage wurde verzögert, bis ein Teil der Steuerschuld verjährt war und die Summe des Betruges unter 1 Mio Euro lag. Mehr kann man in dem Buch Inside Steuerfahndung (ISBN: 978-3-86883-105-4) von Frank Wehrheim und Michael Gösele nachlesen. Die Probleme liegen jedenfalls nicht in der Verfügbarkeit von Bargeld.

6.3 Bitcoin

Bitcoin ist eine digitale Peer-2-Peer Währung ohne zentrale Verwaltung. Sie ist unabhängig von der Geldpolitik einer Zentralbank und entwickelt sich marktgetrieben durch die Aktivitäten der Teilnehmer, die Bitcoin als Zahlungsmittel akzeptieren oder verwenden.

Die Wurzeln der ökonomischen Theorie dieser virtuellen Währung liegen in der *Austrian school of economics*, die von den Ökonomen Eugen v. Böhm-Bawerk, Ludwig Mises und Friedrich A. Hayek entwickelt wurde. Die Ökonomen kritisieren das gegenwärtige System des Fiatgeldes der Zentralbanken. Sie sehen in den massiven, politisch motivierten Interventionen der Zentralbanken in den Geldumlauf eine wesentliche Ursache für den Krisenzyklus. Als Ausweg empfehlen sie eine Internationalisierung der Währungen und die Rückkehr zum Goldstandard.

Gegenwärtig ist Bitcoin der populärste Versuch zur Umsetzung einer Währung in Anlehnung an die Konzepte der *Austrian school of economics*. Die Software löst mit kryptografischen Methoden vor allem zwei Probleme:

1. Das Kopieren und mehrfache Verwendung der Bits und Bytes, die ein Coin repräsentieren, ist nicht möglich.
2. Die Gesamtmenge der verfügbaren Coins ist limitiert. Neue Bitcoins werden nach einem festen Schema generiert und die Gesamtzahl ist limitiert.

Darauf aufbauend könnte man Bitcoin als Bezahlmethode verwendet werden. Bitcoins lassen sich in reale Währungen hin- und zurücktauschen. Der Kurswert der Bitcoins beim Tausch gegen reale Währungen (z. B. Euro) ergibt sich dabei ausschließlich aus dem Markt. Die Bezahlungen können relativ schnell am PC abgewickelt werden. Es dauert in der Regel nur 30-60min, bis das Bitcoin Netzwerk eine Transaktion hinreichend bestätigt hat.

In der Praxis ist Bitcoin aber als Zahlungsmittel unbrauchbar geworden:

- In den letzten Jahren ist Bitcoin zu einem Spekulationsobjekt geworden. Durch gezielt verursachte Währungsschwankungen, die durch einzelne Spekulaten mit hohem finanziellen Einsatz verursacht werden, ist der Kurs sehr volantil. Wenn der Kurs in wenigen Wochen um 50% schwankt ist ein kalkulierter, kommerzieller Einsatz kaum möglich.
- Durch die teilweise intensiven Spekulationskäufe und -verkäufe bei Kursschwankungen steigen die Transaktionsgebühren. Im Dez. 2017 musste man für eine Transaktion zeitweise bis zu 100 US-Dollar als Gebühren zahlen um sicherzustellen, dass die Transaktion innerhalb einer vertretbaren Zeit in die Blockchain aufgenommen wird.[8]

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

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

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

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

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

- Der Wettkampf der Bitcoinminer beim Schürfen neuer Coins ist völlig außer Kontrolle geraten und ist ein sinnloser Einsatz von immer mehr Rechenleistung, um sich gegenseitig zu übertrumpfen. Es ist nur noch eine gewaltige Energieverschwendung.

  Die Webseite Bitcoin Energy Consumption Index[10] schätzte den Energieverbrauch im Nov. 2017 auf 30 Terrawattstunden pro Jahr (Energieverbrauch von Irland: 25 TWh, Marokko: 29 TWh oder Dänemark: 34 TWh jährlich). Ende Januar 2018 wurde der Energieverbrauch von Bitcoin auf 40 Terrawattstunden pro Jahr geschätzt, Tendenz weiter steigend. Wenn die Tendenz weiter anhält, könnte Bitcoin noch vor Ende des Jahres 2020 den Energieverbrauch der USA übertreffen ohne irgendeinen Nutzwert zu liefern außer Umverteilung von Geld durch Spekulation.

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

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

[9] https://www.heise.de/ct/ausgabe/2018-3-Bitcoin-3942380.html
[10] https://digiconomist.net/bitcoin-energy-consumption
[11] https://bitcoinblog.de/2017/11/27/bitcoin-verbraucht-mehr-strom-als-159-laender-wirklich

Kapitel 7

Allgemeine Hinweise zur E-Mail Nutzung

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

7.1 E-Mail Provider

Als erstes braucht man eine oder mehrere E-Mail Adressen. Es ist empfehlenswert, für unterschiedliche Anwendungen auch verschiedene E-Mail Adressen zu verwenden. Es erschwert die Profilbildung anhand der E-Mail Adresse und verringert die Spam-Belästigung. Wenn Amazon, Ebay oder andere kommerzielle Anbieter zu aufdringlich werden, wird die mit Spam überschwemmte E-Mail Adresse einfach gelöscht ohne die private Kommunikation zu stören.

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

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

Eine kleine Liste von empfehlenswerten E-Mail Providern:

- **Mailbox.org** [1] (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, PGP verschlüsselte Inbox, verschlüsselter Mailversand und -empfang nur über SSL/TLS aktivierbar, DANE, IP-Adressen der Nutzer und User-Agent werden aus dem Mail Header entfernt, anonyme Accounts möglich, Bezahlung per Brief oder Bitcoin, OTP-Login mit HW-Token und FreeOTP für Webinterface, Tor Hidden Service für POP3, IMAP, SMTP und XMPP)
- **Posteo.de** [2] (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, S/MIME oder PGP verschlüsselte Inbox, verschlüsselter Mailversand aktivierbar aber nicht für Empfang, DANE, IP-Adressen der Nutzer werden

[1] https://mailbox.org
[2] https://posteo.de

aus dem E-Mail Header entfernt aber User-Agent Kennung nicht, anonyme Accounts möglich, anonyme Bezahlung per Brief, 2FA mit OTP suboptimal umgesetzt, außerdem unfreundliche Reaktion auf Kritik [3])

- **Mailfence.com** [4] (belgischer Provider, kostenlose Accounts möglich, Premium ab 2,50 Euro pro Monat allerdings mit mehr Speicherplatz als die 1,- Euro Accounts der Mitbewerber, POP3, IMAP und SMTP nur für bezahlte Accounts, OpenPGP im Webinterface möglich mit eigener Implementierung, OTP-Login mit FreeOTP für Webinterface, anonyme Bezahlung via Bitcoin oder ohne Anonymität via Kreditkarte)
- **KolabNow** [5] (Groupware Hosting in der Schweiz mit Adressbuch, Kalender und E-Mail, Mailaccounts für 4.41 CHF pro Monat, Groupware für 10 CHF pro Monat, IP-Adressen der Nutzer und User-Agent werden aus dem E-Mail Header entfernt)
- **runbox.com** [6] (privacy-engagierter norwegischer E-Mail Provider, Server stehen ebenfalls in Norwegen, Accounts ab 1,66 Dollar pro Monat)
- **dismail.de** (DE) und **disroot.org** (NL) bieten neben Services wie XMPP auch kostenfreie E-Mail Accounts. Beide Provider bieten einen hochwertigen, privacyfreundlichen Service und werden durch Spenden finanziert. IP-Adressen der Nutzer werden aus dem E-Mail Header entfernt, disroot.org entfernt auch den User-Agent.

  (Nach den Erfahrungen der letzten Jahre muss man leider damit rechnen, das kostenfreie, spendenfinazierte E-Mail Dienste (wie SecureMail.biz, Xalia u.a.) nur für ein paar Jahre verfügbar sind und dann eingestellt werden könnten.)

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

Nicht empfohlene E-Mail Provider

Einige Gründe, warum verschiedene E-Mail Provider mit gutem Ruf nicht in die Liste der Empfehlungen aufgenommen wurden:

- Web.de und GMX.de sammeln bei der Registrierung zuviele Daten: Vor- und Nachname, Land, PLZ und Ort, Straße, Hausnummer und die Mobilfunknummer.

  Mit der Registrierung erklärt man sich damit einverstanden, dass die Daten für Marketing-Zwecke verwendet werden. Die Daten werden an den Mutterkonzern übermittelt und mit anderen verbundenen Unternehmen geteilt. Außerdem werden die Daten für postalische Werbung sowie für Markt- und Meinungsforschung genutzt und Non-Profit Organisationen für Werbung zur Verfügung gestellt. (Falls man sich schon öfters mal gefragt hat, woher Meinungsforschungsinstitute die Telefonnummern haben...)

  Der EmailPrivacyTest[7] zeit, dass Web.de und GMX.de bei der Nutzung des Web-GUI nicht gegen Tracking Elemente in E-Mails schützen und ermöglichen es damit vielen Diensten, die Nutzer beim Lesen der E-Mails zu beobachten. Web.de setzt selbst HTML-Wanzen in den eigenen Newslettern ein (3 Tracking Wanzen in jedem Newsletter) und verfolgt damit die Lesegewohnheiten der Nutzer.

- Hushmail speichert zuviel Daten. Neben den üblichen Daten beim Besuch der Webseite werden die E-Mails gescannt und folgende Daten unbegrenzt lange gespeichert:

  1. alle Sender- und Empfänger E-Mail Adressen (VDS-artig)
  2. alle Dateinamen der empfangenen und gesendeten Attachements
  3. Betreffzeilen aller E-Mails (nicht verschlüsselbar)

[3] https://www.privacy-handbuch.de/diskussion.htm#take-down-notiz-von-posteos-anwaelten
[4] https://mailfence.com
[5] https://kolabnow.com
[6] https://secure.runbox.com
[7] https://www.emailprivacytester.com

4. URLs aus dem Text unverschlüsselter E-Mails
5. ... and any other information that we deem necessary

Diese Daten werden bei der Kündigung eines Account NICHT gelöscht.

Bei der Bezahlung für einen Premium-Account werden die IP-Adresse des Kunden sowie Land, Stadt und PLZ an Dritte weitergeben. Außerdem bindet Hushmail.com Dienste von Drittseiten ein. Die ID des Hushmail Account wird beim Besuch der Webseite nach dem Login an diese Drittseiten übermittelt. Für die Privacy-Policy dieser Drittseiten übernimmt Hushmail.com keine Verantwortung.

- In der EU-Studie *Fighting cyber crime and protecting privacy in the cloud*[8] warnen die Autoren in Kapitel 5.4 (S. 48) vor Risiken bei der Speicherung von Daten in den USA. Aufgrund des *US PATRIOT Act* (insbesondere S. 215ff) und der *4. Ergänzung des FISA Amendments Act* ist es für US-Behörden ohne juristische Kontrolle möglich, die Kommunikation von Nicht-US-Bürgern zu beschnüffeln. Dabei ist es unerheblich, ob der Cloud- bzw. E-Mail Provider eine US-Firma ist oder nicht. Es reicht nach Ansicht der Amerikaner, wenn die Server in den USA stehen.

  Außerdem hat US-Präsident Trump als eine seiner ersten Handlungen die Behörden in den USA per Dekret aufgefordert, den Datenschutz für Ausländer vollständig aufzuheben. Es ist unklar, welche Auswirkungen das Dekret und die damit angedeutete Richtung im Datenschutz zukünftig für EU-Bürger haben wird.[9].

  Aus diesem Grund ist ein Server-Standort *USA* für deutsche Nutzer eher ungeeignet. Das betrifft u.a. die E-Mail Provider SecureNym, S-Mail, Fastmail.fm, Rise-up.net...

- Weitere Beispiele werden auf der Webseite des Handbuches genannt.[10]

7.2 ProtonMail und Tutanota

Die E-Mail Dienste ProtonMail (Schweiz) und Tutanota (Deutschland) stellen einfache Nutzung von Verschlüsselung sowie Kompatibilität mit den gängigen E-Mail Protokollen in den Vordergrund und bemühen sich um Schutz gegen staatlichen Zugriff.

Das Schreiben und Lesen von E-Mails erfolgt primär im Webinterface mit einem Webbrowser. Einen E-Mail Client wie Thunderbird kann man nur über Umwege verwenden. Das ermöglicht die Realisierung einer einfach nutzbaren E-Mail Verschlüsselung.

Vorteile gegenüber Web.de, GMX.de, GMail.com u.a.

ProtonMail und Tutanota bieten viele Vorteile für Normalanwender, die Ihre E-Mails bisher im Webinterface von GMail, Yahoo! oder Hotmail bearbeiten.

- Die Provider respektieren die Privatsphäre der Nutzer, schnüffeln nicht in den Mails, geben keine Daten weiter und beobachten euch nicht beim Lesen von Newslettern.
- Die Daten werden verschlüsselt auf den Servern gespeichert. Auch die Betreiber haben keinen Zugang zu den Daten. Das schützt gegen Beschlagnahme von Daten durch Behörden aber nicht gegen eine TKÜ nach §100 a/b StPO.
- Die Provider bieten einen einfachen Zugang zur E-Mail Verschlüsselung für nicht-IT affine Nutzer. Man muss sich nur wenig mit der Verschlüsselung beschäftigen, um sie in der Praxis einsetzen zu können. Zwischen den Nutzern des Dienstes werden die Nachrichten automatisch verschlüsselt.

[8] http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050
[9] https://netzpolitik.org/2017/datenschuetzer-raetseln-schafft-trump-datenschutz-abkommen-zwischen-usa-und-eu-ab/
[10] https://www.privacy-handbuch.de/handbuch_31.htm

- Auch auf dem Smartphone ist verschlüsselte Kommunikation via E-Mail nutzbar. Tutanota und Protonmail bieten passende Apps im Google Playstore und für iPhones.
- Protonmail bietet vollständigen OpenPGP-Support auch für die Kommunikation mit externen Partnern. Man kann seine öffentlichen Schlüssel exportieren und dem Partner schicken. Außerdem kann man die Schlüssel der externen Partner importieren.

  Externe Nutzer, die keinen Account bei Tutanota haben, können nicht direkt via PGP-verschlüsselten E-Mails kommunizieren. Der Nutzer von Tutanota muss eine Nachricht an den externen Kontakt schicken. Die Nachricht wird verschlüsselt auf dem Server gespeichert und der Empfänger bekommt nur einen Link, unter dem er die Nachricht lesen und beantworten kann.
- Die Verwendung von E-Mail Clients ist nur bei ProtonMail möglich. Dafür muss man die ProtonMail Bridge lokal auf dem eigenen Rechner installieren. Die Bridge ist ein lokales Mail Gateway mit SMTP- und IMAP-Schnittstelle (kein POP3). Die Schlüsselverwaltung erfolgt dabei weiterhin auf dem ProtonMail Server.
- Die SSL/TLS-Verschlüsselung für die Webseiten wird vom Qualsys SSL Server Test mit A+ bewertet und Features zur Verbesserung der Transportsicherheit für E-Mails werden zeitnah implementiert.
- Tutanota unterstützt U2F als zweiten Faktor zur Anmeldung im Webinterface.

Am besten kommen die Vorteile zur Geltung, wenn alle Kommunikationspartner einen Account bei ProtonMail bzw. Tutanota haben.

Nachteile der Verschlüsselung im Browser

Konzeptionell bedingt haben diese Mailprovider einige Schwächen. Die Verschlüsselung bietet *hinreichende Sicherheit* und ist für hohe Sicherheitsansprüche nicht geeignet. Das wird im Threat Model bei ProtonMail auch deutlich angesprochen:

> *If you are Edward Snowden, or the next Edward Snowden, and have a life and death situation that requires privacy, we would not recommend using ProtonMail.*

Webanwendungen bieten mehr Angriffsmöglichkeiten auf die Verschlüsselung als lokal installierte Tools. Thomas Roth demonstrierte in dem Video *Hacking protonmail - with a browser*, wie man die Verschlüsselung von ProtonMail mit einfachen XSS-Hacks angreifen konnte. Die Lücken sind inzwischen beseitigt, vergleichbare Probleme hätte es bei Thunderbird aber nie geben können.

Die alternative Nutzung starker Kryptografie mit OpenPGP Smartcards ist bei beiden Diensten nicht möglich, auch wenn man dazu in der Lage wäre.

Der Code für die Verschlüsselung wird durch die Webanwendung beim Aufruf der Webseite geladen oder aktualisert. Außerdem werden die Schlüssel der Empfänger bei Bedarf vom Server geladen. Dieses Konzept nennt man *Server-basierte Kryptografie*. (Es ist damit nicht *Server-basierte Verschlüsselung* gemeint!) Das Konzept ist nicht neu. Es wurde bereits von Hushmail und Countermail eingesetzt (mit Java statt Javascript) oder von Cryptocat (für Chats) und die Kritikpunkte an dem Konzept kann man hier übernehmen.

- Die Server-basierte Kryptografie von Hushmail wurde bereits 2007 von der US Drogenbehörde DEA kompromittiert[11]. Hushmail wurde gezwungen, die E-Mails von mehreren Accounts entschlüsselt bereitzustellen und musste der Aufforderungen nachkommen. Auch alle oben genannten Dienste könnten die Verschlüsselung unbemerkt kompromittieren, wenn sie es für staatliche Behörden tun müssten.
- Server-basierte Kryptografie ist für hohe Sicherheitsansprüche politischer Aktivisten nicht geeignet wie P. Ball in einem Essay bei Wired.com[12] ausführlich dargelegt.

[11] http://www.wired.com/2007/11/encrypted-e-mai
[12] http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/

Tutanota und ProtonMail bieten inzwischen Apps für Android und iPhone an, die den Code für die Verschlüsselung enthalten und aus den Appstores installiert werden können. Damit entfällt diese Schwäche für Smartphone Nutzer.

Auf dem Desktop PC könnte man die *ProtonMail Bridge* als Mail-Gateway installieren oder die Software von Tutatnota von Github auschecken und lokal installieren. Auch das schützt gegen diese Angriffe, ist allerdings komplizierter, als OpenPGP zu konfigurieren.

Key Recovery durch den Provider (aka Krypto-Key-Backdoor)

Die genannten Provider speichern alle Nachrichten und Kontakte verschlüsselt auf den Servern. Die Nutzer können auf die Daten zugreifen, wenn sie sich mit einem Passwort authentifizieren. Das Passwort schützt den Zugriff auf die Kryptoschlüssel.

Welche Möglichkeiten gibt es für ein Key Recovery, wenn man sein Passwort vergisst?

- ProtonMail bietet ein Key Recovery via externer Mailadresse, wenn man sein Passwort vergessen hat. Wenn man diese Möglichkeit nutzt, werden alle vorhandenen E-Mails und Daten gelöscht, da sie ohne das Passwort des Nutzers nicht mehr entschlüsselt werden können. Wer das Passwort vergisst, verliert zwar alle Daten aber nicht den Account.[13]

- Tutanota bietet für normale Nutzer keine Möglichkeit des Key Recovery. Bei Tutanota Premium Accounts werden die Daten mit dem Key des Nutzers und dem Key der Account Administratoren verschlüsselt. Das heißt, der Administrator eines Premium Account könnte sich Zugriff auf die Daten verschaffen, aber die Administratoren von Tutanota haben keine konzeptuelle Backdoor für den Zugriff auf die Daten.[14]

Somit gibt es bei beiden Services keine konzeptuelle Backdoor.

7.3 Mozilla Thunderbird

Alle E-Mail Provider bieten die Möglichkeit, die E-Mail Kommunikation im Webinterface mit einem Browser zu verwalten, aber trotzdem ist ein E-Mail Client empfehlenswert:

- Der Browser ist eine Sandbox zum Anzeigen von Webseiten. Aufgrund des Funktionsumfangs moderner Browser und der bösartigen Feindlichkeit des Internet muss man von viel mehr Angriffsmöglichkeiten ausgehen, als bei einem Programm, dass speziell für die Bearbeitung von E-Mails optimiert wurde.

- Sichere Ende-zu-Ende Verschlüsselung ist im Browser nicht möglich, auch wenn immer mehr E-Mail Provider Lösungen dafür anpreisen. Diese Lösungen haben gegenüber der lokalen Verschlüsselung im E-Mail Client Nachteile bei der Sicherheit.

- Einige E-Mail Provider wie WEB.de und GMX.de blockieren nicht alle Tracking Elemente in E-Mails im Webinterface (weil sie selbst Möglichkeiten zum Tracking ihrer Newsletter nutzen). Mit einem E-Mail Client wie Mozilla Thunderbird kann man dafür sorgen, dass man seine E-Mails unbeobachtet liest.

Informationen und Downloadmöglichkeiten für Mozilla Thunderbird stehen auf der deutschsprachigen Website des Projektes [15] für Windows, Linux und MacOS zur Verfügung. Linux Distributionen enthalten Thunderbird. Mit der Paketverwaltung kann Thunderbird und die deutsche Lokalisierung installiert werden.

[13] https://protonmail.com/support/knowledge-base/resetting-mailbox-password
[14] https://tutanota.uservoice.com/knowledgebase/articles/470716-was-passiert-wenn-ich-mein-passwort-vergesse-k%C3%B6n
[15] https://www.mozilla.org/de/thunderbird/

7.3.1 Account erstellen

Nach dem ersten Start von Thunderbird führt ein Assistent durch die Schritte zur Einrichtung eines E-Mail Kontos. Nach Eingabe der E-Mail-Adresse sowie des Passwortes erkennt der Assistent die nötigen Einstellungen für den Mailserver oft automatisch. Es können auch die Einstellungen eines bisher verwendeten Programms übernommen werden. Bei der Einrichtung des E-Mail Account sollten einige Punkte beachtet werden.

Die Grafik im Bild 7.1 zeigt den Weg einer E-Mail vom Sender zum Empfänger. In der Regel ist man nicht direkt mit dem Internet verbunden. Der Zugang erfolgt über ein Gateway des Providers oder der Firma.

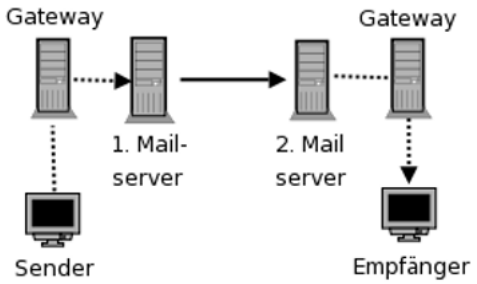


Abbildung 7.1: Der Weg einer E-Mail durch das Web

Der 1. Mailserver nimmt die E-Mail via SMTP entgegen und sendet sie an den 2. Mailserver. Hier liegt die E-Mail, bis der Empfänger sie via POP3 oder IMAP abruft und löscht. Die gestrichelten Verbindungen zu den Mailservern können mit SSL bzw. TLS kryptografisch gesichert werden. Das hat nichts mit einer Verschlüsselung des Inhalts der E-Mail zu tun. Es wird nur die Datenübertragung zum Mailserver verschlüsselt und es wird sichergestellt, dass man wirklich mit dem gewünschten Server verbunden ist. Aktuelle Versionen von Thunderbird aktivieren dieses Feature beim Einrichten eines Account standardmäßig.

Abbildung 7.2: POP3-Account anlegen

Begrifferklärung: SMTP, POP3, IMAP

Diese Abkürzungen sind für den Laien etwas verwirrend.

SMTP: ist das Protokoll zum Versenden von E-Mails.

POP3: ist das Protokoll zum Herunterladen von empfangenen E-Mails auf den lokalen Rechner. Die E-Mails werden auf dem Server sofort (oder etwas später) gelöscht.

Hinweis: bei POP3 wird nur der Ordner *Posteingang* vom Server geholt. Wenn man im Webinterface des Mailproviders weitere Ordner angelegt hat und mit Filtern E-Mails automatisch sortieren lässt, dann hat man mit POP3 keinen Zugriff auf diese Mails. Die automatische Sortierung muss in Thunderbird erfolgen.

IMAP: ist ein Kommunikationsprotokoll, um die empfangenen E-Mails auf dem Server zu verwalten und nur zum Lesen temporär herunter zu laden. Auch die versendeten E-Mails und die E-Mail Entwürfe werden bei der Nutzung von IMAP auf dem Mailserver des Providers gespeichert.

IMAP bietet damit die Möglichkeit, mit verschiedenen E-Mail Clients von unterschiedlichen Rechnern und Smartphones auf den Account zuzugreifen und stets Zugriff auf alle E-Mails zu haben. Die Möglichkeit des weltweiten Zugriffs auf seine Mails erkauft man sich aber mit Einschränkungen des Datenschutzes.

Die auf dem Server des Providers gespeicherten E-Mails unterliegen NICHT mehr dem Telekommunikationsgeheimnis nach Artikel 10 GG, wenn der Nutzer Gelegenheit hatte, sie zu löschen. Das BVerfG hat diese Rechtsauffassung 2009 in dem Urteil 2 BvR 902/06 bestätigt [16].

Mit der Reform der Telekommunikationsüberwachung im Dezember 2012 und die im Rahmen des Gesetzentwurfes zur Bekämpfung von Rechtsterrorismus und Hasskriminalität vorgelegten Anpassungen am Telemediengesetz von 2019 soll es jedem Dorfpolizisten ohne richterliche Prüfung erlauben, diese Daten abzurufen. Es wäre u.U. unschön, wenn man dort die gesamte Kommunikation der letzten 15 Jahre vorfindet.

Kompromiss: ist möglich, um mit mehreren Geräten (PC zuhause, Smartphone unterwegs...) auf einen E-Mail Account zuzugreifen:

1. Das Hauptgerät (PC) greift via POP3 auf den Mailserver zu, holt sich alle E-Mails und archiviert sie. Dieser E-Mail Client löscht alle Mails auf dem Server nach einer oder zwei Wochen oder wenn sie lokal gelöscht werden. So bleiben nur wenige E-Mails auf dem Server, man hat aber trotzdem privat ein vollständiges Archiv.
2. Alle anderen Geräte wie Smartphones u.ä. greifen vie IMAP auf den E-Mail Account zu und können so tagesaktuelle Geschäfte erledigen und E-Mails kurzfristig unterwegs lesen und beantworten.

Begrifferklärung: SSL/TLS oder STARTTLS

Wie einfach es ist, unverschlüsselte Verbindungen zu belauschen, die Passwörter zu extrahieren und das Mail-Konto zu kompromittieren, wurde von T. Pritlove auf der re:publica 2007 demonstriert [17].

Alle brauchbaren Mail-Server bieten Möglichkeit der verschlüsselten Kommunikation zwischen Thunderbird und Mailserver. Diese Option ist in Thunderbird bei der Einrichtung eines neuen Kontos auszuwählen. Der Assistent erledigt das in der Regel automatisch anhand der Vorgaben vom Mailserver. In der Regel kann man zwischen old-style SSL/TLS oder STARTTLS wählen, wobei die Voreinstellung seltsamerweise meist STARTTLS ist.

[16] https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-079.html
[17] http://tim.geekheim.de/2007/04/24/netzwerksicherheit-auf-der-republica/

SSL/TLS: Wenn man SSL/TLS verwendet, wird als erstes eine verschlüsselte Verbindung aufgebaut und danach beginnt die protokoll-spezifische Kommunikation. Es werden keine Daten unverschlüsselt übertragen.

Es werden keine Daten über eine unverschlüsselte Verbindung gesendet und der Server muss sich zuerst authentifizieren, bevor der Client irgendwelche Daten sendet.

STARTTLS: Wenn STARTTLS genutzt wird, beginnt die Kommunikation erst einmal unverschlüsselt. Der E-Mail Client wartet ab, ob der Mailserver in den Capabilities mit 250-STARTTLS eine Transportverschlüsselung anbietet. Erst dann erfolgt ein Aufbau der verschlüsselten Verbindung und der Client beginnt nochmal von vorn.

Eine SMTP-Verbindung wird mit STARTTLS wie folgt aufgebaut:

```
Client: unverschlüsselter Connect
Server: 220 smtp.server.tld Simple Mail Transfer Service Ready
Client: EHLO 192.168.23.44
Server: 250-smtp.server.tld
Server: 250-SIZE 100000000
Server: 250-AUTH LOGIN PLAIN
Server: 250-STARTTLS
Client: STARTTLS
Server: 220 go ahead
SSL/TLS Handshake zwischen Client und Server
Client (TLS-verschlüsselt): EHLO 192.168.23.44
```

Wie man sieht, können dabei unter Umständen auch private Daten unverschlüsselt gesendet werden. Bei SMTP wird im ersten EHLO Kommando die IP-Adresse oder der Hostname des Rechners aus dem internen Netz unverschlüsselt gesendet. Ein *Lauscher am Draht* kann damit u.U. den Mitarbeiter in einer Firma identifizieren.

Bewusst oder unbewusst können auch Internetzugangsprovider die sichere Übertragung deaktivieren und damit den Traffic mitlesen. Es wird einfach die Meldung des Mail-Servers 250-STARTTLS gefiltert und überschrieben (SSL strip attack). Scheinbar verfügen alle DSL-Provider über die Möglichkeit, dieses Feature bei Bedarf für einzelne Nutzer zu aktivieren[18]. Einige E-Mail Clients bieten die Option *"STARTTLS wenn möglich"* an. Diese Einstellung ist genau in dem Moment wirkungslos, wenn man es braucht, weil der Traffic beschnüffelt werden soll.

STARTTLS wurde als Erweiterung für bestehende Protokolle entwickelt, um TLS Verschlüsselung für unterschiedliche Domains mit unterschiedlichen Zertifikaten auf einem Server anbieten zu können. Es wurde nicht mit der Zielstellung entwickelt, die Sicherheit von SSL/TLS zu erhöhen. Man sollte sich nicht irritieren lassen und evtl. schlussfolgern, dass old-style SSL/TLS veraltet sein könnte.

Auch die IETF empfiehlt in RFC 8314[19] SSL/TLS gegenüber STARTTLS zu bevorzugen.

Hinweis für Nutzer der Telekom-Router

Die aktuellen Versionen der DSL-Router, die von der Telekom bereitgestellt werden, haben ein Feature, um Spambogs das Versenden von E-Mails zu erschweren. SMTP-Verbindungen auf den Ports 25, 465 und 587 sind nur für eine Whitelist von Mail-Servern erlaubt. Die empfohlenen E-Mail Provider sind nicht alle in der standardmäßig aktivierten Whitelist enthalten.

In der Router Konfiguration kann man im Menüpunkt *"Internet - Liste der sicheren E-Mail-Server"* das Feature abschalten oder den SMTP-Server des Providers hinzufügen.

[18] https://heise.de/-206233
[19] https://tools.ietf.org/html/rfc8314

Dieses Feature wird auch bei einem Update der Firmware älterer Telekom-Router aktiviert. Wenn man trotz korrekter Konfiguration in Thunderbird keine E-Mails mehr versenden kann, sollte man einen Blick in die Konfiguration des Routers werfen.

7.3.2 Sichere Optionen für TLS-Verschlüsselung

Die Transportverschlüsselung (TLS) sichert die Verbindung zwischen einem E-Mail Client und dem Mailserver des Providers gegen unerwünschte Lauscher. Seit der Einführung des Internet wird diese diese Verschlüsselung ständig weiterentwickelt und an neue, moderne Erkenntnisse der Kryptografie angepasst. Gleichzeit werden aus Kompatibilitätsgründen alte, unsichere Versionen mitgeschleppt statt abgeschaltet.

1. In der aktuellen zivilen Kryptoanalyse gilt nur TLS 1.3 als uneingeschränkt sicher.

   Um den Handshake zur Aushandlung einer TLS-Verschlüsselung einige Millisekunden zu beschleunigen, wurde ein Zero-Round-Trip Handshake in TLS 1.3 eingeführt. Viele Sicherheitsexperten sehen dieses Feature kritisch und als zukünftigen Angriffspunkt. In Thunderbird wurde bereits eine Option implementiert, um es abzuschalten.

2. Bei TLS 1.2 gibt es Einschränkungen bezüglich Sicherheit, da nicht alle in diesem Standard definierten Cipher Suiten als uneingeschränkt sicher eingestuft werden. Gemäß IETF RFC 7525 und BSI TR-03116-4 nur folgende Ciphersuiten als sicher:

   ```
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
   ```

   Die neueren Ciphersuiten mit CHACHA20-POLY1305 von D.J. Bernstein können ebenfalls als sicher eingestuft werden. Bei DHE-Ciphersuiten ist zu beachten, dass diese Cipher nur sicher sind, wenn hinreichend große Diffie-Hellman Parameter verwendet werden (was nicht immer gegeben ist). Es tritt immer wieder der Fehler auf, dass nur 1024 Bit DH-Parameter verwendet werden, was die NSA seit 2010 on-the-fly knacken kann. Deshalb ist die Deaktivierung der DHE-Cipher empfehlenswert.

3. TLS 1.0 und TLS 1.1 gelten als unsicher und sollten nicht mehr verwendet werden. Leider sind diese TLS Versionen nicht bei allen E-Mail Providern abgeschaltet, aber Thunderbird 78.x verwendet diese veralteten Protokolle nicht mehr.

TLS 1.3-only Konfiguration für Thunderbird

Am einfachsten aktiviert man eine sichere TLS-Verschlüsselung, wenn man nur TLS 1.3 verwendet. Dafür aktiviert man in den erweiterten Einstellungen folgende Option:

```
security.tls.version.min = 4
```

Außerdem kann man den Zero-Round-Trip Handshake von TLS 1.3 deaktivieren:

```
security.tls.enable_0rtt_data = false
```

Diese Einstellung funktioniert mit E-Mail Providern wie mailbox.org oder Posteo.de, die Wert auf Sicherheit legen. Bei vielen anderen E-Mail Providern gibt es damit Probleme.

Der Server *download.mozilla.com* hat eine grottenschlechte TLS Konfiguration und unterstützt kein TLS 1.3. Wenn Thunderbird darauf angwiesen ist, Updates von diesem Server zu beziehen (z. B. die MacOS Version oder Portable Thunderbird), dann wird es beim Update Prozess Probleme geben. Man könnte die jeweils aktuelle Version im Browser herunter laden und installieren oder man verwendet die TLS 1.2-secured Konfiguration.

Außerdem kann es Probleme beim Abrufen von einigen RSS Feeds geben, wenn der Webserver, der den Feed bereit stellt, kein TLS 1.3 unterstützt.

TLS 1.2-secured Konfiguration für Thunderbird

Standardmäßig erlaubt Thunderbird 78.x die Nutzung von TLS 1.2 und TLS 1.3. Wenn man noch TLS 1.2 nutzen muss, weil der E-Mail Provider TLS 1.3 nicht flächendeckend auf allen Servern einsetzt, dann sollte man die schwachen Cipher Suiten des TLS 1.2 Standard deaktivieren. Folgende Einstellungen sind in diesem Fall empfehlenswert:

```
security.tls.version.min =  3 (default ab Thunderbird 78.x)

security.ssl3.dhe_rsa_aes_128_sha     = false
security.ssl3.dhe_rsa_aes_256_sha     = false
security.ssl3.ecdhe_ecdsa_aes_128_sha = false
security.ssl3.ecdhe_ecdsa_aes_256_sha = false
security.ssl3.ecdhe_rsa_aes_128_sha   = false
security.ssl3.ecdhe_rsa_aes_256_sha   = false
security.ssl3.rsa_aes_128_sha         = false
security.ssl3.rsa_aes_256_sha         = false
security.ssl3.rsa_des_ede3_sha        = false
```

Weiterer Einstellungen für die TLS Verschlüsselung

- Insecure Renegotiation verbieten wird seit 2009 als Sicherheitsproblem eingestuft. Ein Angreifer kann die Login Credentials (Username und Passwort) abschnorcheln ohne die Verschlüsselung knacken zu müssen. Tools zum Ausnutzen der Insecure Renegotiation für einen Angriff gibt es auch als OpenSource (z.B. dsniff). Deshalb:

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

- Strenges Certifikate Pinning erzwingen (z.B. für Add-on Updates):

  ```
  security.cert_pinning.enforcement_level = 2
  ```

- Für RSS Feeds und die Webseiten Ansicht in Feeds kann man den HTTPS-only Mode aktivieren und das Laden von unverschlüseltem Content verbietet::

  ```
  security.mixed_content.upgrade_display_content = true
  dom.security.https_only_mode                   = true
  network.ftp.enabled                            = true
  ```

Verbindungsprobleme mit sicheren TLS-Einstellungen

Wenn man die im Bild 7.3 gezeigte, schwer verständliche Fehlermeldung beim Abrufen oder Senden von E-Mails erhält, gibt es Probleme beim Aufbau einer sicheren Verbindung und man wechselt am besten den Mail-Provider.

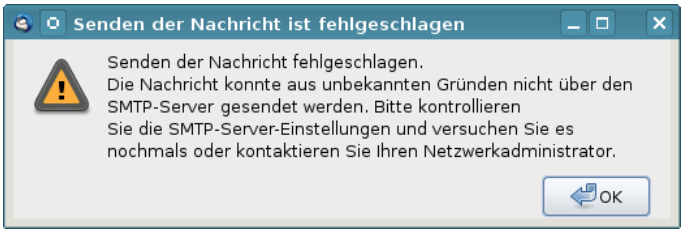


Abbildung 7.3: Fehlermeldung bei unsicherer Verbindung

7.3.3 Sichere Konfiguration des E-Mail Client

Einige Hinweise für die sichere Nutzung des Mediums E-Mail mit Mozilla Thunderbird:

- Mit der Verwendung von HTML in E-Mails steht dem Absender ein ganzes Bestiarium von Möglichkeiten zur Beobachtung des Nutzers zur Verfügung: HTML-Wanzen, Cookies usw. Der *E-Mail Privacy Test*[20] demonstriert viele Trackingmöglichkeiten.

  Die Firma ReadNotify beispielsweise nutzt diese Möglichkeiten, um E-Mails und Dokumente für die Beobachtung des Empfängers zu präparieren (User-Tracking).

  Standardmäßig blockiert Thunderbird alle Trackingelemente und auch Spam Mails in der HTML Ansicht. Trotzdem empfehle ich, E-Mails als Plain Text zu lesen. Die Option findet man im Menüpunkt *Ansicht -> Nachrichtentext* (siehe Bild 7.4). Das erleichtert auch die Erkennung von Phishing E-Mails.

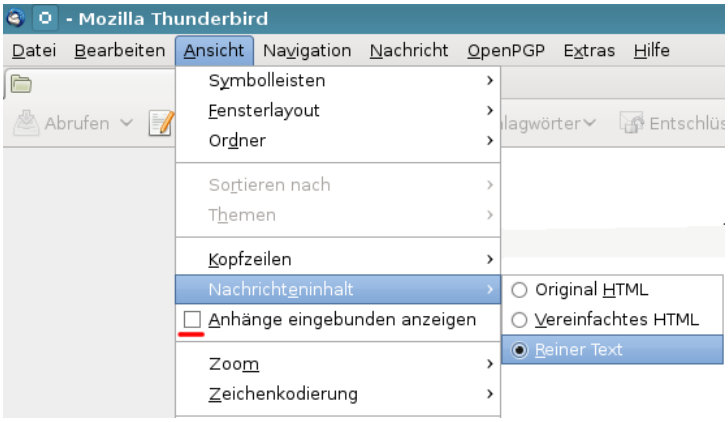


Abbildung 7.4: E-Mails als reinen Text darstellen

- Die Option *Anhänge eingebunden anzeigen* im Menü *Ansicht* sollte man ebenfalls deaktivieren, um gefährliche Anhänge nicht schon beim Lesen einer E-Mail automatisch zu öffnen. Der alte Trick mit einem Virus in der E-Mail wird noch immer genutzt, insbesondere wenn man ein Opfer gezielt angreifen will, um den Rechner mit einem Trojaner zu infizieren.

  In der Konfiguration kann man dafür folgenden Parameter setzen:

```
mail.inline_attachments = false
```

- Es ist nicht immer möglich, E-Mails als Plain Text zu lesen. Viele Newsletter sind nur als HTML-Mail lesbar, eBay verwendet ausschließlich HTML-Mails für Benachrichtigungen usw. In der Regel enthalten diese HTML Mails mehrere Trackingelemente.

  Um diese E-Mails trotzdem lesen zu können (wenn auch nicht in voller Schönheit), kann man die Darstellung *Vereinfachtes HTML* nutzen. Außerdem können folgende Features in den *Erweiterten Einstellungen* deaktiviert werden, die jedoch nur für die Darstellung von HTML E-Mails in der Ansicht *Orginal HTML* relevant sind oder für andere Komponenten, die den HTML-Viewer nutzen:

```
javascript.enabled                    =  false
network.cookie.cookieBehavior         =  2
beacon.enabled                        =  false
layout.css.visited_links_enabled      =  false
media.hardware-video-decoding.enabled =  false
media.navigator.enabled               =  false
```

[20] https://emailprivacytester.com

```
media.video_stats.enabled             =  false
gfx.downloadable_fonts.enabled        =  false
network.IDN_show_punycode             =  true
network.http.sendRefererHeader        =  0
security.family_safety.mode           =  0
```

Da JavaScript generell deaktiviert wird, muss man im Gegensatz zu Firefox die Geolocation, DOMStorage, IndexedDB, AudioContext-API, Timing-APIs, Gamepad-API ... usw. nicht einzeln abschalten.

Thunderbird 60+ verwendet die Gecko Engine von Firefox Quantum zum Rendern von HTML Content (z.B. in RSS Feeds) und kennt Surf-Container. Wie bei Firefox kann man FirstParty.Isolate als Trackingschutz aktivieren:

```
privacy.firstparty.isolate = true
```

- Im Kopf einer E-Mail kann man zusätzliche Informationen anzeigen lassen:

  1. Ein E-Mail Absender besteht aus einem Namen und der E-Mail Adresse. Standardmäßig zeigt Thunderbird nur den Namen an. Informativer und sicherer ist es, die vollständige E-Mail Adresse mit anzuzeigen. Das aktiviert man in den *Erweiterten Einstellungen* mit folgender Option:

     ```
     mail.showCondensedAddresses = false
     ```

  2. Eine E-Mail kann den Absender im FROM Header und/oder im Header SENDER enthalten. Wenn beide angegeben sind, zeigt Thunderbird nur den FROM Header an. Ein Angreifer könnte das nutzen, um eine E-Mail mit gefakten S/MIME Zertifikaten als signiert erscheinen zu lassen. Um diesen Angriff zu erkennen, kann man sich beide Absenderinformationen anzeigen lassen (wenn vorhanden) und sollte stutzig werden, wenn sie unterschiedlich sind:

     ```
     mailnews.headers.showSender = true
     ```

  3. Die Anzeige des E-Mail Programms, das der Absender verwendet, ist immer mal wieder interessant. Diese Anzeige kann man mit folgender Option in den *Erweiterten Einstellungen* aktivieren:

     ```
     mailnews.headers.showUserAgent = true
     ```

- Die Nutzung der Safebrowsing Funktion deaktiviert man in Thunderbird 60 genauso wie in Firefox ESR. Gegen Phishing Angriffe schützen keine technische Maßnahmen vollständig sondern in erster Linie das eigene Verhalten. Und gegen Malware schützen regelmäßige Updates des Systems besser als Virenscanner und URL-Listen.

```
browser.safebrowsing.phishing.enabled                              = false
browser.safebrowsing.malware.enabled                               = false
browser.safebrowsing.blockedURIs.enabled                           = false
browser.safebrowsing.downloads.enabled                             = false
browser.safebrowsing.downloads.remote.enabled                      = false
browser.safebrowsing.downloads.remote.block_dangerous              = false
browser.safebrowsing.downloads.remote.block_dangerous_host         = false
browser.safebrowsing.downloads.remote.block_potentially_unwanted   = false
browser.safebrowsing.downloads.remote.block_uncommon               = false
```

- Alle Bilder in HTML-Mails, die von einem externen Server geladen werden, können direkt mit der E-Mail Adresse des Empfängers verknüpft sein. Anhand der Logdaten kann der Absender erkennen, wann und wo die E-Mail gelesen wurde. Einige Newsletter verwenden auch HTML-Wanzen. Im Newsletter von Paysafecard findet man beispielsweise ganz unten eine kleine 1x1-Pixel Wanze, die offenbar mit einer individuellen, nutzerspezifischen URL von einem Trackingservice geladen wird:

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

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

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

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

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

Auch andere Medienformate können von einem externen Server geladen und als Wanzen genutzt werden. Einen deartigen Einsatz von Audio- oder Videodateien habe ich bisher nicht gefunden, aber technisch wäre es möglich. Man kann das Laden von Videos und Audiodateien mit folgenden Parametern unterbinden:

```
media.webm.enabled  =  false
media.wave.enabled  =  false
media.ogg.enabled   =  false
```

Die Links in HTML-Mails führen oft nicht direkt zum Ziel sondern werden ebenfalls über einen Trackingservice geleitet, der jeden Aufruf des Link individuell für jede Empfängeradresse protokollieren kann. Als Bespiel soll ein Link aus dem Paysafecard Newsletter dienen, der zu einem Gewinnspiel bei Paysafecard führen soll:

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

Diesem Tracking kann man nur entgehen, wenn man diese Links in HTML-Mails nicht aufzuruft! Der Trackingservice hat die Möglichkeit, Logdaten von verschiedenen E-Mails zu verknüpfen und evtl. auch das Surfverhalten einzubeziehen. Wichtige Informationen findet man auch auf der Webseite des Absenders.

- Im SMTP-Dialog mit dem Mailserver beim Versenden einer E-Mail sendet Thunderbird im EHLO Kommando standardmäßig die lokale IP-Adresse:

  ```
  SSL/TLS Handshake zwischen Client und Server
  Client: EHLO 192.168.23.44
  ```

  Viele Mailserver vermerken diese lokale IP-Adresse aus dem EHLO Kommando im ersten Received Header der E-Mail zusammen mit der externen IP-Adresse, die der Mailserver sieht, und teilen sie damit auch Dritten mit:

  ```
  Received: from cefige3264.dynamic.kabel-deutschland.de
  ([188.192.92.109] helo=[192.168.23.44]) by smtp.server.tld
  ```

  Um zu vermeiden, dass diese Information veröffentlicht wird, kann in den *Erweiterten Einstellungen* eine neue String Variable anlegen und einen Fake definieren:

  ```
  mail.smtpserver.default.hello_argument = [127.0.0.1]
  ```

  Privacy-freundliche E-Mail Provider entfernen den ersten Received Header vollständig, da er nicht nur die lokale IP-Adresse aus dem internen Netzwerk enthält, sondern auch die externe IP-Adresse, die Hinweise auf den Aufenthaltsort des Absenders liefert und von Datensammlern mit dem Surfprofil verknüpft werden kann.

- In dem Adressbuch *Gesammelte Adressen* werden die E-Mail Adressen der Empfänger aus den versendeten E-Mails gesammelt. Diese E-Mail Adressen stehen dann für die Autocomplete Funktion zur Verfügung, wenn man beim Schreiben einer E-Mail die Empfänger Adressen eingibt.

  Wenn man die E-Mail Adressen der Empfänger nicht automatisiert speichern möchte, dann kann man das kann man das Feature in den Einstellungen in der Sektion *Verfassen* abschalten.

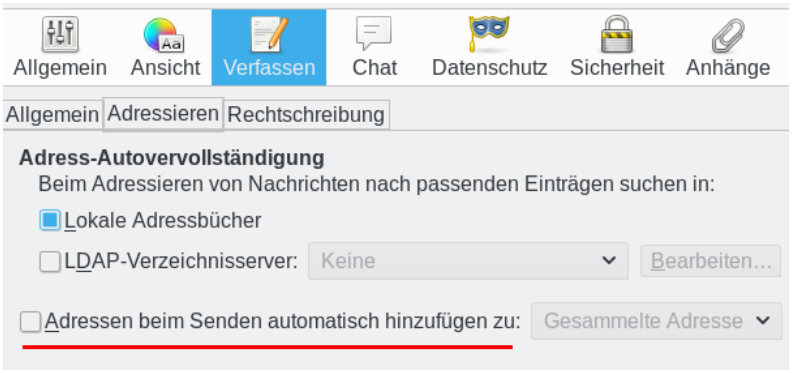


Abbildung 7.5: Sammeln von E-Mail Adressen abschalten

  In den *Erweiterten Einstellungen* kann man folgenden Wert setzen:

```
mail.collect_email_address_outgoing = false
```

  Dann muss man sich aber selbst um die Pflege des Adressbuches kümmern.

- Die *extension blocklist* kann Mozilla nutzen, um einzelne Add-ons in Thunderbird zu deaktivieren. Es ist praktisch ein kill switch für Add-ons. Beim Aktualisieren der Blockliste werden außerdem detaillierte Informationen an Mozilla übertragen.

  Ich mag es nicht, wenn jemand irgendetwas remote auf meinem Rechner deaktiviert oder deaktivieren könnte. In den *Erweiterten Einstellungen* kann man es abschalten:

```
extensions.blocklist.enabled = false
```

- Thunderbird kontaktiert täglich den AMO-Server von Mozilla und sendet eine genaue Liste der installierten Add-ons. Als Antwort sendet der Server Statusupdates für die installierten Add-ons. Diese Funktion ist unabhägig vom Update Check für Add-ons, es ist nur eine zusätzliche Datensammlung von Mozilla. In den erweiterten einstellungen kann amn dieses Feature abschalten:

```
extensions.getAddons.cache.enabled = false
```

- Alle Übertragungen von Telemetriedaten, Healthreport usw. an Mozilla unterbindet man ab Thunderbird 45 mit folgendem globalen Kill-Switch:

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

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

7.3.4 Datenverluste vermeiden

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

- Das Antiviren-Programm ist so einzustellen, dass es den Profilordner von Thunderbird NICHT(!) scannt. Die automatische Beseitigung von Viren kann zu Datenverlusten führen.
- Der Ordner *Posteingang* sollte so leer wie möglich gehalten werden. Gelesene E-Mails sollten auf themenspezifische Unterordner verteilt werden.
- Die Ordner sollten regelmäßig komprimiert werden, um gelöschte E-Mails engültig aus der MBOX zu entfernen und den Speicherplatz freizugeben.
  - In den Einstellungen in der Sektion *Erweitert* kann man eine automatische Komprimierung konfigurieren, sobald x MB Speicherplatz dadurch frei werden. Bei jedem Start prüft Thunderbird, ob die Ordner komprimiert werden können.
  - Alternativ kann man mit der rechten Maustaste auf einen Ordner zu klicken und der Punkt *Komprimieren* wählen. Während des Komprimierens sollten keine anderen Aktionen in Thunderbird ausgeführt werden.
- Regelmäßig sollten Backups des gesamten Profils von Thunderbird angelegt werden. Unter Linux ist *$HOME/.thunderbird* zu sichern, Unter WINDOWS sichert man *C:/Dokumente und Einstellungen/<NAME>/Anwendungsdaten/Thunderbird*.

7.3.5 Wörterbücher installieren

Für die automatische Rechtschreibkontrolle beim Schreiben einer E-Mail muss man die nötigen Wörterbücher für die bevorzugten Sprachen installieren. Man kann neben dem immer vorhandenen Englisch die Wörterbücher für weitere Sprachen hinzufügen.

- Unter Linux nutzen Thunderbird und Firefox die Hunspell Wörterbücher für die Rechtschreibkontrolle. Mit dem bevorzugten Paketmanager kann man die Wörterbücher für verschiedene Sprachen installieren. Für Debian/Ubuntu könnte man *apt* verwenden. Neben *hunspell-de-de* für deutsches Deutsch gibt es auch Pakete für Österreicher (*hunspell-de-at*) oder Schweizer (*hunspell-de-ch*):

  ```
  > sudo apt install hunspell-de-de
  ```

  Fedora und QubesOS fassen alle deutschen Sprachvariationen in einem Paket zusammen:

  ```
  > sudo dnf install hunspell-de
  ```

- Für andere Betriebssysteme kann man fehlende Wörterbücher von der Webseite für Language Tools[21] herunter laden. Nach dem Download der Wörterbücher ist Thunderbird als zu starten. Der Menüpunkt *Extras -> Add-ons* öffnet den Dialog für die Verwaltung. Wenn man oben rechts auf das kleine Werkzeugsymbol klickt (Bild 7.6, kann man die Dateien mit den Wörterbüchern als Add-on installieren.

Danach kann man in den Einstellungen von Thunderbird die Rechtschreibprüfung aktivieren und die bevorzugte Sprache auswählen. Die Auswahl der Sprache kann man beim Schreiben einer Mail jederzeit ändern.

[21] https://addons.mozilla.org/de/thunderbird/language-tools/

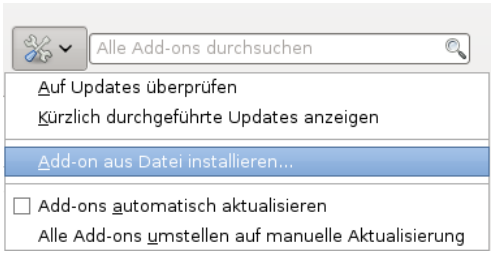


Abbildung 7.6: Wörterbücher in der Add-on Verwaltung installieren

7.3.6 User-Agent Kennung modifizieren

Ich habe gelesen, dass es böse Buben geben soll, die via Internet ihre Software auf fremden Rechnern installieren möchten. Das Versenden von böstigen E-Mail Attachements via E-Mail ist Bestandteil jeder Werkzeugkiste für Angreifer.

- Der Bundestrojaner, den das BKA zu Spionage einsetzt, wird unter anderem via E-Mail auf den Rechner der Zielperson transportiert, wie die Tagesschau berichtete.[22]
- 2010 wurde Google bzw. von US-Regierungsvertretern genutzte GMail Accounts von chinesischen Hackern angegriffen. Auch dabei wurden E-Mails mit bösartigen Attachements verwendet, wie Google in einem Statement berichtete.[23]
- Auch als unbescholtener Bürger kann man zufällig Target für einen gezielten Angriff werden. Beispielsweise hackt die NSA gezielt die Rechner von Sysadmins, um über diesen Weg Zugang zu technischer Infrastruktur zu bekommen.[24]

Voraussetzung für diese gezielten Angriffe ist die Kenntnis der vom Opfer zum Lesen von E-Mails verwendete Software. Dann kann ein Angreifer gezielt für diesen E-Mail Client oder Browser einen Exploit auswählen, der unauffällig funktioniert. 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: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0)
            Gecko/20100101 Thunderbird/38.2.0
X-Enigmail-Version: 1.8.1
...

------- BEGIN PGP MESSAGE -------
Version: GnuPG v1.4.12 (GNU/Linux)
...
```

Aha, er nutzt also Thunderbird in der Version 38.2.0 unter Windows 7 (64 Bit), hat das Enigmail Add-on Version 1.8.1 installiert und verwendet die GnuPG-Version 1.4.12.

Einige privacy-freundliche Mailprovider wie mailbox.org und Mail.de reinigen die Mails für Ihre Kunden und löschen die User-Agent Kennung aus dem E-Mail Header. Wenn man einen Account bei einem anderen Mailprovider hat, dann muss man sich selbst kümmern.

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.

[22] https://www.tagesschau.de/inland/meldung490134.html
[23] https://googleblog.blogspot.de/2010/01/new-approach-to-china.html
[24] https://theintercept.com/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/

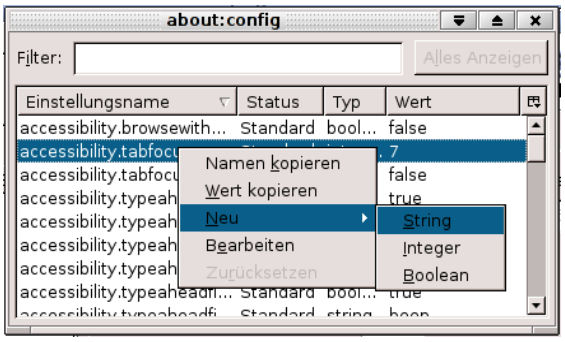


Abbildung 7.7: Neue Config-Variable anlegen

Hier fügt man die neue String-Variable **general.useragent.override** als neuen Wert ein, indem man mit der rechten Maustaste auf einen freien Bereich klickt und im Kontext-Menü den Punkt *Neu - String* wählt.Als Wert für diese Variable wird eine leere Zeichenkette eingesetzt. Damit sendet Thunderbird keine Kennung mehr.

Nachteile im tagtäglichen Betrieb sind nicht erkennbar. Man kann aber in der Add-on Verwaltung von Thunderbird keine Add-ons mehr direkt vom Server installieren. Der AMO Server von Mozilla überprüft die Version von Thunderbird anhand der User-Agent Kennung und gibt Add-ons nur dann zur Installation frei, wenn die Version passt.

Als Alternative könnte man das gewünschte Add-on mit einem Webbrowser von der Webseite des Entwicklers herunter laden (in Firefox: Rechtsklick auf den üblichen Install-Button und dann *Speichern unter...* wählen) und danach die lokale XPI-Datei in der Add-on Verwaltung von Thunderbird installieren.

Seit Thunderbird 78.0 wird die Lightning Version der Kalender- und Aufgabenverwaltung nicht mehr automatisch an den User-Agent angehängt. Den Parameter calendar.useragent.extra, der bei älteren Thunderbird Versionen ebenfalls gesetzt werden musste, gibt es nicht mehr.

7.3.7 Spam-Filter aktivieren

Das Mozilla Team bezeichnet nicht erwünschte E-Mails (Spam) als Junk. Den integrierten lernfähigen Filter kann man in Account Einstellungen unter *Junk-Filter* aktivieren, wenn der E-Mail Provider keinen guten Spam-Filter einsetzt.

(Ich nutze lieber einen guten E-Mail Provider und brauche daher diesen Spam-Filter seit längerer Zeit nicht mehr.)

7.3.8 Spam vermeiden

Die E-Mail Adresse ist ein wichtiges Identitätsmerkmal. Datensammler wie Rapleaf verwenden sie als ein Hauptmerkmal für die Identifikation, um darauf aufbauend Profile zu erstellen. Stichproben im Internet Traffic weisen einen hohen Anteil von Suchanfragen nach Informationen zu den Inhabern von E-Mail Adressen aus.

Man muss die eigene E-Mail Adresse nicht bei jeder Gelegenheit im Web angeben, wenn irgendwo eine E-Mail Adresse verlangt wird (bei der Registrierung in Foren, einfachen Blog Postings usw). Um die eigene E-Mail Adresse nicht zu kompromittieren und trotzdem diese Angebote zu nutzen, kann man E-Mail Aliases, Wegwerf-Adressen oder temporäre E-Mail Adressen nutzen.

E-Mail Aliases nutzen

Jeder brauchbare E-Mail Provider bietet die Möglichkeit, Aliases für einen E-Mail Account anzulegen. Man kann im Webinterface in den Konfigurationseinstellungen einen oder mehrere Aliases für den Account erstellen, diese Adressen für die Kommunikation mit bestimmten Zweck (z.B für Hotel Reservierung oder Flug Buchung) für eine begrenzte Zeit nutzen und dann löschen. Konkrete Anleitungen findet man in den FAQ oder der Online Hilfe des Mail Providers.

Die Verwendung von E-Mail Aliases hat gegenüber temporären E-Mail Adressen und Wegwerf-Adressen einige Vorteile:

- E-Mail Aliases können auch als Absender zum Senden von E-Mails verwendet werden. Das ist z.B. ein Vorteil, wenn man nach der Registrierung eines Accounts den Support des Anbiters kontaktieren muss. Mit temporären Adressen kann man in der Regel nur Nachrichten empfangen.
- E-Mail Aliases werden nicht gesperrt. In vielen Diskussionsforen (z.B. bei Zeit.de) sind E-Mail Adressen von Temp.-Mail Anbietern für die Registrierung von Accounts gesperrt.
- Gute E-Mail Provider haben ein sichere TLS Transportverschlüsselung für ihre Mailserver. Bei den Anbietern temporärer E-Mail Adressen werden die Mails in der Regel ohne oder mit schlechter TLS Verschlüsselung durch das Internet gesendet und können von Dritten (z.B. vom BND in Rahmen der Fernmeldeaufklärung) problemlos mitgelesen werden.

E-Mail Adress-Erweiterungen

Bei vielen E-Mail Providern Mailbox.org, Runbox, Gmail, Yahoo! Mail Plus, Apple's iCloud, Outlook.com oder FastMail kann man E-Mail Adress-Erweiterungen nutzen. Wenn man die E-Mail Adresse *name@provider.tld* als Account oder E-Mail Alias registriert hat, kann man beliebig viele Adresse nach dem Muster *name+extension@provider.tld* zum Empfang verwenden. Es ist ein Standardfeature des MTA Postfix und kann auch auf eigenen Mailservern einfach aktiviert werden.

Einige E-Mail Provider bewerben dieses Feature als Spamschutz. Nach unserer Meinung ist der Wert als Spamschutz aber sehr gering. Jeder, der sich ein bisschen mehr mit E-Mail Features beschäftigt hat (und davon kann man bei Datensammlern ausgehen), kennt das Feature und kann die Erweiterungen leicht ausfiltern. Der Vorteil von E-Mail Adress-Erweiterungen liegt eher in der einfach konfigurierbaren, automatischen Sortierung eingehender Nachrichten und nicht beim Spamschutz.

AnonBox des CCC

Bei der AnonBox.net des CCC [25] kann ein E-Mail Account für den Empfang von einer Nachricht erstellt werden. Der Account ist bis 24:00 Uhr des folgenden Tages gültig (24-48h) und nicht verlängerbar. Die empfangene Nachricht kann man nur im Webinterface lesen und sie wird nach dem Abrufen gelöscht. Sie kann nur 1x gelesen werden! Zusammen mit der E-Mail wird auch der Account gelöscht. Man kann praktisch nur eine Mail empfangen.

Beim Erzeugen einer E-Mail Adresse erhält man einen Link, unter dem man die ankommende Mail lesen kann. Wenn noch nichts angekommen ist, dann bleibt die Seite leer. Der Link ist als Lesezeichen zu speichern, wenn man später nochmal nachschauen möchte.

[25] https://anonbox.net

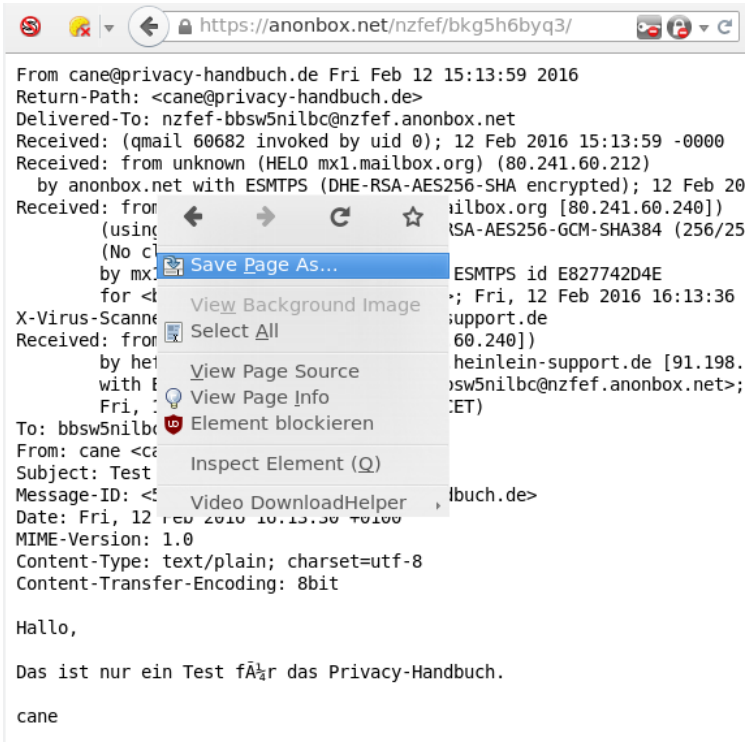


Abbildung 7.8: E-Mail im Web-GUI der AnonBox.net als Datei speichern

Eine empfangene E-Mail wird im Quelltext dargestellt. Wer aus dem Konvolut nicht schlau wird, kann mit de rechten Maustaste in die Textwüste klicken und als Datei speichern, wie in Bild 7.8 gezeigt. Die Datei ist mit der Endung **.eml** zu speichern und kann dann in einem E-Mail Client wie z.B. Mozilla Thunderbird geöffnet werden (Bild 7.9).

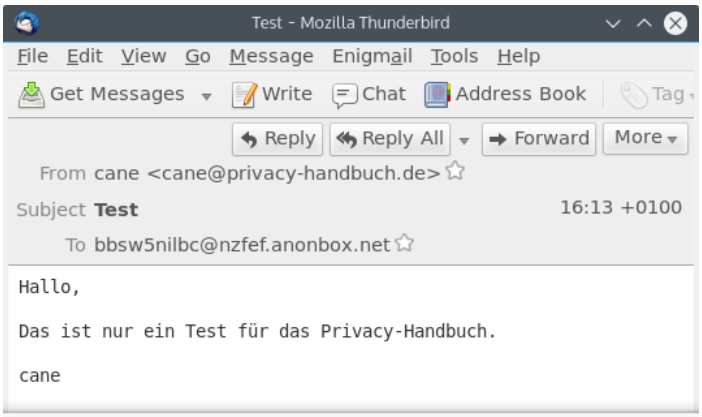


Abbildung 7.9: E-Mail aus AnonBox.net in Thunderbird geöffnet

Sicherheit unterliegt bei der AnonBox.net starken Schwankungen:

- Die SSL-Konfiguration des Webservers von AnonBox.net war früher mal auf dem aktuellen Stand der Technik mit Forward Secrecy und starken DH-Parametern und ist jetzt (Sept. 2018) katastrophal.
- Die TLS-Verschlüsselung des Mailservers hatte ich vor einiger Zeit schon einmal kriti-

siert, wurde danach auf den aktuellen Stand gebracht und ist jetzt (Sept. 2018) wieder kaputt.

Wegwerf-Adressen

Einige Anbieter von Wegwerf-E-Mail-Adressen bieten einen sehr einfach nutzbaren Service, der keinerlei Anmeldung erfordert und auch kein Erstellen der Adresse vor der Nutzung. E-Mail Adressen der Form *pittiplatsch@trash-mail.com* oder *pittiplatsch@weg-werf-email.de* kann man überall und ohne Vorbereitung unbekümmert angeben. Das Postfach ist unbegrenzt gültig.

In einem Webformular auf der Seite des Betreibers findet man später alle eingegangenen Spam- und sonstigen Nachrichten für das gewählte Pseudonym. Für das Webinterface des Postfachs gibt es in der Regel keinen Zugriffsschutz. Jeder, der das Pseudonym kennt, kann die Nachrichten lesen und löschen. Wenn eine Wegwerf-Adresse für die Registrierung eines Account genutzt wurde, könnte ein Angreifer problemlos die Passwort Recovery Funktion nutzen!

Nachrichten werden nach 6-12h automatisch gelöscht. Man muss also regelmäßig den Posteingang prüfen, wenn man eine Wegwerf-Adresse nutzt.

Liste einiger Anbieter (unvollständig):

- https://discard.email (SSL-Verschlüsselung für Webserver aber nicht für Mailserver, Passwortschutz, E-Mail schreiben möglich, Session-Cookies und JavaScript erforderlich)
- https://www.trash-mail.com (HTTPS, Cookies und JavaScript freigeben, Schreiben von E-Mails möglich)
- https://www.guerrillamail.com (HTTPS, Cookies und JavaScript freigeben, Schreiben von E-Mails möglich)
- http://crapmail.dk (Antwort schreiben möglich, Cookies freigeben)
- http://vsimcard.com/trashmails.php (bietet auch Wegwerf-SMS Nummern)
- http://www.7mail7.com (Cookies und JavaScript freigeben, RSS-Feed für Inbox)
- http://www.mailcatch.com (keine Cookies oder JavaScript nötig, E-Mails können gelöscht werden)
- http://www.mailinator.com/ (JavaScript nötig freigeben, E-Mails können gelöscht werden)

In der Regel speichern diese Anbieter die Informationen über eingehende E-Mails sowie Aufrufe des Webinterface und stellen die Informationen bei Bedarf den Behörden zur Verfügung. Es handelt sich dabei nicht Anonymisierungsdienste.

Temporäre Adressen

Im Gegensatz zu Wegwerf-E-Mail-Adressen muss man eine temporäre E-Mail Adresse zuerst auf der Webseiten des Anbieter erstellen, die dann für 10min bis zu mehreren Stunden gültig ist. Erst danach kann diese Mail-Adresse verwendet werden. Bei Bedarf kann die Verfügbarkeit der E-Mail Adresse im Browser mehrfach verlängert werden.

Um eine temporäre E-Mail Adresse für die Anmeldung in einem Forum o.ä. zu nutzen, öffnet man als erstes eine der oben angegebenen Webseiten in einem neuen Browser-Tab. Session-Cookies sind für diese Website freizugeben, mit JavaScript sind die Webseiten oft besser bedienbar. Nachdem man eine neue temporäre Mail-Adresse erstellt hat, überträgt

man sie mit Copy & Paste in das Anmeldeformular uns schickt das Formular ab. Dann wechselt man wieder zu dem Browser-Tab der temporären Mailadresse und wartet auf die eingehende Bestätigungsmail. In der Regel einhält diese Mail einen Link zur Verifikation. Auf den Link klicken - fertig. Wenn der Browser-Tab mit der temporäre E-Mail Adresse geschlossen wurde, hat man keine Möglichkeit mehr, ankommende Mails für diese Adresse zu lesen.

Die folgenden Anbieter erlauben nur zufällig erstellter E-Mail Adressen. Die Verwendung dieser Adressen für die Registrierung von Accounts ist sicherer, da ein Angreifer die Passwort Recovery Funktion des Webdienstes nicht nutzen kann, um sich ein neues Passwort zuschicken zu lassen und den Account zu übernehmen:

- https://temp-mail.ru (2h, HTTPS, Cookies und JavaScript freigeben, russisches GUI)
- www.10minutemail.com (10min gültig, verlängerbar)
- http://www.10minutemail.com/ (10min gültig, verlängerbar, Cookies und JavaScript freigeben)
- http://tmpeml.info (60min gültig, Cookies freigeben)
- http://disposable.pingfu.net (60min gültig, JavaScript freigeben)
- http://getairmail.com (24h gültig, Cookies und JavaScript freigeben)

Bei den folgenden Anbieter kann man neben zufällig generierten E-Mail Adressen auch selbst definierte E-Mail Adresse nutzen. Man kann damit einen bestimmten E-Mail Account mehrfach verwenden. Das ist für einige Anwendungsfälle ein Vorteil, manchmal eher ein Nachteil:

- http://www.tempmailer.de (60min gültig, Session-Cookies freigeben)
- http://www.squizzy.de (60min gültig, Session-Cookies freigeben)
- http://dontmail.net (24h, Cookies und JavaScript freigeben)
- http://www.migmail.net (24h, Cookies und JavaScript freigeben)

7.3.9 RSS-Feeds

RSS-Feeds bieten die Möglichkeiten, sich schnell über Neuigkeiten in häufig gelesenen Blogs zu informieren ohne die Webseiten einzeln abklappern zu müssen. Thunderbird enthält einen RSS-Reader, den man dafür nutzen kann.

Um mehrere interessante RSS-Feeds zu sammeln, erstellt man in der *Konten Verwaltung* ein neues Konto und wählt den Typ *Anderes Konto hinzufügen....*

Im zweiten Schritt wählt man den Typ *Blogs und RSS-Feeds* und danach eine beliebige Kontenbezeichnung.

In den Einstellungen für das RSS-Feed Konto kann man festlegen, in welchem Intervall die Feeds abgerufen werden sollen und ob die RSS-Feeds beim Start von Thunderbird aktualisiert werden sollen. Danach kann man die *Abonnements verwalten* und die Adressen der RSS-Feeds hinzufügen. Man kopiert die URL des RSS-Feeds von der Webseite des

Blogs in das Feld für die Feed URL und klickt auf den Button *Hinzufügen* wie im Bild 7.10 dargestellt.

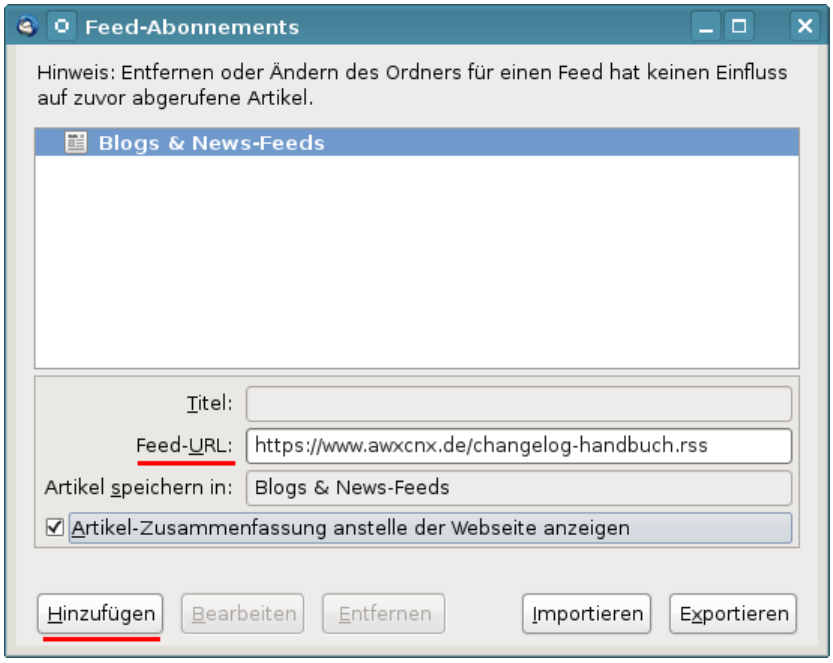


Abbildung 7.10: RSS-Feed hinzufügen

Die Neuigkeiten aus den Blogs kann man zukünftig wie E-Mails lesen. Dabei kann man eine simple Textanzeige wählen oder die Ansicht als Webseite. Wer die Ansicht als Webseite bevorzugt, sollte JavaScript, Cookies und andere Tracking Elemente deaktivieren. Zum Kommentieren muss man allerdings die Webseite des Blogs im Browser aufrufen.

Aus Sicherheitsgründen ist es empfehlenswert, den RSS-Feed als Plain Text zu lesen und nicht als Webseite zu laden. Das sieht nicht so hübsch aus, verringert aber man die Angriffsmöglichkeiten durch bösartigen Schadcode oder Media Elemente, wenn die Webbrowser-Komponente von Thunderbird kritische Lücken enthält (z.B. CVE-2016-9899 und CVE-2016-9893).

```
rss.display.prefer_plaintext        =  true
rss.display.disallow_mime_handlers  =  3
rss.display.html_as                 =  1
rss.show.content-base               =  1
```

Bei jedem Start kontaktiert Thunderbird standardmäßig die Webserver, auf denen die RSS-Feeds liegen, und sucht nach den Favicons der Webseite für die Darstellung in der Liste der Feeds. Dieses Verhalten kann man Thunderbird abgewöhnen, indem man folgenden Parameter in den Einstellungen setzt:

```
browser.chrome.site_icons  =  false
```

7.3.10 Filelink

Seit Version 13.0 bietet Thunderbird die Möglichkeit, große Dateianhänge bei einem Filehoster hochzuladen und dem Empfänger nur den Link zum Download per E-Mail zu senden. Aktuelle Thunderbird Versionen nutzen dafür den Filehoster *Box.com*[26] standardmäßig. Weitere Dienste wie OwnCloud, DropBox, FileRun oder WebDAV Speicher können

[26] https://www.box.com

via Add-ons genutzt werden. Eine Liste findet man im Support Bereich von Mozilla[27].

Ich kann dieses Feature nicht empfehlen.

1. Filelink ist nicht in die E-Mail Verschlüsselung integriert. Auch wenn man eine verschlüsselte E-Mail schreibt, werden die Uploads unverschlüsselt auf dem Server abgelegt. Man muss sich selbst um die Verschlüsselung der Dateien kümmern und könnte sie dann gleich zu einem 1-Click-Hoster hochladen.
2. Die bei einem Cloud-Service gespeicherten Dateianhänge unterliegen nicht dem besonderen Schutz des Post- und Fernmeldegeheimnisses.
3. Der standardmäßig unterstütze Dienst *Box.com* erfordert die Registrierung eines Accounts. Aufgrund der euphemistisch als Datenschutzerklärung[28] bezeichneten Auflistung der Datensammeltechniken kann man von diesem Dienst nur abraten.

   Es werden neben Cookies auch moderne Tracking Techniken wie HTML5 EverCookies eingesetzt. Do-Not-Track Header werden ausdrücklich ignoriert. Dabei wird nicht nur der Absender von Dateianhängen getrackt, sondern auch der Empfänger, der damit möglicherweise nicht einverstanden ist.

In Thunderbird 78.x kann man FileLink mit folgender Option komplett abschalten:

```
mail.cloud_files.enabled = false
```

7.4 Private Note

E-Mails werden auf dem Weg durch das Netz an vielen Stellen mitgelesen und ausgewertet. Ein Postgeheimnis existiert praktisch nicht. Kommerzielle Datensammler wie Google und Yahoo scannen alle Mails, die sie in die Finger bekommen. Geheimdienste wie NSA, SSSI, FRA oder BND haben Monitoringprogramme für den E-Mail Verkehr.

Gelegentlich möchte man aber nicht, das eine vertrauliche Nachricht von Dritten gelesen wird. Verschlüsselung wäre eine naheliegende Lösung. Das ist aber nur möglich, wenn Absender und Empfänger über die nötige Kompetenz verfügen.

Als Alternative kann man *PrivNote*[29] der Firma *insophia* nutzen. Man schreibt die Nachricht auf der Webseite des Anbieters und klickt auf den Button *Create Note*. JavaScript muss dafür frMan schreibt die Nachricht auf der Webseite des Anbieters. JavaScript muss dafür freigegeben werden. In den Optionen kann man festlegen, wann die Nachricht gelöscht werden soll, man kann zusätzlich ein Passwort für das Lesen setzen und eine E-Mail bekommen, wenn die Nachricht gelöscht wird.

Das zusätzliche Passwort ist nur sinnvoll, wenn es über einen unabhängigen Kanal zum Empfänger übertragen wird. Man könnte z.B. bei einem Treffen ein Passwort vereinbaren und dieses Passwort dann nutzen, bis man ein neues Passwort austauscht. Das Passwort könnte man mit jeder Nachricht ändern, so dass die aktuelle Nachricht immer das Passwort für die nächste Nachricht enthält. Man kann es beliebig kompliziert gestalten, solange beide Seiten den Überblick behalten. Es ist aber nicht sinnvoll, ein Passwort zusammen mit dem Link zum Lesen der Nachricht in der gleichen E-Mail zu schicken, das ist Bullshit.

Wenn man auf den Button *Create note* klickt, wird ein Link generiert, unter dem man die Nachricht EINMALIG abrufen kann. Die Nachricht wird im Browser verschlüsselt auf dem Server gespeichert und nur der Link enthält den Key, um die Daten zu entschlüsseln.

[27] https://support.mozilla.org/de/kb/filelink-fuer-grosse-dateianhaenge
[28] https://www.box.com/de-de/legal/privacypolicy
[29] https://privnote.com

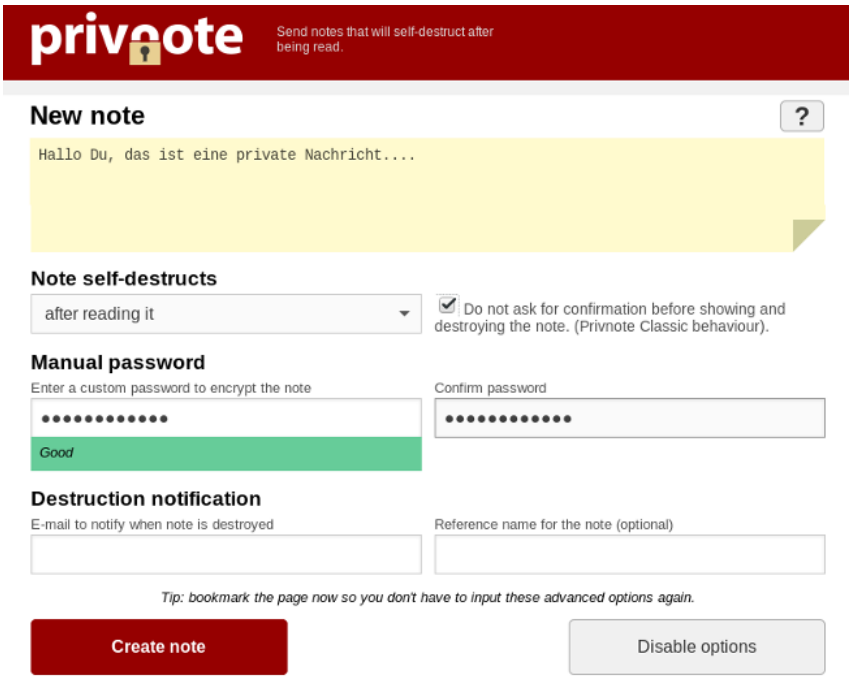


Abbildung 7.11: Eine Private Note schreiben

Den Link kann man per E-Mail dem Empfänger der Nachricht senden. Er kann die Nachricht im Browser abrufen. Nach dem Abruf der Nachricht wird sie auf dem Server gelöscht, sie ist also nur EINMALIG lesbar. Darauf sollte man den Empfänger hinweisen. Sollte die Nachricht nicht abgerufen werden, dann wird sie spätestens nach 30 Tagen gelöscht.

Man kann den Link NICHT über irgendwelche Kanäle in Social Networks (z.B. Facebook) versenden. Wenn man auf den Link klickt, läuft im Hintergrund ein Crawl der Seite bevor man weitergeleitet wird. Facebook holt sich die Nachricht und der Empfänger kommt zu spät.

PrivNote ist nicht kryptografisch abhörsicher wie die E-Mail Verschlüsselung mit OpenPGP. Wenn ein Angreifer unbedingt den Inhalt der Nachricht lesen will, kann er die Nachricht vor dem Empfänger abrufen und über den Inhalt Kenntnis erlangen. Der eigentliche Empfänger kann nur den Angriff erkennen, da die Nachricht auf dem Server gelöscht wurde. Damit sind die Angebote für private Nachrichten geeignet, aber nicht geeignet für geheime oder streng vertrauliche Informationen.

Kapitel 8

E-Mails verschlüsseln

Weltweit wird der unverschlüsselte E-Mail Verkehr systematisch gescannt. Führend ist die NSA mit *Echelon*, das auch zur Industriespionage sowie zum Abhören von NGOs verwendet wird, und Abhörschnittstellen bei allen großen amerikanischen ISPs. Frankreich betreibt ein ähnliches System unter dem Namen *French ECHELON*. Das russische Pendant zur NSA ist der SSSI (früher FAPSI). Der schwedische Geheimdienst FRA und das Schweizer Onyx Projekt nutzen Supercomputer zur Verarbeitung der abgeschnorchelten Datenmengen. Für Saudi Arabien, Syrien, Iran, Tunesien und Ägypten wurden entsprechende Aktivitäten nachgewiesen und die *Great Firewall* von China verfügt ebenfalls über die nötigen Features.

In Deutschland wird der E-Mail Verkehr im Rahmen der *Strategischen Fernmeldeaufklärung* von den Geheimdiensten gescannt. Eine von der G-10 Kommision genehmigte Stichwortliste mit 16.400 Begriffen (Stand 2010) wird für die automatisierte Vorauswahl verwendet, um nach Waffenhandel, Prolieferation und Terroristen zu suchen. Im Jahr 2010 meldeten die Scanner 37 Mio. E-Mails als verdächtig. 2011 hat der BND es geschafft, die automatisierten Scanner mit einem Spamfilter zu kombinieren, so dass "nur noch" 2,1 Mio. E-Mails als verdächtig gemeldet und kopiert wurden.

OpenPGP und S/MIME

OpenPGP und S/MIME (*Secure MIME Protokoll*) sind fast 20 Jahre alte Standards für E-Mail Kryptografie. Sie können folgende Aufgaben erfüllen:

1. Mit dem **Verschlüsseln** von E-Mails wird die Vertraulichkeit des Inhalts der E-Mail gewährleistet. Eine Nachricht kann nur vom Empfänger mit dem paasenden Schlüssel geöffnet und gelesen werden.

2. Mit dem **Signieren** von E-Mails wird die Authentizität der Nachricht gewährleistet. Anhand der Signatur kann der Empfänger prüfen, ob eine Mail wirklich von dem angegebenen Absender kommt und unterwegs nicht modifiziert wurde.

3. Die Metadaten im Header der E-Mail (Absender, Empfänger, verwendete Software, evtl. die IP-Adresse des Absenders usw.) werden durch diese beiden Verfahren nicht(!) verschleiert und können für die Kommunikationsanalyse verwendet werden.

OpenPGP und S/MIME nutzen **Asymmetrische Kryptografie**. Das heißt, es wird ein Schlüsselpaar mit unterschiedliche Schlüssel zum Verschlüsseln und zum Entschlüsseln verwendet. Das Grundprinzip ist einfach erklärt:

- Jeder Anwender generiert ein Schlüsselpaar bestehend aus einem geheimen und einem öffentlichen Schlüssel. Während der geheime Schlüssel sorgfältig geschützt nur dem Anwender zur Verfügung stehen sollte, ist der öffentliche Schlüssel an alle Kommunikationpartner zu verteilen.

- Wenn Beatrice eine verschlüsselte Nachricht an Anton senden will, nutzt sie den öffentlichen Schlüssel von Anton, um die Nachricht zu chiffrieren. Nur Anton kann den Inhalt der E-Mail mit seinem geheimen Schlüssel dechiffrieren und lesen.
- Wenn der Anton eine signierte E-Mail an die Beatrice senden will, erstellt er eine Signatur (digitale Unterschrift) mit seinem geheimen Schlüssel. Beatrice kann mit dem öffentlichen Schlüssel von Anton die Unterschrift und damit die Echtheit der Nachricht verifizieren, da nur Anton Zugriff auf seinen geheimen Schlüssel haben sollte.

Verschlüsselung und Signatur können kombiniert werden. Dabei wird der Inhalt der Nachricht zuerst signiert und dann alles zusammen (Nachricht + Signatur) verschlüsselt.

PGP, GnuPG und S/MIME haben es in den letzten 20 Jahren nicht geschafft, eine massentaugliche Usability zu entwickeln. Wenn man erst einmal 20 Seiten Anleitung lesen muss, um die E-Mail Verschlüsselung zu verstehen, Software selbst konfigurieren muss, sich selbst die notwendigen Schlüssel erstellen muss oder beglaubigen lassen muss, sich um die Verteilung der Schlüssel selbst kümmern muss und es danach noch jedem Partner einzeln erklären muss, dann ist diese Krypto einfach nicht massentauglich.

Pretty Easy Privacy (PEP) und Autocrypt

PEP und Autocrypt hatten das Ziel, die Usability von OpenPGP zu verbessern und damit eine breitere Anwendung von E-Mail Verschlüsselung zu ermöglichen. Es wurden bei Sicherheit und Flexibilität teilweise erhebliche Einschränkungen in Kauf genommen, ohne dabei das Ziel einer nennenswert größeren Verbreitung von OpenPGP zu erreichen.

Bei **Pretty Easy Privacy** (PEP) sind die Einschränkungen moderat:

- Bei der Einrichtung eines Accounts erstellt PEP im Hintergrund automatischen ein Schlüsselpaar (private und public Key). Der private Key wird nicht mit einem Passwort gesichert und der Anwender wird nicht mit Aufforderung zum Backup des Schlüsselpaares belästigt. (Backups sind nur etwas für Feiglinge?).
- Bei jeder versendeten E-Mail hängt PEP den public Key als Attachement an. Der Anwender soll sich keine Gedanken um die Schlüsselverteilung machen müssen. Keyserver, Web Discovery oder DNS werden nicht zur Verteilung verwendet.
- Auf der Gegenseite akzeptiert PEP den ersten Key von einem Kommunikationspartner und verwendet ihn zukünftig automatisch. (*trust in first use*). Alle weiteren Keys werden verworfen, um Sicherheitsprobleme wie bei Autocrypt zu vermeiden.
- Die Verwendung mehrerer Geräte oder der Austausch eines Schlüssels vor Ablauf der Gültigkeit sind nicht vorgesehen. Verlorene Schlüssel (Verlust/Tausch des Gerätes und kein Backup) oder kompromittierte Schlüssel haben keinen Platz in dem Konzept.
- Verifizierung von Schlüsseln wird als Luxusproblem für Experten eingestuft.

(Das klingt vereinfachend, kann im konkreten Fall aber unschön kompliziert werden, wenn man das Gerät zum Lesen der E-Mails wechselt, ein PEP Nutzer seinen Schlüssel verliert o.ä. Die Simplifizierung mit PEP vereinfacht E-Mail Verschlüsselung, wenn man geringe Anforderungen an Sicherheit hat und keine Sonderwünsche.)

Mit **Autocrypt**[1] wurden die Sicherheit von OpenPGP drastisch geschwächt, um den Austausch der Schlüssel zu vereinfachen. OpenPGP mit Autocrypt bietet keine sichere Verschlüsselung sondern nur noch **some protection most of the time**. Außerdem wurden die E-Mail Provider per Definition als vertrauenswürdig deklariert und damit das wesentlich Ziele einer Ende-zu-Ende Verschlüsselung über Board geworfen. Der Schutz gegen

[1] https://autocrypt.org

den E-Mail Provider war und ist das wesentliche Ziel jeder Ende-zu-Ende Verschlüsselung.

Eine Ende-zu-Ende Verschlüsselung, die nicht mehr gegen die Provider schützt, ist einfach überflüssig. Bedauerlicherweise ist Autocrypt in vielen Tools zur E-Mail Verschlüsselung standardmäßig aktiviert, was die Nutzung von OpenPGP für sicherheitskritische Anwendungen (beispielsweise Whistleblower) kaputt gemacht hat.

In der Entwickler Community sind die Ansichten gespalten. Bei dem Mailvelope Browser Add-on wurde Autocrypt implementiert und standardmäßig aktiviert. Die Thunderbird Entwickler haben diesen Schlüsseltausch nicht implementiert.

Mit **countermitm**[2] gibt es eine Erweiterung für den Autocrypt Schlüsseltausch, die eine Verifizierung von Schlüsseln einführt und ein *Network of Trust*, um bei Autocrypt mögliche Man-in-the-Middle Angriffe für verifizierte Schlüsseln zu verhindern. *contermitm* gehört nicht zum Autocrypt Standard und wird unabhängig davon entwickelt.

8.1 E-Mails verschlüsseln mit Thunderbird

Thunderbird stellt alle Features für die Verschlüsselung mit OpenPGP und S/MIME bereit.

Sichere Konfiguration: Der Efail Angriff hat demonstriert, dass eine sichere Konfiguration des E-Mail Client eine notwendige Voraussetzung für sichere Verschlüsselung ist (E-Mails als Plain Text anzeigen, keine eingebundene Anzeige von Anhängen usw.)

Masterpasswort aktivieren: Thunderbird sichert die privaten Keys mit einer zufälligen Passphrase, die in der Passwortdatenbank gespeichert wird. Es ist daher wichtig, die Passwortdatenbank mit einem Masterpasswort zu sichern.

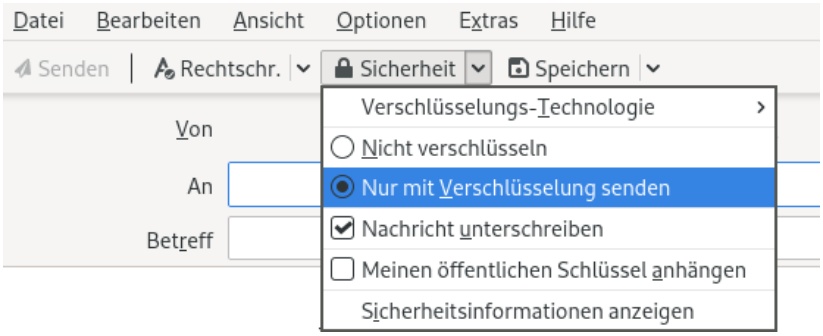
Schlüssel erstellen: Um die Verschlüsselung von E-Mails zu aktivieren, muss man in den Kontoeinstellungen in der Sektion *Ende-zu-Ende Verschlüsselung* einen PGP-Schlüsselpaar generieren oder importieren oder ein S/MIME Zertifikat importieren.

Schlüssel verteilen: Um verschlüsselt mit Kommunikationspartnern via E-Mail kommunizieren zu können, muss man die öffentlichen Schlüssel (public keys) austauschen. Bei modernen Krypto-Messengern wird das im Hintergrund automatisch erledigt. Bei der E-Mail Verschlüsselung muss man sich noch selbst darum kümmern.

1. Damit die Partner verschlüsselt schreiben oder Signaturen prüfen können, muss man ihnen den eigenen Schlüssel zusenden oder zum Download anbieten.
2. Damit man selbst verschlüsselt schreiben kann, muss man die Schlüssel der Kommunikationspartner in Thunderbird importieren.
3. Die frisch importierten Schlüssel der Partner müssen akzeptiert bzw. verifiziert werden, bevor man sie zum Verschlüsseln von E-Mails verwenden kann.

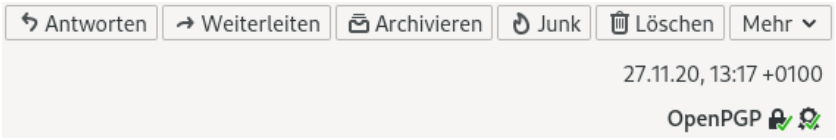
E-Mails schreiben: Wenn man die Hürden beim Austausch der Schlüssel überwunden hat, kann man beim Schreiben die Verschlüsselung mit zwei Klicks aktivieren:

[2] https://countermitm.readthedocs.io/en/latest/index.html



Leider bietet Thunderbird (noch) keine Möglichkeit, Präferenzen zur Verschlüsselung für bestimmte Empfänger zu definieren. Man muss vor dem Versenden einer E-Mail kurz innehalten und über die Verschlüsselungsoptionen nachdenken.

E-Mails lesen: Verschlüsselte E-Mails werden von Thunderbird automatisch entschlüsselt und angezeigt, wenn man sie öffnet. Man sieht oben rechts im Kopf der E-Mail ein oder zwei kleine Symbole bei verschlüsselten und/oder signierten E-Mails:



Verschlüsselte E-Mails werden nicht in den globalen Index aufgenommen und können nicht bei einer Suche nach Begriffen aus dem Inhalt der Mail gefunden werden.

8.1.1 Eigenen OpenPGP Schlüssel erstellen oder importieren

Um OpenPGP zu aktivieren, muss man in der Verwaltung des E-Mail Account unter *Ende-zu-Ende Verschlüsselung* einen Schlüsselpaar für OpenPGP erzeugen oder importieren.

Wenn man ein neues Schlüsselpaares erstellt, gibt es nicht viele Fragen (Abb. 8.1).

Wenn man bereits OpenPGP verwendet, kann man seinen bereits in GnuPG vorhandenen privaten Schlüssel in eine Datei exportieren und diese in Thunderbird importieren. Auf der Kommandozeile erledigt man den Export aus GnuPG in die Datei mit:

```
> gpg --export-secret-keys --armor user@sever.tls > mein-key.asc
```

Die Datei mit dem Schlüssel kann man als eigenen Schlüssel importieren.

8.1.2 Eigenen OpenPGP Schlüssel mit GnuPG verwenden

Die Verwaltung der privaten Schlüssel mit der OpenPGP.js Implementierung von Thunderbird ist zwar einfach aber aus Sicht der kryptografischen Sicherheit nur suboptimal. GnuPG schützt den privaten Schlüssel besser und für hohe Sicherheitsanforderungen sind Smartcards empfehlenswert.

Wer eine OpenPGP Smartcard verwendet oder den privaten Schlüssel nicht an Thunderbird übergeben sondern für hohe Sicherheitsanforderungen weiterhin die bereits vorhandene GnuPG Installation zur Verwaltung des privaten Schlüssel verwenden möchte, kann folgende Variable in den erweiterten Einstellungen von Thunderbird aktivieren:

```
mail.openpgp.allow_external_gnupg = true
```

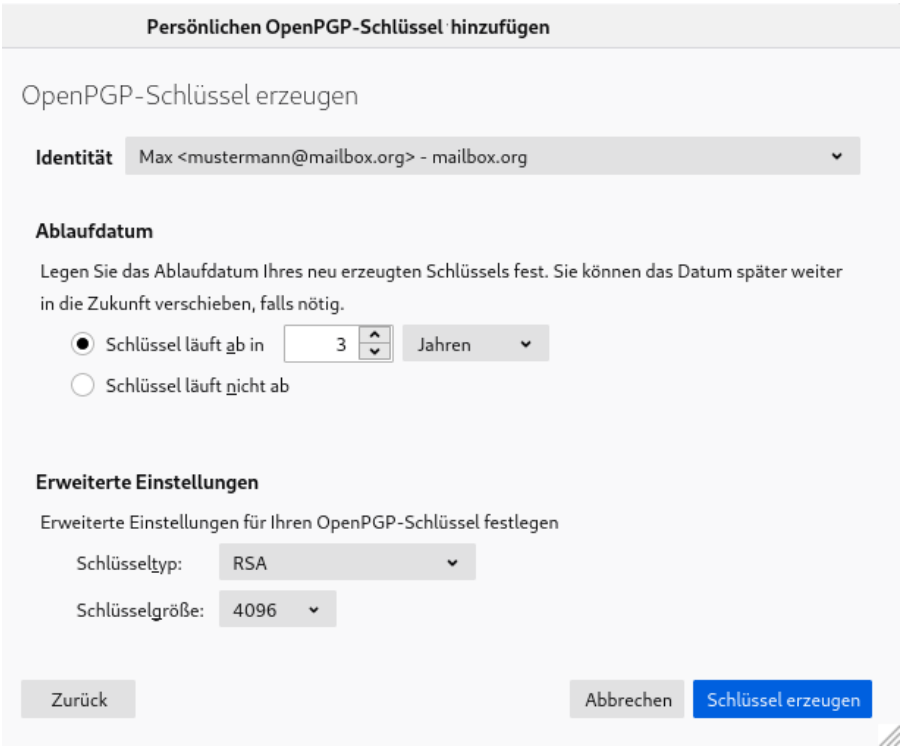


Abbildung 8.1: Neues OpenPGP-Schlüsselpaar in Thunderbird erstellen

Dann wird für die Einrichtung des eigenen Schlüssels eine dritte Option angeboten. Im folgenden Schritt kann man die ID des eigenen Schlüssels angeben, der im GnuPG Keyring liegt (Abb. 8.2). Der Zugriffsschutz für den privaten Key wird dann von GnuPG geregelt. Die Krypto-Operationen mit dem privaten Key werden dann ebenfalls von GnuPG ausgeführt statt mit OpenPGP.js in Thunderbird, was die kryptografische Sicherheit verbessert.

Den public Key und die Schlüssel der Kommunikationspartner muss man immer in Thunderbird importieren. Sie können nicht von einem externen GnuPG verwaltet werden.

8.1.3 Den eigenen öffentlichen Schlüssel verteilen

Damit Kommunikationspartner mir verschlüsselt schreiben oder die Signatur meiner E-Mail verifizieren können, muss man ihnen den eigenen öffnentlichen Schlüssel zusenden oder zum Download anbieten. Dafür gibt es mehrere Möglichkeiten:

1. Man kann den eigenen öffentlichen Schlüssel auf einem Webserver zum Download bereitstellen oder in einer Cloud hochladen und den Download Link für alle freigeben. In der Signatur jeder E-Mail weist man auf den Download hin und gibt damit dezent zu verstehen, dass man nach Möglichkeit verschlüsselte E-Mails bevorzugt.

   Echte Profis stellen den Schlüssel auch für Web key Discovery (WKD) bereit.

2. Man kann den öffentlichen Schlüssel in den OpenPGP Keyserver Pool hochladen.[3]

   Auf der Webseite kann man seinen eigenen Schlüssel hochladen. Es werden E-Mails mit der Aufforderung zur Bestätigung an alle Adressen gesendet, die im Schlüssel genannt sind. Die E-Mails enthalten einen Link, den man im Browser öffnen muss, um den Erhalt der E-Mail zu bestätigen. Danach wird der Schlüssel freigeschaltet.

   Die OpenPGP Keyserver bieten einen Link zum Download, den man in der E-Mail Signatur verwenden kann, um auf die Möglichkeit zum Download hinzuweisen.

[3] https://keys.openpgp.org

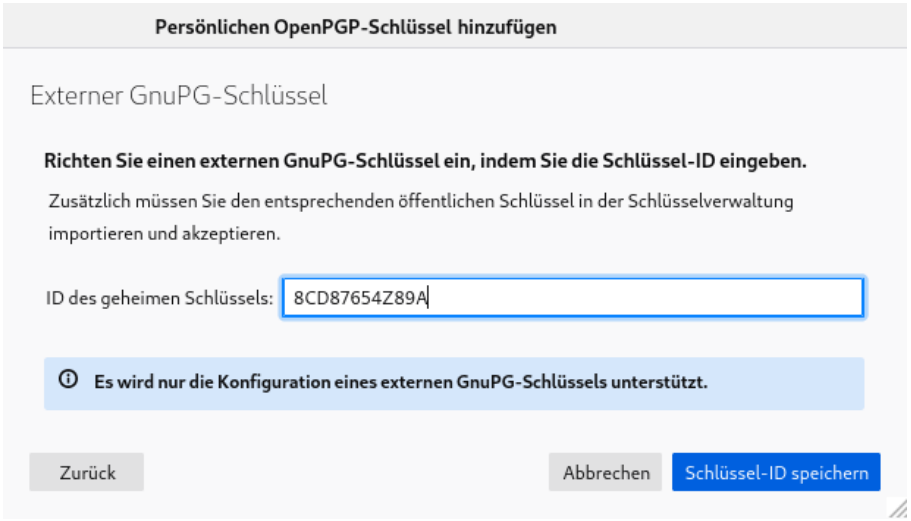


Abbildung 8.2: Privaten OpenPGP Schlüssel mit GnuPG verwalten

3. Man kann die Möglichkeiten nutzen, die E-Mail Provider zur Unterstützung der Schlüsselverteilung anbieten. Näheres findet man in den FAQ seines Providers.

4. Man kann es auch ganz klassisch machen und den Schlüssel an eine E-Mail als Attachment an eine signierte E-Mail anhängen. (Thunderbird fügt dabei auch einen Autocrypt Header ein, um anderen E-Mail Clients den Import zu erleichtern.)

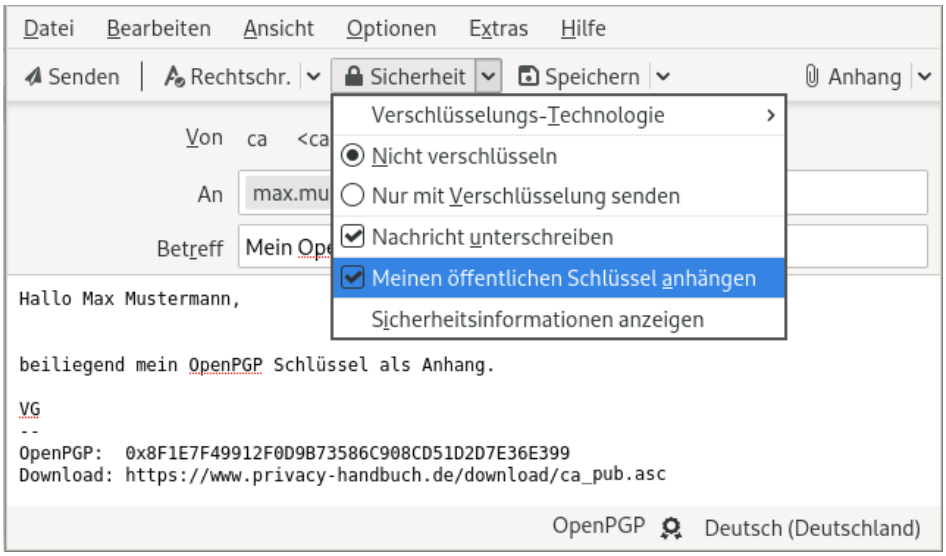
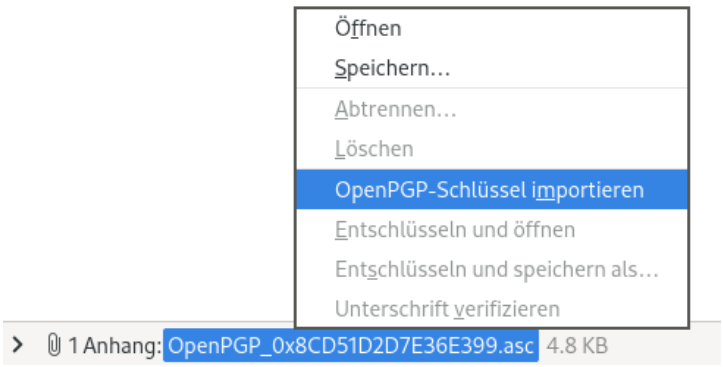


Abbildung 8.3: Öffentlichen OpenPGP Schlüssel per E-Mail verteilen

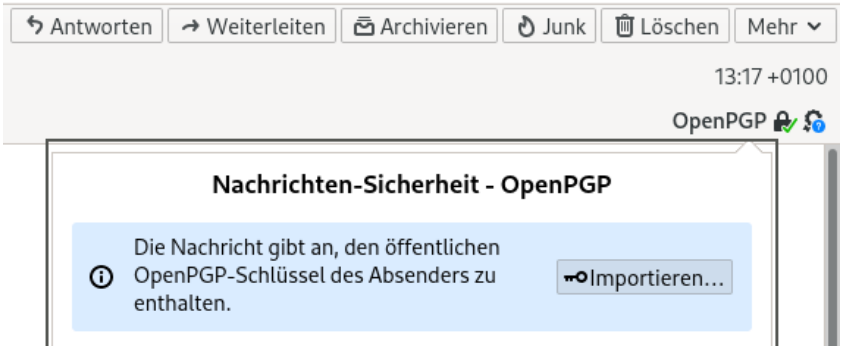
8.1.4 Fremde Schlüssel importieren

Für den Import der Schlüssel der Kommunikationspartner gibt es mehrere Möglicheiten:

1. Wenn man einen OpenPGP Schlüssel als Anhang per E-Mail erhalten hat, kann man ihn mit zwei Mausklicks importieren.



2. Wenn eine E-Mail einen Autocrypt Header mit dem OpenPGP-Schlüssel des Absenders enthält, kann man ihn ebenfalls mit zwei Mausklicks importieren.



3. In der OpenPGP Schlüsselverwaltung, die man unter *Extras - OpenPGP-Schlüssel verwalten* findet, gibt es weitere Optionen zum Importieren von Schlüsseln:

   - Man kann einen oder mehrere Schlüssel aus einer Datei importieren.
   - Man kann einen Schlüssel aus der Zwischenablage importieren.
   - Man kann den Schlüssel von einer Download URL abrufen, wenn man die Donwload URL auf einer Webseite findet oder in der Signatur einer E-Mail.
   - Man kann den Schlüssel anhand der E-Mail Addr. via Web Key Discovery (WKD) und auf OpenPGP Keyservern suchen und importieren.

8.1.5 Fremde Schlüssel akzeptieren bzw. verifizieren.

Es reicht nicht aus, die Schlüssel der Kommunikationspartner in Thunderbird zu importieren, um sie anschließend verwenden zu können. Man die muss die importierten Schlüssel noch akzeptieren oder anhand des Fingerabdruck den Schlüssels verifizieren, um ausdrücklich zu bestätigen, dass man diese Schlüssel in Zukunft verwenden will.

Um Schlüssel zu akzeptieren bzw. zu verifizieren, öffnet man die Schlüsselverwaltung, wählt den frisch importierten Schlüssel aus und öffnet den Dialog *Schlüsseleigenschaften*.

Auf dem Reiter *Ihre Akzeptanz* kann man angeben, dass man vermutlich den richtigen Schlüssel erhalten hat (akzeptieren) oder dass man den Fingerabdruck des Schlüssels über einen sicheren Kanal oder bei einem persönlichen Treffen mit dem Inhaber des Schlüssel verifiziert hat und dass man sicher ist, den richtigen Schlüssel zu verwenden (Abb. 8.4).

8.2 Gedanken zum Mailvelope Browser Add-on

Mailvelope ist ein Add-on für die Browser Mozilla Firefox und Google Chrome, das OpenPGP Verschlüsselung im Webinterface bietet und immer populärer wird. Es wird von

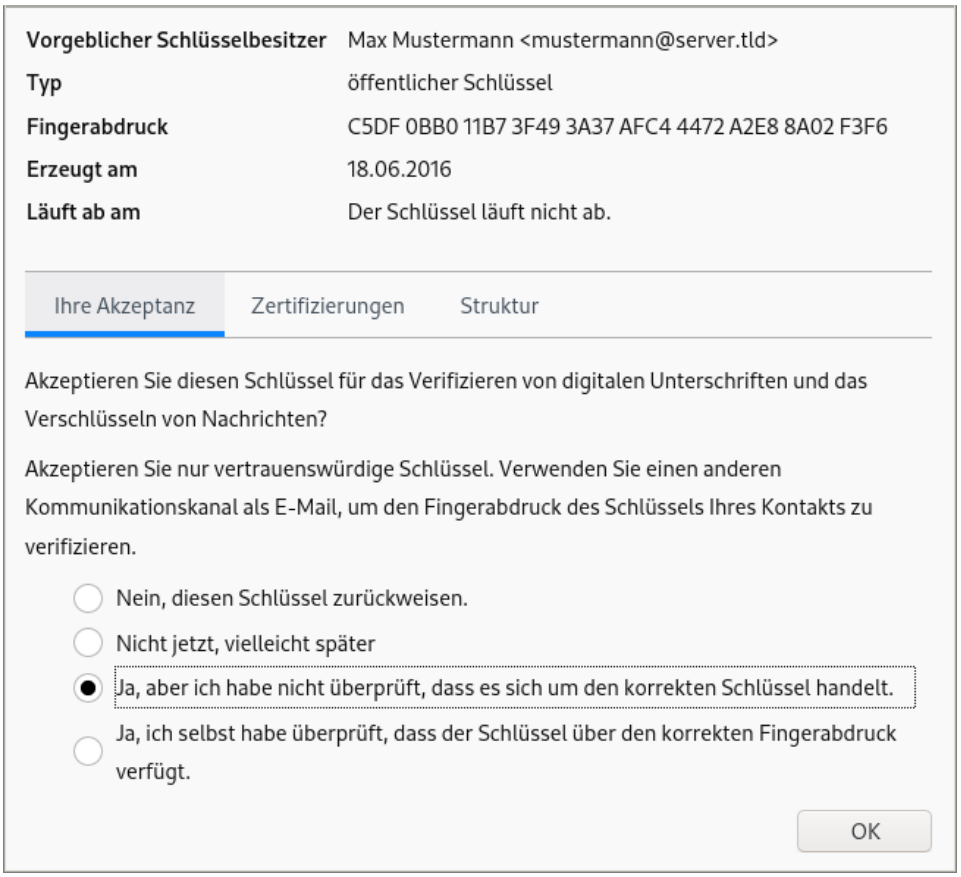


Abbildung 8.4: Importierten OpenPGP Schlüssel akzeptieren oder verifizieren

WEB.de, GMX.de und Posteo.de als sichere Lösung für Ende-zu-Ende Verschlüsselung im Browser beworben und auch vom BSI empfohlen. (Hmmm - das BSI hat manchmal seltsame Empfehlungen.)

Mailvelope kann die interne OpenPGP.js Implementierung nutzen oder eine externe GnuPG Installation. OpenPGP.js hat konzeptuell bedingt einige Schwächen und ist nicht für hohe Sicherheitsanforderungen geeignet. Konzeptuelle Schwächen von OpenPGP.js:

- **Unsichere Speicherung der Schlüssel:** Die Speicherung der Schlüssel im lokalen Storage des Browsers ist konzeptuell unsicher. Es wurden bei verschiedenen Audits immer wieder Angriffsmöglichkeiten via XSS (2015) oder mittels Clickjacking (2019) aufgedeckt, die ein Auslesen der privaten Schlüssel ermöglichten.
- **JavaScript ist nicht für starke Krypto geeignet:** Javascript wurde nicht als Programmiersprache für Krypto-Anwendungen entworfen. Best Practices für die Implementierung von Krypto sind mit Javascript nicht umsetzbar.

  JavaScript bietet keine Möglichkeiten, bei der Programmierung identische Ausführungszeiten für Code Verzweigungen zu erzwingen. Duch Seitenkanalangriffe ist es damit möglich, die Reihenfolge der Nullen und Einsen im privaten Schlüssel durch Beobachtung bei der Codeausführung zu rekonstruieren. In modernen Krypto-Bibliotheken ist das ein Securitybug (z.B. CVE-2016-7056 ECDSA P-256 timing attack key recovery, OpenSSL).

  Seitenkanalangriffe auf Browser sind einfach, da der Rechner nicht kompromittiert werden muss. Das Script für den Angriff kann von einer beliebigen Webseite geladen werden, wie Forscher in dem Paper *The Spy in the Sandbox – Practical Cache Attacks in JavaScript* gezeigt haben.

Mit JavaScript is es nicht möglich, einen geheimen Schlüssel nach der Benutzung aus dem Hauptspeicher zu löschen (Overwriting memory - why?). Das normale Verhalten von Mailvelope wurde bei Tor Onion Router als Security Bug eingestuft.[4]

Was in anderen Krypto-Implementierungen als schwerer Bug gilt, wird bei Mailvelope einfach als JavaScript Limitierung hingenommen.

In den FAQ von Mailvelope wird darauf hingewiesen, dass die geheimen Schlüssel durch das Senden eines Speicherabbildes in Absturzberichten an die Entwickler bei Mozilla oder Google kompromittiert werden könnten. Deshalb sollte man diese Funktion im Browser unbedingt deaktivieren.

8.2.1 Mailvelope mit GnuPG nutzen

Mailvelope bietet die Möglichkeit, eine lokale Installation von GnuPG zu verwenden statt der traditionelle Variante mit der OpenPGP.js Implementierung. Damit vermeidet man die oben genannten Schwächen von OpenPGP.js. Auch das Mailvelope Team empfiehlt in den FAQ[5] die Verwendung von GnuPG zur Verbesserung der Sicherheit. Die Verwendung von OpenPGP Smartcards ist nur Kombination mit GnuPG möglich und nicht mit OpenPGP.js.

Die Verwendung von GnuPG mit Mailvelope wird nicht funktionieren, wenn man unter Linux den Firefox Prozess unter Kontrolle von apparmor oder SELinux laufen lässt.

8.2.2 Mailvelope und Autocrypt

Standardmäßig verwendet Mailvelope den Autocrypt Schlüsseltausch. Da Autocrypt die Sicherheit von OpenPGP massiv schwächt, so dass die Verschlüsselung nur noch *some protection most of the time* bietet und keinen Schutz mehr gegen einen bösartigen E-Mail Provider, ist die Deaktivierung von Autocrypt im Dashboard dringend zu empfehlen.

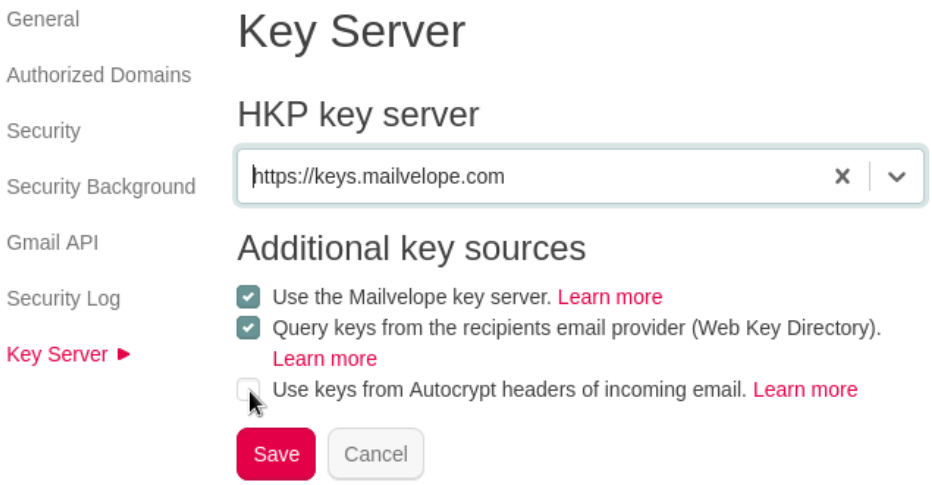


Abbildung 8.5: Autocrypt in Mailvelope deaktivieren

[4] https://heise.de/-1746523
[5] https://www.mailvelope.com/de/faq#gnupg

8.3 Einige Ergänzungen zum Thema GnuPG

GnuPG ist eine frei nutzbare Implementierung des OpenPGP Standards zur Verschlüsselung und Signierung von Daten. Es wird vom GNU Projekt ständig weiterentwickelt. Das Thunderbird Add-on Enigmail verwendet standardmäßig GnuPG 2.x.

Windows: Das Projekt gpg4win [6] stellt ein Paket für Windows bereit mit GnuPG, dem GNU Privacy Assisten für die Schlüsselverwaltung und einer Erweiterung für MS Outlook.

Linux, BSD: installieren GnuPG 2.x nicht immer vollständig. Manchmal muss man etwas nachinstallieren. Für Debian/Ubuntu funtioniert:

```
> sudo apt install gnupg2 gpg-agent pinentry-gtk2 scdaemon
```

Bei einigen Linux Dsitibutionen ist *gpg-agent* im Paket *gpgsm* enthalten. Der *gpg-agent* wird für die Eingabe der Passphrase benötigt und sollte beim Login automatisch gestartet werden. Dafür fügt man in der Konfiguration *$HOME/.gnupg/gpg.conf* folgende Zeile am Ende ein:

```
use-agent
```

In der Datei *$HOME/.gnupg/gpg-agent.conf* kann man konfigurieren, wie lange der Agent die Passphrase für einen Key speichert. Standardmäßig wird eine Passphrase 10min (600s) gespeichert. GPA ändert den Wert aus Sicherheitsgründen auf 300s.

```
default-cache-ttl 300
max-cache-ttl 360
```

Verbesserte Konfiguration von GnuPG

In der Konfigurationsdatei *gpg.conf* kann man nach der Installation ein paar kleine Verbesserungen vornehmen. Die Konfigurationsdatei findet man unter Windows in *%APPDATA%/GnuPG* und unter Linux/BSD im Verzeichnis *$HOME/.gnupg*.

Die Datei kann man mit einem Texteditor bearbeiten und folgende Optionen ergänzen bzw. durch Entfernen des Kommentarzeichens # aktivieren:

```
# keine Informationen über ersion und Betriebssystem einfügen
no-emit-version
no-comments

display-charset utf-8

# 16-stellige Key-IDs verwenden statt 8-stelliger (schwerer zu faken)
keyid-format 0xlong

# Keyserver-URLs in Keys ignorieren (Tracking möglich)
keyserver-options no-honor-keyserver-url, no-auto-key-retrieve, no-include-revoked

# Empfohlene Preferenzen für Krypto Algorithmen
personal-digest-preferences SHA512 SHA384 SHA256
personal-cipher-preferences AES256 AES192 AES TWOFISH
personal-compress-preferences Uncompressed ZIP ZLIB BZIP2
default-preference-list SHA512 SHA384 SHA256 AES256 AES192 AES Uncompressed
```

[6] http://www.gpg4win.org

```
# Signaturalgorithmus für Beglaubigungen
cert-digest-algo SHA512

# Einstellungen für symmetrische Verschlüsselung
s2k-cipher-algo AES256
s2k-digest-algo SHA384

# Cipher mit 64 Bit Blockgröße deaktivieren, weil sie
# schwach sind und ohne MDC verwendet werden (siehe: #Efail)
disable-cipher-algo 3DES
disable-cipher-algo IDEA

# SHA1 als schwachen Algorithmus markieren (wie MD5)
weak-digest SHA1

# sonstiges
fixed-list-mode
verify-options show-uid-validity
list-options show-uid-validity
```

Bei der Erstellung eines OpenPGP Schlüssels werden die aktuell konfigurierten *Default Preference List* für Krypto-Algorithmen in den Schlüssel übernommen. GnuPG verwendet die für den Schlüssel gültigen Preferenzen immer dann, wenn keine Preferenzen in der Konfiguration angegeben wurden, wenn der Kommunikationspartner also keine persönlichen Preferenzen in seiner Config definiert hat.

Wenn man vor einigen Jahren seinen Schlüssel erstellt hat, dann wird in diesem Fall beispielsweise das angeknackste SHA-1 als Digest-Algorithmus bevorzugt verwendet. Man muss die persönlichen Preferenzen auch in die eigenen Schlüssel übernehmen und die Schlüssel danach neu verteilen. Das geht nur auf der Kommandozeile. Man muss das GnuPG Kommandozeilen Tool gpg2 mit der Option *–edit-key* und der Key-ID aufrufen. Danach kann man sich mit dem Kommando *showpref* die Preferenzen für diesen Schlüssel anzeigen und mit dem Kommando *setpref* die Defaults übernehmen:

```
> gpg2 --edit-key mustermann@server.tld
gpg (GnuPG) 2.1.x; Copyright (C) 2016 Free Software Foundation, Inc.
...
gpg> showpref
[ unbekannt ] (1). Max Mustermann <mustermann@server.tld>
   Verschlü.: AES256, AES192, AES, CAST5, 3DES
   Digest: SHA1, SHA256, RIPEMD160
   Komprimierung: nicht komprimiert, ZLIB, BZIP2, ZIP
   Eigenschaften: MDC, Keyserver no-modify

gpg> setpref
Setze die Liste der Voreinstellungen auf:
   Verschlü.: AES256, AES192, AES, 3DES
   Digest: SHA512 SHA384 SHA256, SHA1
   Komprimierung: nicht komprimiert
   Eigenschaften: MDC, Keyserver no-modify
Die Voreinstellungen wirklich ändern? (j/N) j
...
Sie benötigen die Passphrase, um den geheimen Schlüssel zu entsperren.
Benutzer: "Max Mustermann <mustermann@server.tld>"
...
gpg> quit
Änderungen speichern? (j/N) j
```

8.3.1 Gedanken zur Auswahl und Stärke von Schlüsseln

Aktuelle GnuPGP Versionen unterstützen neben RSA und DSA Schlüsseln mit bis zu 4096 Bit Länge auch Schlüssel auf Basis elliptischer Kurven. Alle Optionen hat man zur Auswahl, wenn man ein Schlüsselpaar auf der Kommandozeile im Experten-Modus erstellt:

```
> gpg2 --expert --full-gen-key
```

Welche Schlüssel sollte man nutzen? Ein paar Gedanken zur Auswahl:

1. RSA Schlüssel werden von allen PGP Implementierungen problemlos verwendet. Bei ausreichender Schlüssellänge > 2000 Bit gelten diese Schlüssel als sicher.
2. Das BSI ist derzeit der Meinung, dass RSA Schlüssel mit einer Länge von 2048 Bit bis 2022 eingesetzt werden können (BSI TR-02102-1). (Wenn man also jetzt einen neuen Schlüssel generiert, der für 5 Jahre gültig ist und dann möglicherweise verlängert werden soll, dann sollte man mindestens 3072 Bit Schlüssellänge wählen.)
3. Schlüssel auf Basis elliptischer Kurven werden nur in aktuellen PGP Implementierungen unterstützt, die sich aber noch nicht überall durchgesetzt haben.
4. Für den Einsatz elliptischer Kurven in PGP gibt es folgende Standards:
   - Der RFC 6637 der IETF empfiehlt nur die NIST-Kurven P-256, P-384 und P-512 für OpenPGP.
   - Die Java Bibliothek BountyCastle sowie PGP Implemtierungen für C# und VB.net können außerdem mit den Brainpool Kurven nach RFC 5639 umgehen.
   - Das GnuPGP Team hat mit RFC 4880bis Draft eine Erweiterung vorgeschlagen, auch die Unterstützung für die Kurven Ed25519 und Curve25519 zu integrieren. Dieser Draft ist bisher nur in GnuPG 2.1.x umgesetzt worden.

   Wer jetzt schon Schlüssel auf Basis elliptischer Kurven verwendet, muss mit Problemen bei einigen Empfängern rechnen, insbesondere mit den elliptischen Kurven Ed25519 und Curve25519. Empfehlenswert für langfristige Nutzung sind RSA Schlüssel mit 4096 Bit Länge.

8.3.2 GnuPG Smartcards nutzen

Die Sicherheit asymmetrischer Verschlüsselung hängt von der sicheren Aufbewahrung des privaten Svhlüssels ab. Es gibt mehrere Möglichkeiten, wie privaten Keys kompromittiert werden könnten:

- Wenn man GnuPG auf mehreren Computern nutzt, auf denen andere Nutzer Administrator- bzw. Root-Privilegien haben, könnten die privaten Keys von Administratoren eingesammelt werden.
- Böswillige Buben können mit einem Trojaner versuchen, den privaten Key zu kopieren und die Passphrase mit Keyloggern oder mit Tools wie *Elcomsoft Distributed Password Recovery* ermitteln.
- Die unbedachte Entsorgung einer Festplatte oder eines Computers ist ein weiteres Risiko, wenn die privaten Daten nicht sicher gelöscht wurden.

Smartcards ermöglichen eine sichere Nutzung von GnuPG unter diesen Bedingungen. Der private Key ist nicht auf dem Rechner sondern ausschließlich auf der Smartcard gespeichert, er verläßt diese sichere Umgebung nicht und alle Krypto-Opertionen, die den privaten Schlüssel nutzen, werden auf der Smartcard ausgeführt. Die Nutzung von Smartcards hätte wahrscheinlich die Kompromittierung der Schlüssel von Cryptome.org[7] verhindern können.

Ein paar Angebote für OpenPGP Smartcards:

[7] http://heise.de/-2817797

- Die **GnuPG-Smartcard** gibt es von kernelconcepts.de[8]. Die Bestellung erfolgt per E-Mail und man braucht zusätzlich einen Smartcard Reader oder den ebenfalls dort erhältlichen Gemalto USB Adapter.

- Der **NitroKey**[9] ist ein Open Source Hardware Projekt und der Nachfolger des Cryptostick. Der NitroKey Pro enthält zusätzliche einen OTP-Generator und Passwortspeicher. (Für diese Zusatzfunktion ist die NitroKey App[10] zu installieren.)

- Der **Yubikey** ist ein One-Time-Passwordgenerator (OTP), den man für Logins bei Webdiensten nutzen kann. Er enthält zusätzlich eine OpenPGP Smartcard.[11]

Erster Test

Die GnuPG Software Collection kann Smartcards *out-of-the-box* nutzen. Zuerst sollte man prüfen, ob alles funktioniert und die Smartcard erkannt wird. Smartcard anschließen und auf der Konsole bzw. in der DOS-Box folgendes Kommando eingeben:

```
> gpg2 --card-status
Application ID ...: D27600xxxxxxxxxxxxxxx
Version ..........: 2.0
Manufacturer .....: unknown
...
```

Wenn keine Smartcard gefunden wird, kann man zuerst prüfen, ob die GnuPG Software Collection vollständig installiert wurde (*gpg2* + *gpg-agent* + *scdaemon*) und ob der gpg-agent läuft. Bekannte Probleme gibt es auch mit dem GNOME Keyring Manager (siehe unten).

Funktionen für Genießer

Die Nutzung von gpg2 auf der Kommandozeile bietet etwas mehr Möglichkeiten, als die GUIs von Enigmail oder GPA zur Verfügung. Natürlich stehen auch die mit dem GUI durchführbaren Funktionen auf der Kommandozeile zur Verfügung. Einen Überblick über alle Smartcard-Funktionen gibt die Hilfe mit dem *help* Kommando. Als erstes muss man den Admin Mode aktivieren, dann hat man vollen Zugriff auf alle Funktionen:

```
> gpg2 --card-edit
...
gpg/card> admin
Admin-Befehle sind erlaubt

gpg/card> help
...
gpg/card> quit
```

Neue Schlüssel generiert man auf der Smartcard mit *generate*, die PIN und Admin-PIN kann man mit *passwd* ändern, mit *unblock* kann man den Zähler für Fehlversuche zurück setzen und *factory-reset* löscht alle Schlüssel auf der Smartcard.

Neuer oder fremder Rechner - was nun?

Ein nettes Feature von OpenPGP Smartcards ist es, an einem neuen oder fremden Rechner den Public Key von einer Download Adresse holen zu können. Der private Key ist auf der Card in einer sicheren Umgebung, somit kann man auch unterwegs auf einem halbwegs

[8] https://www.floss-shop.de/de/search?sSearch=OpenPGP
[9] https://www.nitrokey.com/de
[10] https://www.nitrokey.com/de/download
[11] https://www.yubico.com/products/yubikey-hardware/

vertrauenswürdigen, fremden Rechner eines Bekannten mit vollständiger GnuPG Installation die PGP-Verschlüsselung nutzen ohne den privaten Schlüssel zu kompromittieren.

Der Download des Public Key steht nur auf der Kommandozeile zur Verfügung. Nach dem Abrufen des Public Key von der Download URL muss man noch einmal den Card-Status aufrufen, damit der private Schlüssel an den Public Key gebunden wird:

```
> gpg2 --card-edit
...
gpg/card> fetch        (Abrufen des Public Key von der Download URL)
gpg/card> quit
...
> gpg2 --card-status    (Re-bind von private und public Key)
...
```

Vorhandenen Schlüssel mit Smartcard weiter verwenden

Wenn man bereits PGP für die Verschlüsselung nutzt und einen vorhandenen Schlüssel weiter verwenden möchte, dann kann man die Private Keys dieses Schlüssel auch auf eine OpenPGP Smartcard übertragen. Damit erspart man sich die Verteilung eines neuen Schlüssels und kann die Beglaubigungen des Web-of-Trust behalten.

GnuPG erstellt standardmäßig Schlüsselpaare mit einem Hauptschlüssel zum Signieren und Beglaubigen sowie einen Unterschlüssel zum Verschlüsseln. Die OpenPGP Smartcard kennt drei Schlüssel, einen Schlüssel zum Signieren, einen Schlüssel zum Verschlüsseln und einen Schlüssel zum Authentifizieren. Man muss den von GnuPG erstellten Haupt- und Unterschlüssel einzeln auf die korrespondierenden Plätze auf der Smartcard schieben.

Als erstes ruft man *gnupg2* mit der *edit-key* Funktion für den Schlüssel auf, den man auf die Smartcard verschieben will. Mit *toggle* schaltet man auf die Verwaltung der privaten Keys. Dann schiebt man mit *keytocard* zuerst den Hauptschlüssel als Signatur Key auf die Smartcard, wählt den Subkey mit *key 1* aus und schiebt den Encryption Subkey auf den passenden Platz auf der Smartcard.

```
> gpg2 --edit-key mustermann@server.tld
Geheimer Schlüssel ist vorhanden.
...
gpg> toggle

sec  rsa2048/8A02F3F6
     erzeugt: 2016-06-18  verfällt: niemals   Aufruf: SC
ssb  rsa2048/08D68793
     erzeugt: 2016-06-18  verfällt: niemals   Aufruf: E


gpg> keytocard
Den Hauptschlüssel wirklich verschieben? (j/N) j
Wählen Sie den Speicherort für den Schlüssel:
    (1) Signatur-Schlüssel
    (3) Authentisierungs-Schlüssel
Ihre Auswahl? 1

gpg> key 1

sec  rsa2048/8A02F3F6
     erzeugt: 2016-06-18  verfällt: niemals   Aufruf: SC
ssb*  rsa2048/08D68793
```

```
      erzeugt: 2016-06-18  verfällt: niemals   Aufruf: E

gpg> keytocard
Wählen Sie den Speicherort für den Schlüssel:
   (2) Verschlüsselungs-Schlüssel
Ihre Auswahl? 2

gpg> quit
Änderungen speichern? (j/N) j
```

Danach kann man den Status der Smartcard prüfen und sich davon überzeugen, dass die beiden Schlüssel jetzt als *Signature key* und *Encryption key* auf der Smartcard liegen:

```
> gpg2 --card-status

Reader ...........: 20A0:4108:000036C40000000000000000:0
Application ID ...: D2760001240102010005000036C40000
Version ..........: 2.1
...
PIN retry counter : 3 0 3
Signature counter : 0
Signature key ....: C5DF 0BB0 11B7 3F49 3A37  AFC4 4472 A2E8 8A02 F3F6
      created ....: 2016-06-18 15:32:07
Encryption key....: 94E1 D64A 51C0 8C78 CE60  6472 0059 00DC 08D6 8793
      created ....: 2016-06-18 15:32:07
Authentication key: [none]
General key info..: pub  rsa2048/8A02F3F6 <mustermann@server.tld>
sec   rsa2048/8A02F3F6  erzeugt: 2016-06-18  verfällt: niemals
ssb   rsa2048/08D68793  erzeugt: 2016-06-18  verfällt: niemals
```

8.3.3 Adele - der freundliche OpenPGP E-Mail-Roboter

Adele ist der freundliche OpenPGP E-Mail-Roboter der G-N-U GmbH. Man kann mit dem Robot seine ersten verschlüsselten Mails austauschen und ein wenig üben ohne Freunde mit Anfängerproblemen zu belästigen.

1: Den eigenen Schlüssel an Adele senden: Als erstes schickt man den eigenen öffentlichen Schlüssel per E-Mail an *adele@gnupp.de*. Den Schlüssel hängt man als Anhang an die Mail an, indem man die Option *OpenPGP - Meinen öffentlichen Schlüssel anhängen* vor dem Versenden der Mail aktiviert (Bild **??**)

2. Verschlüsselte Antwort von Adele: Als Antwort erhält man nach einigen Minuten eine verschlüsselte E-Mail von Adele. Die E-Mail wird nach Abfrage der Passphrase entschlüsselt und enthält den Schlüssel von Adele:

```
Hallo,

hier ist die verschlüsselte Antwort auf Ihre E-Mail.

Ihr öffentlicher Schlüssel wurde von mir empfangen.

Anbei der öffentliche Schlüssel von adele@gnupp.de,
dem freundlichen E-Mail-Roboter.

Viele Grüße,
adele@gnupp.de
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (GNU/Linux)

mQGiBDyFlIkRBACfVHJxv47r6rux7TwT4jHM7z/2VfyCrmcRegQEsbdLfqu3mEmK
RouuaDQukNINWk2V2ErOWzFnJqdzpapeuPJiOWp0uIEvU3FRPhYlytw9dFfwAHv4
MJ7639tAx9PfXBmZOd1PAoE451+VLhIGlLQiFGFppJ57SZ1EQ71/+/nkSwCg8Mge
....
EQIABgUCPIWUlQASCRDlczRpkqs/9wdlR1BHAAEBv20AoJJGeeZjMCSbXtmNSwfW
QsLOd0+4AKCdXwt552yi9dBfXPo8pB1KDnhtbQ==
=ERT8
-----END PGP PUBLIC KEY BLOCK-----
```

3. Schlüssel von Adele importieren: Man kann die Zeilen von `BEGIN PGP PUBLIC KEY BLOCK` bis einschließlich `END PGP PUBLIC KEY BLOCK` mit der Maus markieren, in die Zwischenablage kopieren und in der Schlüsselverwaltung über *Bearbeiten - Aus Zwischenablage importieren* einfügen.

Alternativ holt man sich Adeles Schlüssel mit der ID 0x92AB3FF7 von einem Keyserver.

4. Adele verschlüsselte E-Mails schreiben Jetzt kann man Adele verschlüsselte E-Mails schicken. Als Antwort erhält man umgehend eine gleichfalls verschlüsselte E-Mail mit dem gesendeten Text als Zitat.

```
Hallo,

hier ist die verschlüsselte Antwort auf Ihre E-Mail.

Ich schicke Ihnen Ihre Botschaft im Wortlaut zurück, damit Sie
sehen, dass ich sie erfolgreich entschlüsseln konnte.

> Hello Adele,
>
> hope you are feeling well.
```

Hinweis: PGP/Inline statt PGP/MIME verwenden. Adele ist schon eine etwas ältere Dame und versteht nur das alte Format PGP/Inline während Enigmail inzwischen das modernere PGP/MIME Format verwendet.

Beim Schreiben einer E-Mail an Adele muss man deshalb immer auf PGP/Inline umschalten, anderenfalls kann Adele die Mail nicht interpretieren. Menüpunkt *Enigmail - Protokoll PGP/Inline* aktivieren!

8.3.4 Memory Hole Project

Eine E-Mail enthält im Header viele Informationen. Neben dem *Betreff:* steht dort auch, auf welche E-Mail geantwortet wurde (*In-Reply-To:* und *References:*). Diese Informationen sind für den Transport der E-Mail nicht nötig und könnten verschlüsselt übertragen werden.

```
To: Max Mustermann <mustermann@server.tld>
From: Maxi Muterfrau <musterfrau@server.tld>
Subject: Re: Plenum der K-Gruppe (KaG) am 32.02.2017 um 26:20 Uhr
References: <5cc396a27b873f3fa@mailbox.org>
In-Reply-To: <5cc396a27b873f3fa@mailbox.org>
Message-ID: <49e6a7bfbc433sfgcfge@secure.mailbox.org>
Date: Wed, 29 Mar 2017 21:55:37 +0200
MIME-Version: 1.0
```

```
Content-Type: multipart/encrypted;
    protocol="application/pgp-encrypted";
...
```

Das Memory Hole Projekt möchte einen Ansatz entwickelt, um die für den Transport unwichtigen Informationen ebenfalls zu verschlüsseln. Die Headerzeilen werden dabei in dem verschlüsselten PGP/MIME Part versteckt und können nur vom Empfänger bei der Entschlüsslung der Mail gelesen und sichtbar gemacht werden.

Enigmail unterstützt dieses Feature bereits. Wenn man die folgenden Parameter setzt, wird der Mail Header *Betreff:* in OpenPGP verschlüsselten E-Mails durch die konfigurierte Floskel *Encrypted Message* ersetzt und der originale Text in den verschlüsselten PGP/MIME Part verschoben. Wenn die Mail entschlüsselt wird, wird der Betreff wieder hergestellt.

```
extensions.enigmail.protectedHeaders      = 2
extensions.enigmail.protectedSubjectText  = Encrypted Message
```

Außerdem kann man die Header *In-Reply-To:* und *References:* im PGP/MIME Part verstecken, indem man zusätzlich folgenden Parameter setzt:

```
extensions.enigmail.protectReferencesHdr  = true
```

Als Ergebnis würden dann die E-Mail Header aus dem oben gezeigten Beispiel wie folgt aussehen:

```
To: Max Mustermann <mustermann@server.tld>
From: Maxi Muterfrau <musterfrau@server.tld>
Subject: Encrypted Message
Message-ID: <49e6a7bfbc433sfgcfge@secure.mailbox.org>
Date: Wed, 29 Mar 2017 21:55:37 +0200
MIME-Version: 1.0
Content-Type: multipart/encrypted;
    protocol="application/pgp-encrypted";
...
```

8.3.5 Autocrypt

Das Verfahren Autocrypt will den Nutzern den manuellen PGP-Schlüsselaustausch abnehmen und ihn dadurch nutzerfreundlich machen. Der PGP-Schlüssel soll im Header jeder E-Mail mitgesendet werden, damit der Empfänger sofort automatisch verschlüsselt antworten kann, ohne sich um den Schlüsseltausch (und Validierung?) zu kümmern.

Für die theoretische Begründung der Sicherheit greift Autocrypt auf das Konzept Opportunistic Security (RFC 7435) zurück. Das bedeutet, das die Verschlüsselung nur noch gegen passive Angreifer schützt soll aber nicht mehr gegen aktive Angreifer, die sich als man-in-the-middle in die Kommunikation einschleichen können.

Wenn jemand **Opportunistic Security** verspricht, dann funktioniert die Verschlüsselung ganz gut, solange sich niemand ernsthaft für die Kommunikation interessiert. Gegen einen ernsthaften, aktiven Angriff bietet dieses Konzept keinen Schutz und man muss im Zweifel davon ausgehen, dass die Verschlüsselung genau dann kompromittiert wird, wenn man sie gebracuht hätte. Opportunistic Security bietet ausdrücklich nur **Some Protection Most of the Time**.

Wie könnte ein E-Mail Provider die Verschlüsselung kompromittieren?

1. Die E-Mail Header werden von den Mailprovidern ständig routiniert manipuliert. Es werden neue Header eingefügt, einige Header werden gelöscht... In gleicher Weise könnten die Autocrypt Header von den versendenden oder empfangenen E-Mail Providern manipuliert werden und ein falscher Schlüssel eingefügt werden.

2. Es ist keine kryptografische Validierung der OpenPGP Schlüssel vorgesehen, die im Autocrypt Header gesendet werden. Der E-Mail Client soll den jeweils neuesten Schlüssel ohne Überprüfung akzeptieren. Wenn ein E-Mail Provider den PGP Schlüssel im Autocrypt Header gegen einen falschen Key austauscht, dann wird der Empfänger der Mail diesen falschen Schlüssel mit hoher Wahrscheinlichkeit verwenden.

3. Wenn ein Antwort geschrieben wird, kann der E-Mail Provider natürlich erkennen, dass eine Mail mit dem Fake Schlüssel verschlüsselt wurde. Er entschlüsselt die Mail, nimmt den Inhalt zu Kenntnis und verschlüsselt sie dann mit dem richtigen Schlüssel, bevor er sie zustellt. Das Opfer bemerkt nicht, dass der PGP Schlüssel ausgetauscht wurde.

Das ist kein Bug sondern ein Feature des zugrunde liegenden Konzeptes.

Das ein solches Szenario nicht nur theoretisch sondern auch in der Praxis relevant sein kann, hat der E-Mail Provider Hushmail demonstriert. 2007 wurde Hushmail von der US-amerikanische DEA gezwungen, die PGP Verschlüsselung für einige Kunden mit gefälschten Schlüsseln zu kompromittieren. Und die Spezialisten der Behörde ZITiS klatschen bestimmt vor Freude in die Hände, wenn Autocrypt großflächig eingesetzt wird.

Ende-zu-Ende Verschlüsselung soll den Inhalt von E-Mails gegen Beobachtung durch die E-Mail Provider schützen. Der E-Mail Provider ist der potentielle **Angreifer**, gegen den uns Ende-zu-Ende Verschlüsselung schützen soll! Eine E2E-Verschlüsselung, die nur unter der Vorraussetzung funktioniert, dass der E-Mail Provider vertrauenswürdig ist, wird zu Bullshit. Wenn auch noch erwartet wird, dass der Provider den Schlüsseltausch durch DKIM Signaturen der Header absichern muss, dann steht die Welt auf dem Kopf.

Der Autocrypt Schlüsseltausch erfordert es, dass man dem E-Mail Provider vertrauen muss und führt damit Ende-zu-Ende Verschlüsslung mit OpenPGP ad absurdum, es kompromittiert die Sicherheit zugunsten (zweifelhafter) Vereinfachungen der Usability.

8.3.6 Verschlüsselung in Webformularen

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

Einige grafische Tools für die Schlüsselverwaltung wie GPA[12] (*GNU Privacy Assistent*) enthalten einen Editor. Man kann den Text in diesem Editor schreiben, mit einem Klick auf den entsprechenden Button signieren oder verschlüsseln und das Ergebnis über die Zwischenablage in die Textbox der Website einfügen. Das Entschlüsseln funktioniert in umgekehrter Reihenfolge.

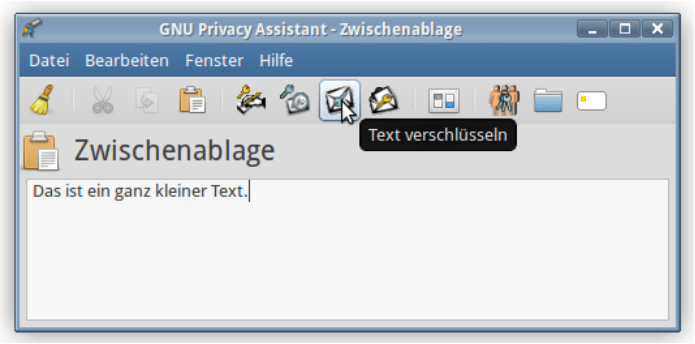


Abbildung 8.6: Text mit GPA verschlüsseln

[12] http://www.gnupg.org/related_software/gpa/index.de.html

Andere grafische Tools wie *Kleopatra* von KDE Projekt bieten die Ver- und Entschlüsselung des Textes in der Zwischenablage an. Um eine verschlüsselte Nachricht zu versenden, schreibt man den Text mit einem beliebigen Editor (Notepad, gedit, mousepad, kwrite...), kopiert danach den gesamten Text in die Zwischenablage (mit den Tasten STRG-A und STRG-C) und wählt dann die Option zum Verschlüsseln der Zwischenablage im Menü (Abb: 13.2). Nach der Auswahl der Empfänger wird der Text aus der Zwischenablage verschlüsselt und das verschlüsselte Ergebnis wieder in der Zwischenablage gespeichert. Diesen unlesbaren Zeichensalat kann man im Textfeld im Webformular einfügen (Taste: STRG-V). Entschlüsseln funktioniert wieder in umgekehrter Reihenfolge.

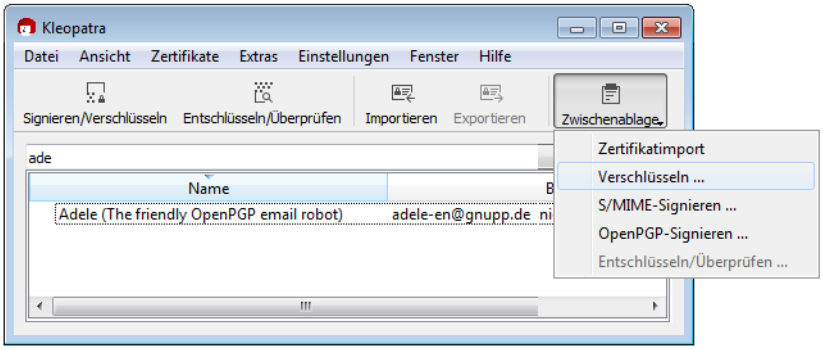


Abbildung 8.7: Kleopatra GnuPG GUI: Assinstent zur Verschlüsselung von Dateien

Linuxer könnten auch das GnuPG Desktop Applet von den TAILS Entwicklern nutzen, das ebenfalls den Text in der Zwischenablage ver- oder entschlüsseln kann. Das Applet kann unter Debian/Ubuntu mit dem bevorzugten Paketmanager installiert werden:

```
> sudo apt install openpgp-applet
```

8.3.7 OpenPGP-Verschlüsselung für Kontaktformulare

Dass Metadaten (z.B. Absender und Empfänger einer E-Mail) für die Überwachung eine große Rolle spielen, ist seit den Veröffentlichungen von Snowden/Greenwald allgm. bekannt. Leser des Privacy-Handbuches haben es evtl. vorher gewusst (siehe: Kommunikationsanalyse).

Kontaktformulare bieten eine Möglichkeit, diese Metadaten zu verschleiern. Wer ein Blog oder eine Webseite betreibt, kann recht einfach ein Kontaktformular zur Verfügung stellen. Es gibt Wordpress Plug-ins für Kontaktformulare, einfache PHP-Scripte oder fertige Perl-CGI Scripte. Man kann eine individuell passende Lösung wählen.

Dabei sollte man auf folgendes achten:

1. Das Kontaktformular sollte den Absender nicht zur Eingabe seiner E-Mail Adresse zwingen. Als work-around kann man im HTML-Code des Formulars das Feld für die Absender E-Mail Adresse als *hidden* deklarieren und einen Standardwert setzen.

2. Das Script sollte die IP-Adresse des Absenders nicht in den Header der E-Mail einfügen. Einige Scripte für Kontaktformulare wollen damit den Spam-Schutz verbessern. Einfach ausprobieren.

3. Das Kontaktformular sollte immer via HTTPS (SSL-verschlüsselt) aufgerufen werden. Wenn die Webseite auch via plain HTTP erreichbar ist, sollten alle Links auf der Webseite zum Kontaktformular mit der vollständigen URL angegeben werden:

```
<a href="https://www.server.tld/kontakt.html">Kontakt</a>
```

Jeder gute Webhoster bietet inzwischen SSL-Verschlüsselung für einen kleinen Aufpreis für alle Kunden, Wordpress.com hat es standardmäßig aktiviert.

Im folgenden möchte ich einige Möglichkeiten vorstellen, wie man ein Kontaktformular mit OpenPGP-Verschlüsselung aufmotzen könnte.

Hinweis: Bei allen Varianten handelt es sich um *server based crypto*, die nicht die gleiche Sicherheit wie richtige Ende-zu-Ende Verschlüsselung gewährleisten kann. Diese Verschlüsselung schützt gegen passive Lauscher am Draht, kann aber durch potente aktive Angreifer kompromittiert werden.

Ganz einfach ohne Programmierung

Man kann einen guten E-Mail Provider nutzen, der TLS-Verschlüsselung für eingehende E-Mails erzwingen kann und ein verschlüsseltes Postfach bietet, z.B. mailbox.org.

- Nachdem man einen E-Mail Account bei mailbox.org erstellt und bezahlt hat, ist der Alias für TLS-verschlüsselten Versand/Empfang zu aktivieren sowie das OpenPGP verschlüsselte Postfach zu aktivieren und der eigene public Key hochzuladen.
- Im Script des Kontaktformulars konfiguriert man als Empfänger die E-Mail Adresse *<name>@secure.mailbox.org* bzw. *<name>@tls.mailbox.org*.

Vom Browser des Absenders wird die Nachricht SSL-verschlüsselt zum Webserver übertragen. Von dort wird sie über eine TLS-verschlüsselte Verbindung an Mailbox.org gesendet und auf dem Mailserver mit dem OpenPGP-Key verschlüsselt.

Diese Variante schützt den Inhalt der Nachrichten gegen den allgemeinen Überwachungswahn und bei Beschlagnahmung von Daten. Sie schützt nicht gegen eine TKÜ nach §100 a/b StPO beim Hoster des Kontaktformulars oder beim E-Mail Provider, da der Inhalt als Plain-Text an diesen Stellen mitgelesen werden kann.

Mit JavaScript im Browser des Absenders

Diese Variante erfordert HTML-Kenntnisse, um einige Anpassungen im HTML-Code des Kontaktformulars vorzunehmen und die Bibliothek *OpenPGPjs* einzubinden.

Hinweis: Verschlüsselung mit JavaScript im Browser bietet keine hohe Sicherheit, lediglich hinreichende Sicherheit. Die Gründe wurden bereits mehrfach erwähnt. Für den Erstkontakt ist es aber besser als eine unverschlüsselte E-Mail.

1. Die Javascript Bibliothek *openpgp.min.js* aus dem Projekt OpenPGPjs[13] ist bei Github auszuchecken und aus dem Verzeichnis *dist* auf den eigenen Webserver kopieren.
2. Das JavaScript Schnipselchen *encrypt_message.js* von der Webseite im Privacy Handbuch[14] herunter laden und auf den Webserver kopieren. Dieses JavaScript Schnipselchen verschlüsselt das Textarea Feld mit der ID *message* mit dem OpenPGP-Schlüssel, der in dem DIV Container *pubkey* steht. Wenn das Textarea oder der DIV Container im Formular eine andere ID haben, sind die Zeilen 5 und 6 anzupassen:

```
function encrypt_message() {
  if (!(window.crypto && window.crypto.getRandomValues)) {
    window.alert("Fehler: der Browser ist veraltet und wird nicht supported!");
  } else {

    var message = document.getElementById("message");
    var pgpkey = document.getElementById("pubkey");
```

[13] https://github.com/openpgpjs/openpgpjs
[14] https://www.privacy-handbuch.de/handbuch_32v.htm

```
    if(message.value == "") {
        window.alert("Kein Text gefunden, das Textfeld ist leer!");
    } else {
        # Verschlüsseln des Textes im Textarea
        var options = { data: message.value,
             publicKeys: openpgp.key.readArmored(pgpkey.innerHTML).keys
         };
        openpgp.encrypt(options).then(function(ciphertext) {
             message.value = ciphertext.data; });
        # Button für Verschlüsseln deaktivieren
        document.getElementById("encrypt").disabled = true;
        document.getElementById("send").disabled = false;
    }
  }
}
```

3. Im HTML-Header der Webseite des Formulares sind die Scripte zu laden:

```
...
<script src="openpgp.min.js" async></script>
<script src="encrypt_message.js" async></script>
...
```

4. Im HTML-Code des Formulares enthält das Textfeld mit der ID *message* und zwei Buttons (*Verschlüsseln* und *Senden*). Der Button zum Absenden des Formulares ist beim Laden der Seite deaktiviert. Der Absender muss zuerst den Text verschlüsseln. Dabei wird der erste Button inaktiv und der Buton zum Versenden wird aktiviert.

```
<FORM name="contact" method="post" action="https://server.tld/....">

<textarea id="message" ...></textarea>

<input type="button" onclick="encrypt_message();"
   value="Verschlüsseln" id="encrypt" />

<button type="submit" disabled="true" id="send">Senden</button>

</FORM>
```

5. Außerdem ist der eigenen OpenPGP public Key als versteckter DIV-Container mit der ID *pubkey* irgendwo im HTML-Code einzubauen.

```
<div id="pubkey" hidden="true">
-----BEGIN PGP PUBLIC KEY BLOCK-----
....
-----END PGP PUBLIC KEY BLOCK-----
</div>
```

6. Für Surfer, die JavaScript standardmäßig deaktivieren kann man ein Hinweis einfügen, dass JavaScript für die Funktion des Formulares nötig ist:

```
<NOSCRIPT>
Bitte aktivieren Sie JavaScript für die Verschlüsselung der Nachricht!
</NOSCRIPT>
```

Hinweise: Einige ältere Browser können keine krypto-tauglichen Zufallszahlen mit JavaScript erzeugen. Das kann die Verschlüsselung deutlich schwächen. Deshalb ist es mit diesen Browsern nicht möglich, das Formular zu nutzen. Außerdem kann die Verschlüsselung auf dem Server durch unbemerkte Modifikationen am JavaScript Code angegriffen werden. Trotzdem ist es besser, als keine Verschlüsselung zu verwenden.

8.3.8 OpenPGP Keyserver

Die OpenPGP Keyserver bilden eine Infrastruktur im Web, um öffentliche Schlüssel auch Unbekannten zum Download anzubieten. Die verschiedenen Server synchronisieren ihren Datenbestand. Man kann die Keyserver nach einem passenden Schlüssel durchsuchen.

- Auf der Kommandozeile bzw. DOS-Box kann man nach OpenPGP Schlüsseln anhand der E-Mail Adresse suchen und einen der gefundenen Schlüssel importieren:

  ```
  > gpg2 --search cane@privacy-handbuch.de
  ```

  Wenn man die Key-ID oder den Fingerprint des Schlüssels kennt und weiss, dass der Schlüssel auf einem Keyserver zu finden ist, kann man ihn auch direkt importieren:

  ```
  > gpg2 --recv 0x8F1E7F49912F0D9B73586C908CD51D2D7E36E399
  ```

- In Enigmail findet man die Suchfunktion in der Schlüsselverwaltung unter dem Menüpunkt *Schlüssel-Server -> Schlüssel suchen*.

Keyserver Pool von OpenPGP (mit E-Mail Verifikation)

Der Keyserver Pool https://keys.openpgp.org stellt einen modernen Keyserver für OpenPGP Schlüssel zur Verfügung, der einige Probleme der alten Keyserver wie die des SKS Keyserver Pools vermeidet. Insbesondere werden die E-Mail in den Schlüsseln verifiziert, um das Problem mit Fake Keys (siehe unten) zu lösen. Der Pool ist außerdem auch als Tor Onion Service v3 Adresse erreichbar.

Auf der Webseite kann man seinen eigenen Schlüssel hochladen. Es werden E-Mails mit einer Aufforderung zur Bestätigung an alle Adressen gesendet, die im Schlüssel genannt werden. Die E-Mails enthalten einen Link, den man im Browser öffnen muss, um den Erhalt der E-Mail zu bestätigen. Danach werden die Schlüssel freigeschaltet.

Thunderbird verwendet standardmäßig nur diesen Keyserver, eine Anpassung der Konfiguration ist nicht nötig. Um den Keyserver auch mit dem Programm *gpg2* auf der Kommandozeile zu nutzen, kann man den Keyserver in der Konfigurationsdatei *$HOME/.gnupg/dirmngr.conf* (Linux) bzw. *%APPDATA%/GnuPG/dirmngr.conf* (Windows) konfigurieren und folgende Optionen einfügen:

```
keyserver hkps://keys.openpgp.org
keyserver hkp://zkaan2xfbuxia2wpf7ofnkbz6r5zdbbvxbunvp5g2iebopbfc4iqmbad.onion
```

Wenn genau zwei Keyserver konfiguriert werden und einer davon ein Tor Onion Service ist, dann verwendet GnuPG automatisch den Onion Service, wenn Tor Onion Router läuft.

Nach der Änderung der Konfiguration muss Dirmngr beendet evtl. werden:

```
> gpgconf --kill dirmngr
```

(Zukünftige Versionen von GnuPG werden diesen Keyserver standrdmäßig nutzen.)

Hinweis: dieser Keyserver entfernt aus Sicherheitsgründen alle Signaturen von Dritten aus den hochgeladenen Schlüsseln. Die Verifikation von Schlüsseln anhand der Signaturen (*Web of Trust*) ist also nicht möglich.

Vorsicht bei der Nutzung von veralteten SKS-Keyservern

Man kann auf den Keyservern des SKS Pool u.ä. veralteten Servern nach Schlüsseln anhand E-Mail Adressen, 8-stellige oder 16-stellige Key IDs oder bekannten Fingerprints suchen.

1. Wenn man nach der E-Mail Adresse sucht, dann werden unter Umständen mehrere Schlüssel zum Importieren angeboten. Es gibt immer wieder Witzbolde, die Schlüssel für fremde E-Mail Adressen auf den Keyservern hochladen (um zu stänkern?).

   Wenn man zum Beispiel den Schlüssel von Felix v. Leitner (Fefe) sucht, dann findet man fünf Schlüssel. Aber nur der Schlüssel von Okt. 2013 ist korrekt (nicht der neueste Schlüssel!), wie Fefe in seinem Blog schreibt.[15]

Abbildung 8.8: Fünf OpenPGP-Schlüssel für eine E-Mail Adresse

   J. Schmidt von Heise.de beklagt, dass ein Scherzkeks OpenPGP Schlüssel für seine E-Mail Adresse auf die Keyserver hochgeladen hat und dass er damit verschlüsselten E-Mails nicht lesen kann (Editorial c't 6/2015).

   Erinn Clark signierte die Downloads des TorBrowserBundle. Für ihre E-Mail Adresse wurden Fake Schlüssel auf den Keyserver publiziert.[16]

   Gavin Andresen signierte die Bitcoin Binaries, für seine E-Mail Adresse wurden ebenfalls Fake Schlüssel auf den Keyserver publiziert.[17]

2. Statt E-Mail Adressen kann man auch nach der 8-stelligen Key-ID suchen (zB. 0xA534A9C6). Diese Methode liefert besser Ergebnisse, allerdings muss man die richtige Key-ID kennen. Auch diese Methode ist nicht sicher, da man diese Key-IDs ebenfalls faken kann, wie ein Forscherteam demonstrierte.[18]

3. Die 16-stellige Key-ID (zB. 0xFC32CEECA534A9C6) ist schwieriger zu faken, aber auch nicht als kryptografisch sichere ID entworfen.

4. Am besten ist es, wenn man den gesuchten Schlüssel anhand des Fingerprint sucht (zB. 0x68995C53D2CEE11B0E4182F62146D0CD2B3CAA3E). Diese Suche liefert als einzige Variante vertrauenswürdige Ergebnisse.

8.3.9 Web des Vertrauens (WoT)

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

Hat Beatrice die Echtheit des Schlüssels von Conrad überprüft, kann sie diesen mit ihrem geheimen Schlüssel signieren und der Community zur Verfügung stellen oder direkt an Anton schicken. Anton, der den Schlüssel von Beatrice bereits überprüft hat und(!) Beatrice als *vertrauenswürdige Person* definiert, kann damit aufgrund der Signatur auch dem Schlüssel von Conrad vertrauen. Es bildet sich ein kleines Netz von Vertrauensbeziehungen. Die Grafik 8.9 zeigt eine mögliche Variante für den Key von Anton (A).

- Anton (A) vertraut dem Schlüssel von Conrad (C), weil er von Beatrice (B) unterschrieben wurde und Beatrice für Anton eine vertrauenswürdige Person ist.

[15] https://blog.fefe.de/?ts=aa27d652
[16] https://lists.torproject.org/pipermail/tor-talk/2014-March/032308.html
[17] http://gavintech.blogspot.ch/2014/03/it-aint-me-ive-got-pgp-imposter.html
[18] http://heise.de/-2473281

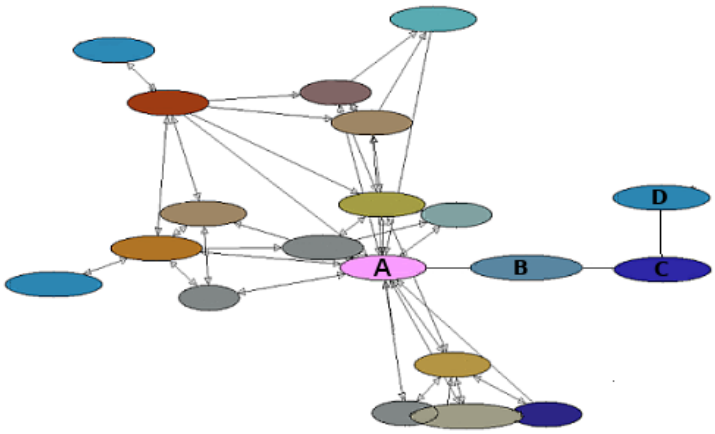


Abbildung 8.9: Beispiel für ein Web of Trust

- Anton (A) vertraut dem Schlüssel von Doris (D) nicht, obwohl er von Conrad unterschrieben wurde und der Schlüssel Conrad durch die Signatur von Beatrice als vertrauenswürdig gilt.

Warum vertraut Anton (A) dem Schlüssel von Doris (D) nicht automatisch? Weil er Conrad (C) nicht kennt und ihn daher nicht als *vertrauenswürdige Person* definiert hat!

Es bildet sich also kein weltweites Vertrauensnetz automatisch, indem man irgendwelche Schlüssel irgendwie unterschreibt und dann verteilt! Das Web of Trust funktioniert nur in einer kleinen Umgebung, weil zwei(!) Bedingungen erfüllt sein müssen. Neben einer digitalen Signaturkette muss auch jeder unterschreibender Nutzer in der Kette als *vertrauenswürdige Person* gekennzeichnet sein. Das geht nur, wenn man die Personen kennt.

Hinweis: Aktuelle GnuPG Versionen importieren keine Signaturen von Dritten, wenn man sich einen PGP Schlüssel von einem Keyserver holt, und moderne Keyserver wie der Pool von OpenPGP.org stellen auch keine Signaturen von Dritten mehr bereit. Thunderbird unterstützt das Signieren von Schlüsseln ebenfalls nicht mehr. **Das WoT ist praktisch tot.**

Das Web of Trust funktioniert nur in Ausnahmefällen, wenn man die Schlüssel direkt untereinander austauscht oder auf einer Webseite zum Download bereitstellt.

Certification Authorities

Diese Infrastruktur kann auch von vertrauenswürdigen Institutionen (Certification Authorities, CAs) genutzt werden. Die Nutzer wenden sich an die CA und lassen gegen Vorlage von Ausweisdokumenten den eigenen OpenPGP-Key signieren. Alle Partner benötigen lediglich den öffentlichen Schlüssel der CA, um die Echtheit der Schlüssel zu überprüfen.

In einer Gruppe kann eine vertrauenswürdige Person diese Rolle übernehmen. Alle Mitglieder eines Vereins oder Arbeitsgruppe oder Mitarbeiter einer Firma senden ihre OpenPGP Schlüssel an diese Person, die Schlüssel werden überprüft und signiert und an zentraler Stelle zum Download bereitgestellt. Die Mitglieder der Gruppe müssen nur den Schlüssel der Vertrauebsperson überprüfen, signieren und die Vertrauenswürdigkeit des Inhaber setzen. Dann kann die Gruppe mit verifizierten Schlüsseln kommunizieren.

Weitere Beispiele für Certification Authorities sind:

- CAcert.org signiert auch OpenPGP-Schlüssel
- Krypto-Kampagne der Zeitschrift c't

- PCA des Deutschen Forschungsnetzes (DFN-PCA)

8.4 Verschlüsselte Dokumente per E-Mail senden

Manchmal möchte man eine vertrauliche E-Mail an einen Kommunikationspartner schreiben, der keine Ahnung von E-Mail Verschlüsselung hat. Oder man möchte nicht, das Schnüffelprogramme von Google, Yahoo! oder Microsoft die Mail lesen.

Als Alternative zur E-Mail Verschlüsselung könnte man den Inhalt der Mail in ein verschlüsseltes Dokument packen und dieses Dokument als Anhang mit der Mail versenden. **LibreOffice** Dokumente werden mit AES256 verschlüsselt, wenn man beim Speichern des Dokumentes die Option *Mit Kennwort speichern* aktiviert. Außerdem kann LibreOffice Dokumente mit OpenPGP verschlüsselt speichern (Abb. 13.1).

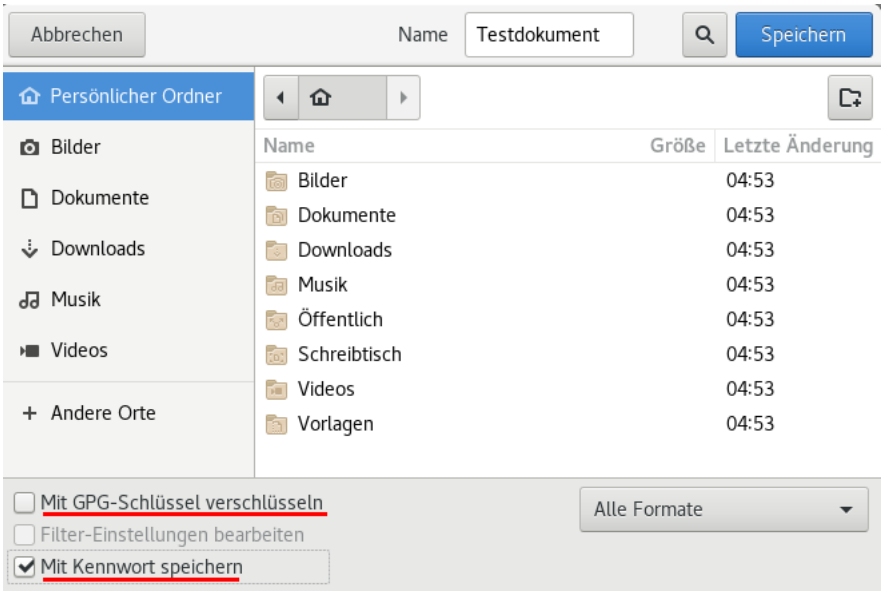


Abbildung 8.10: Verschlüsselte Speicherung in LibreOffice aktivieren

Wenn man keine OpenPGP Schlüssel verwendet sondern ein Kennwort, dann muss man dem Empfänger das Kennwort zu Öffnen der Datei über einen sicheren 2. Kanal mitteilen oder man schreibt im Text der E-Mail eine Andeutung, die nur der Empfänger interpretieren kann:

Das Passwort ist der Name der Bar, in der wir neulich ein Bier getrunken haben.

Man muss nicht für jede Nachricht ein neues Passwort definieren, man kann ein einmal sicher ausgetauschte Passwort natürlich auch über einen längeren Zeitraum verwenden. Das ist sicherer, als immer wieder unsichere Methoden für den Passworttausch zu nutzen.

8.5 Eine Bemerkung zum Abschluß

"Mache ich mich verdächtig, wenn ich meine E-Mails verschlüssel?"

Eine Frage, die häufig gestellt wird, wenn es um verschlüsselte E-Mails geht. Bisher gab es darauf folgende Antwort:

"Man sieht es einer E-Mail nicht an, ob sie verschlüsselt ist oder nicht. Wer befürchtet, dass jemand die Mail beschnüffelt und feststellen könnte, dass sie verschlüsselt ist, hat einen Grund mehr, kryptografische Verfahren zu nutzen!"

Aktuelle Ereignisse zeigen, dass diese Frage nicht mehr so einfach beantwortet werden kann. Dem promovierten Soziologen Andrej H. wurde vorgeworfen, Mitglied einer terroristischen Vereinigung nach §129a StGB zu sein. Der Haftbefehl gegen ihn wurde unter anderem mit **konspirativem Verhalten** begründet, da er seine E-Mails verschlüsselte.

Am 21.Mai 2008 wurden in Österreich die Wohnungen von Aktivisten der Tierrechtsszene durchsucht und 10 Personen festgenommen. Der Haftbefehl wurde mit Verdunklungsgefahr begründet, da die Betroffenen z.B. über verschlüsselte E-Mails kommunizierten.

Am 18.10.07 hat der Bundesgerichtshof (BGH) in seinem Urteil Az.: StB 34/07 den Haftbefehl gegen Andrej H. aufgehoben und eindeutig festgestellt, dass die Verschlüsselung von E-Mails als Tatverdacht NICHT ausreichend ist, entscheidend sei der Inhalt:

"Ohne eine Entschlüsselung der in den Nachrichten verwendeten Tarnbegriffe und ohne Kenntnis dessen, was bei den - teilweise observierten und auch abgehörten - Treffen zwischen dem Beschuldigten und L. besprochen wurde, wird hierdurch eine mitgliedschaftliche Einbindung des Beschuldigten in die 'militante gruppe' jedoch nicht hinreichend belegt."

Außerdem geben die Richter des 3. Strafsenat des BGH zu bedenken, dass Andrej H. *"ersichtlich um seine Überwachung durch die Ermittlungsbehörden wusste"*. Schon allein deshalb konnte er *"ganz allgemein Anlass sehen"*, seine Aktivitäten zu verheimlichen. Woher Andrej H. von der Überwachung wusste, steht bei http://annalist.noblogs.org.

Trotz dieses Urteils des BGH bleibt für uns ein bitterer Nachgeschmack über die Arbeit unser Ermittler und einiger Richter. Zumindest die Ermittlungsrichter sind der Argumentation der Staatsanwaltschaft gefolgt und haben dem Haftbefehl erst einmal zugestimmt.

Kapitel 9

Instant Messaging und Telefonie

Instant Messaging und verschlüsselte Audio- und Videotelefonie wachsen immer mehr zusammen. Typische Messenger kann man auch für verschlüsselte Telefonie nutzen und Telefonie Anwendungen können auch kurze Nachrichten und Dateien austauschen.

1. Messenger Apps bieten neben 1:1 Chats und Dateitransfer auch Gruppenchats, Abstimmungstools und andere Social Features für textbasierte Kommunikation. Audiotelefonie ist inzwischen häufig enthalten, Videotelefonie gibt es öfters.

   Die sogenannten Kanäle/Channels bieten eine Top-Down Kommunikation (der Boss spricht und Abonnenten dürfen lauschen). Außerdem unterscheiden sie sich von Gruppenchats darin, dass die Anzahl der Mitglieder unbegrenzt ist und dass ein Mitglied/Abonnent andere Mitglieder nicht sehen kann (Privatsphäre).

2. Telefonie Apps wurden in erster Linie für verschlüsselte Audio- und Videotelefonie entwickelt. Als Zusatzfeature gibt es auch die Versendung von Nachrichten und Dateien aber in der Regel keine Gruppenchats und keine Kommunikation in Gruppen.

3. Videokonferenz Systeme können in der Regel einfach mit einem Webbrowser genutzt werden, für Smartphones sind Apps verfügbar. In den Videokonferenzen kann man die Kamera abschalten und nur via Audio Talk teilnehmen, es gibt eine Screen Sharing Funktion und man kann einzelnen Teilnehmern Nachrichten schicken.

Messenger mit verschlüsselter Audio- und Videotelefonie

Messenger werden primär auf dem Smartphone genutzt, denn die Erreichbarkeit ist eine wesentliche Voraussetzung für ÏnstantMMessaging. Desktop Clients sind in der Regel auch vorhanden, aber manchmal nur als Zusatzoption zur Smartphone App.

Threema ist einer der sichersten Messenger und hat eine 7-stellige Nutzerbasis. Im Unterschied zu einigen anderen Messengern wird nicht die Telefonnummer als individuelle Kennung verwendet sondern eine zufällig Buchstabenkombination. Neben Messaging Funktionen gibt es auch verschlüsselte Audio- und Videotelefonie.

Signal App ist kostenlos nutzbar, weil das Projekt durch großzügige Spenden von reichen Mäzenen finanziert wird. Der Messenger ist intuitiv bedienbar, hat inzwischen eine 9-stellige Nutzerbasis und ist führend bei Sicherheit und Privatsphäre. Signal App verwendet die Telefonnummer als Kennung für den Account und man benötigt ein Smartphone. Die Software ist Open Source aber die Infrastrukur ist zentralisiert.

Signal App kann man für die private Kommunikation mit Bekannten und Freunden nutzen, die nicht IT-affin sind und denen man bedenkenlos die eigene Telefonnummer geben kann. Neben Chats und Gruppenchats gibt es verschlüsselte Audio- und Videotelefonie und Videokonferenzen mit bis zu 5 Teilnehmern sind möglich.

Telegram bietet viele Social Features und ist als zensurresistente Twitter Alternative mit Black Market Features populär geworden (z. B. bei Protesten in Hongkong und Belarus 2020) aber als Messenger für vertrauliche Kommunikation eher ungeeignet.

Jabber/XMPP, matrix sind ebenfalls kostenlos und Open Source. Im Gegensatz zu Threema, Signal App oder Telegram wird die förderale Infrastruktur von Enthusiasten betrieben. Jeder, der sich dazu in der Lage fühlt, kann eigene Server betreiben. Die Kennung für einen Account ist unabhägig von einer Telefonnummer frei wählbar und man kann einen oder mehrere Accounts in beliebigen Kombinationen auf mehreren PCs oder Smartphones nutzen. [matrix] bietet neben Chats und flexibel konfigurierbaren Gruppenchats auch verschlüsselte Audio- und Videotelefonie.

Ein Hauptziel von [matrix] und Jabber/XMPP ist es, eine förderale Infrastrutur ähnlich wie bei E-Mail zu schaffen, die mit beliebigen Clients genutzt werden kann. Während [matrix] expandiert, verliert Jabber/XMPP kontinuierlich an Bedeutung.

Community-basierte Entwicklung und förderale Infrastruktur erschweren die Einführung und Umsetzung von Sicherheitsfeatures. M. Marlspike hat diese Phänomene als systemimmanent für diese Kategorie von Open Source Projekten beschrieben.[1]

Der **bwmessenger** ist ein Fork für den Einsatz von [matrix] in der Bundeswehr. Für die Nutzung des *bwmessenger* gelten in der Bundeswehr die gleichen Regeln[2], wie für unverschlüsselte E-Mail und Telefonie:

- Auf Standdardgeräten (Smartphones, Laptops, PCs) darf der bwmessenger in der Bundeswehr nur für offen eingestufte Kommunikation verwendet werden.
- Auf dienstlichen SMK-Geräten, die für **S**ichere **M**obile **K**ommunikation geeignet sind (SINA Laptops, SecuSUITE Smartphones), darf der bwmessenger genau wie unverschlüsselte E-Mails auch für VS-NfD Kommunikation genutzt werden, da die SMK-Plattform die kryptografische Sicherheit gewährleistet.

Briar (nur für Android) ist ein Messenger für hohe Sicherheitsanforderungen. Die Kommunikation und Speicherung ist vollständig verschlüsselt. Es werden keine zentralen Server genutzt sondern Peer-2-Peer Kommunikation via Tor Onion Router oder direkt via WLAN/Bluetooth, wenn kein Internet verfügbar ist.

Kontakte können nur bei einem persönlichen Treffen (Face-2-Face) hinzugefügt werden, indem man gegenseitig die QR-Codes scannt. Nur so ist nach Meinung der Entwickler sichergestellt, dass man wirklich mit der gewünschten Person kommuniziert.

Einen idealen Messenger, der alle Bedingungen erfüllt, gibt es nicht. Man muss abwägen, welche Schwerpunkte man bei seinen Anforderungen setzt. Um viele Kontakte zu erreichen, könnte man mehrere Messenger parallel verwenden.

Apps für verschlüsselte Audio- und Videotelefonie

Anwendungen für verschlüsselte Telefonie konnten sich in den letzten 10 Jahren im privaten Bereich nicht großflächig etablieren, obwohl die technischen Vorraussetzungen seit 2011 mit der Standardisierung des SRTP/ZRTP Protokolls vorhanden gewesen wären. Aktuell bieten Messenger (siehe oben) eine einfach nutzbare Möglichkeit für verschlüsselte Audio- und Videotelefonie und machen die Installation zusätzlicher SIP Clients mit ZRTP Verschlüsselung im privaten Bereich eigentlich überflüssig.

Jami ist eine Open Source App für verschlüsselte Telefonie, die weitestgehend ohne zentrale Server auskommt. Es wird eine Distributed Hash Table (DHT) zum Aufbau der Verbindung zwischen Clients verwendet Die Kommunikation läuft direkt zwischen den Clients. In einigen speziellen Fällen kommen zentrale Server zum Einsatz.

Wie andere Anwendungen, die Daten über eine DHT verteilen, sollten Jami aus dem Internet erreichbar sein. Anderenfalls kommt es zu zeitverzögerten, unregelmäßigen Zustellung von Nachrichten und verpassten Anrufen. Die Entwickler empfehlen, UPnP auf dem Router zu aktivieren und die Firewall abzuschalten, damit Jami das Portforwarding auf dem Router automatisch konfigurieren kann und erreichbar ist.

[1] https://www.signal.org/blog/the-ecosystem-is-moving
[2] https://www.presseportal.de/pm/76712/4764023

Hinweis: Das BSI, das FBI oder die US Homeland Security empfehlen ausdrücklich die Deaktivierung von UPnP zur Vermeidung von Sicherheitsrisiken! Wenn man diesen Empfehlungen folgt, wird man mit Jami im P2P Modus nicht glücklich.[3] [4] [5]

Linphone ist ein Open Source VoIP Client für Smartphones und PCs. Wie bei VoIP üblich werden die Accounts auf förderal organisierten SIP-Servern verwaltet. Die Kommunikation erfolgt direkt zwischen den Clients oder über einen TURN-Server, wenn keine direkte Verbindung möglich ist. Als Besonderheit bietet Linphone verschlüsselte Audio Konferenzen. Die Verschlüsselung der Audio- und Videokommunikation erfolgt mit SRTP/ZRTP.

Hinweis: VoIP Clients, die das SIP Protokoll nutzen, müssen ebenfalls aus dem Internet erreichbar sein, damit der SIP Server den Client bei Anrufen kontaktieren und die Verbindung vermitteln kann. Die Konfiguration von Router und Firewall ist machbar, für Nicht-ITler aber nicht ganz trivial. Deshalb konnte sich verschlüsselte VoIP Telefonie in den letzten 20 Jahren im privaten Bereich nicht in der Breite durchsetzen.

Simlar.org ist ein deutsches Open Source Projekt für verschlüsselte VoIP Telefonie. Der Source Code für Clients und Server ist bei Github zu finden. Die Verschlüsselung der Kommunikation erfolgt mit SRTP/ZRTP. Die SIP-Server stehen in Deutschland.

Es gibt Apps für Android und iPhone. Im F-Droid Store gibt es eine Google-freie Version. Diese Version muss ständig laufen und sollte nicht beendet werden, wenn man Anrufe annehmen will, da die Google Push Services nicht verwendet werden.

Tox ist ein offenes Protokoll für verschlüsselte Telefonie und Chats. Die Kommunikation läuft direkt von Client zu Client. Es gibt keine zentralen Server und keinen Provider, der Kommunikationsprofile erstellen könnte. Tox ist ein Protokoll, das für hohe Sicherheitsansprüche und Anonymität entwickelt wurde.

Lösungen für Videokonferenzen

Kommerzielle Lösungen für Videokonferenzen wie Microsoft Teams, Zoom oder Slack sind nicht DSGVO-konform. Es gibt Alternativen, die man selbst betreiben kann:

Jitsi Meet ist eine Open Source Software für den eigenen Konferenzserver. M. Kuketz hat eine Anleitung[6] für die Nutzung von Jitsi Meet geschrieben und betreibt selbst einen Jitsi Meet Server. Weitere Server in DE, die von Freifunk Gruppen, Golem.de oder L. Neumann betrieben werden, findet man in dieser Liste auf Github.[7]

Nextcloud Talk ist eine weitere Open Source Lösung für Videokonferenzen.

Für die Teilnahme an einer Videokonferenz benötigt man nur den Link zur Webkonferenz, evtl. das Passwort und einen Webbrowser, der nicht zu restriktiv konfiguriert ist. Die Verwendung von WebRTC und Javascript muss möglich sein und das OpenH264 Plugin muss aktiviert worden sein. Um Firefox etwas zu zähmen, könnte man die *minimale user.js* aus dem Kapitel *Spurenarm Surfen* verwenden.

Bevor man sich mit vollem Elan in die Videokonferenz stürzt, kann man mit dem **WebRTC Test**[8] prüfen, ob Kamera, Mikrofon und Verbindungsaufbau korrekt funktionieren.

Eine durchgehende Ende-zu-Ende Verschlüsselung gibt es bei Videokonferenzen nicht. In der Regel könnte der Server Betreiber die Konferenzen beobachten. Man kann den Server selbst aufsetzen oder eine vertrauenswürdigen Betreiber wählen.

[3] https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/basisschutz_fuer_den_router.html
[4] https://www.howtogeek.com/122487/htg-explains-is-upnp-a-security-risk/
[5] https://www.zdnet.com/article/homeland-security-disable-upnp-as-tens-of-millions-at-risk/
[6] https://www.kuketz-blog.de/kurzanleitung-jitsi-meet-videokonferenz-per-browser-oder-app/
[7] https://github.com/jitsi/jitsi-meet/wiki/Jitsi-Meet-Instances
[8] https://test.webrtc.org/

Kommerzielle Angebote für Unternehmen

GSMK Cryptophones bieten einen ganzheitliches Sicherheitskonzept und High End Security. Sie sind aber auch mit 2.000+ Euro entsprechend teuer.

Silent Circle bietet mobile, verschlüsselte Kommunikation für Unternehmen, NGOs und Regierungen mit Enterprise Features wie Verwaltung der Nutzer und Geräte.

SecuSUITE for Samsung Knox ist derzeit die bevorzugte Lösung für sichere, mobile Kommunikation in deutschen Bundesbehörden, vom BSI für VS-NfD zugelassen.

Mobile Encryption App der Telekom addressiert Unternehmen und Behörden, die sich etwas preiswerter gegen Spionage durch starke (ausländische) Angreifer schützen wollen. Die App verschlüsselt Telefonie nach dem GSMK-Protokoll.

Die App verwendet ein eigenes verschlüsseltes Adressbuch und bietet einen sicheren Speicher für Notizen. Sie kann auch ohne SIM Karte genutzt werden, da die Teilnehmer über individuelle +800 Telefonnummern addressiert werden. Die Infrastruktur wird von der Deutschen Telekom in deutschen Rechenszentren betrieben. Im Sept. 2019 wurde die iOS Version vom BSI für VS-NfD zugelassen. Die Freigabe der Android Version für VS-NfD ist für 2020 geplant. Mit Kosten von 10-20 Euro pro Person ist die Mobile Encryption App für Unternehmen mit hohen Sicherheitsanforderungen eine preiswerte Alternative zu GSMK Kryptophones.

9.1 Verschlüsselte Telefonie

Für verschlüsselte Telefonie gibt es mehrere Protokolle:

- SRTP/ZRTP von Phil Zimmermann kümmert sich um die Verschlüsselung des Datenstroms bei Audio- und Videotelefonie. Die Ende-zu-Ende Verschlüsselung des Datenstroms erfolgt mit SRTP, den automatischen Schlüsseltausch erledigt ZRTP und die Verifizierung erfolgt mit SAS. Die Verbindung zwischen den Clients kann entweder via SIP Protokoll aufgebaut werden oder auch über andere Protokolle.

- WebRTC wurde maßgeblich von Google und Mozilla initiiert, um der Konkurrenz von Microsoft Skype etwas entgegen zu setzen. Es wurde vom W3C standardisiert und ist seit 2017 in allen Browsern enthalten. Es wird aber auch in einigen Messengern für verschlüsselte Audiotelefonie verwendet.

  Der Datenstrom wird bei WebRTC ebenfalls mit SRTP verschlüsselt. Die Verwaltung der Accounts erfolgt auf zentralen Servern aber die Sprachkommunikation läuft über eine direkte Verbindung zwischen den Clients. Für den Aufbau der Verbindung kann ICE (Internet Connectivity Establishment) genutzt werden. Wenn keine direkte Verbindung zwischen den Clients möglich ist, werden TURN Server als Proxys genutzt.

- Das GSMK-Protokoll verschlüsselt den Datenstrom doppelt mit AES256 und Twofish. Die niedrige, feste Datenrate von 4,8 kBit/s soll eine Kommunikation auch dann ermöglichen, wenn verschlüsselte VoIP Telefonie mittels DPI blockiert wird, wie es beispw. in einigen Gebieten von Frankreich, in VAE oder Saudi Arabien üblich ist.

Verschiedene Forschungsergebnisse wie *Language Identification in Ecrypted VoIP Traffic* (2007), *Recovering Spoken Phrases in Encrypted VoIP Conversation* (2008) und *Phonotatic Reconstruction of Encrypted VoIP Conversations* (2011) zeigen, dass es bei der Verschlüsselung von Telefonie Angriffsmöglichkeiten gibt, um gesprochene Phrasen anhand der variierenden Datenrate aus dem verschlüsselten Datenstrom zu rekonstruieren ohne die Verschlüsselung knacken zu müssen. Deshalb wird für hohe Sicherheitsanforderungen die Verwendung einer feste Datenrate empfohlen. Diese Technik ist auch bei den Geheimdiensten seit mehreren Jahren im Einsatz.

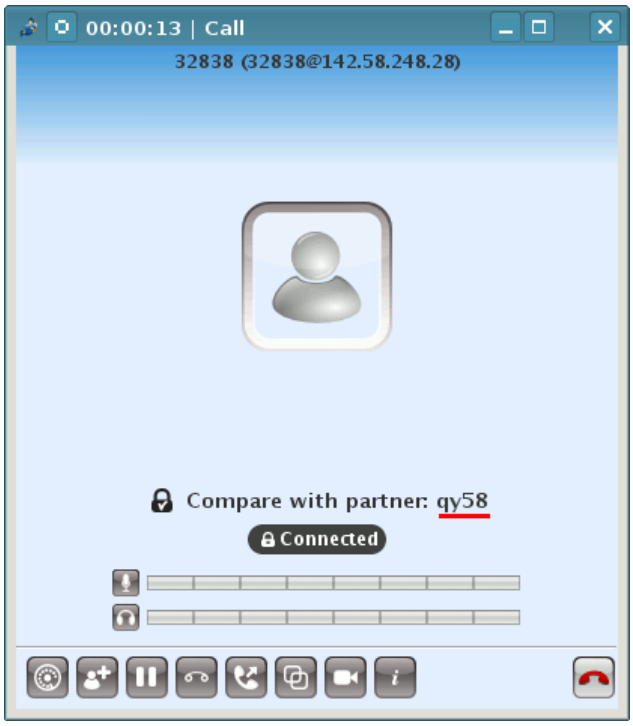


Abbildung 9.1: SAS Authentication bei Jitsi als Beispiel

9.1.1 SRTP/ZRTP Verschlüsselung

Das SRTP/ZRTP-Protokoll[9] von Phil Zimmermann (Erfinder von PGP) spielt eine zentrale Rolle bei verschlüsselter Telefonie. Es gewährleistet eine sichere Ende-zu-Ende-Verschlüsselung der Sprachkommunikation. Wenn beide Kommunikationspartner eine Software verwenden, die das ZRPT-Protokoll beherrscht, wird die Verschlüsselung automatisch ausgehandelt. Kurze Erläuterung der Begriffe:

SRTP definiert die Verschlüsselung des Sprachkanals. Die Verschlüsselung der Daten erfolgt symmetrische mit AES128/256 oder Twofish128/256. Für die Verschlüsselung wird ein gemeinsamer Schlüssel benötigt, der zuerst via ZRTP ausgehandelt wird.

ZRTP erledigt den Schlüsselaustausch für SRTP und nutzt dafür das Diffie-Helman Verfahren. Wenn beide VoIP-Clients ZRTP beherrschen, wird beim Aufbau der Verbindung ein Schlüssel für SRTP automatisch ausgehandelt und verwendet. Der Vorgang ist transparent und erfordert keine Aktionen der Nutzer. Allerdings könnte sich ein Man-in-the-Middle einschleichen, und die Verbindung kompromittieren (Belauschen).

SAS dient dem Schutz gegen Man-in-the-Middle Angriffe auf ZRTP. Den beiden Kommunikationspartnern wird eine 4-stellige Zeichenfolge angezeigt, die über den Sprachkanal zu verifizieren ist. Üblicherweise nennt der Anrufer die ersten beiden Buchstaben und der Angerufenen die beiden letzten Buchstaben. Wenn die Zeichenfolge identisch ist, kann man davon ausgehen, dass kein Man-in-the-Middle das Gespräch belauschen kann.

9.1.2 Verschlüsselt chatten und telefonieren mit qTox

Tox ist ein Protokoll für verschlüsselte Telefonie und Chats. Die Kommunikation läuft direkt von Client zu Client. Die Teilnehmer finden sich gegenseitig über eine Distributed

[9] https://tools.ietf.org/html/draft-zimmermann-avt-zrtp-22

Hash Table (DHT). Es gibt keinen Provider, der Kommunikationsprofile erstellen könnte oder zur Implementierung von Backdoors für Behörden gezwungen werden könnte.

Tox verwendet für die Krypto nicht die üblichen, vom NIST standartisierten Verfahren sondern Verfahren von D.J. Bernstein. Der ECDHE Schlüsseltausch nutzt curve25519, statt AES wird XSALSA20 verwendet und statt SHA256 kommt POLY1350 zum Einsatz.

Es gibt mehrere Clients, die das Protokoll beherrschen. Für PCs und Laptops eignet sich **qTox** am besten. Für Android gibt es **Antox** (im Google Playstore) und den **TRIfA Tox Client** im F-Doid-Store und Playstore. Für iPhones gibt es keinen Tox Client.

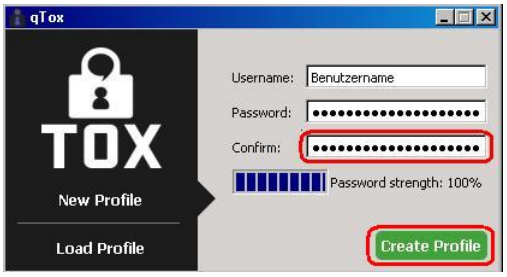
Bei Smartphones ist zu beachten, dass die Call History (Liste aller Anrufe) an Google übertragen wird, wenn die App die Anrufe auf dem Sperrbildschirm anzeigen kann. Dort werden die Daten für 4-6 Monate gespeichert (private Vorratsdatenspeicherung bei NSA PRISM Partnern). Geheimdienste haben Zugriff auf diese Daten und die Firma Elcomsoft liefert die nötigen Tools für die Auswertung. Die Datenspeicherung lässt sich deaktivieren, indem man die Nutzung der Google Cloud Services komplett deaktiviert.

Installation von qTox

Windows: auf der Downloadseite steht eine Setup Datei zur Verfügung. Nach dem Download muss man das Ausführen der Setup-Datei zulassen, da die Datei aus dem Internet stammt und die Ausführung deshalb möglicherweise blockiert wird. Dafür klickt man mit der rechten Maustaste auf die Datei und wählt den Menüpunkt *Eigenschaften*. Danach startet man das Setup mit einem Rechtsklick auf die Datei, wählt den Menüpunkt *Als Administrator ausführen* und folgt dem Installationsassitenten.

Account erstellen

qTox lässt sich mit Klick auf das Programmsymbol starten. Es öffnet sich sich das Profilmenü. Hier hat man die Wahl, ein bereits bestehendes Profil zu laden (*LoadProfile*) oder ein neues Profil anzulegen. Zunächst wählt man den Benutzernamen und das Passwort.



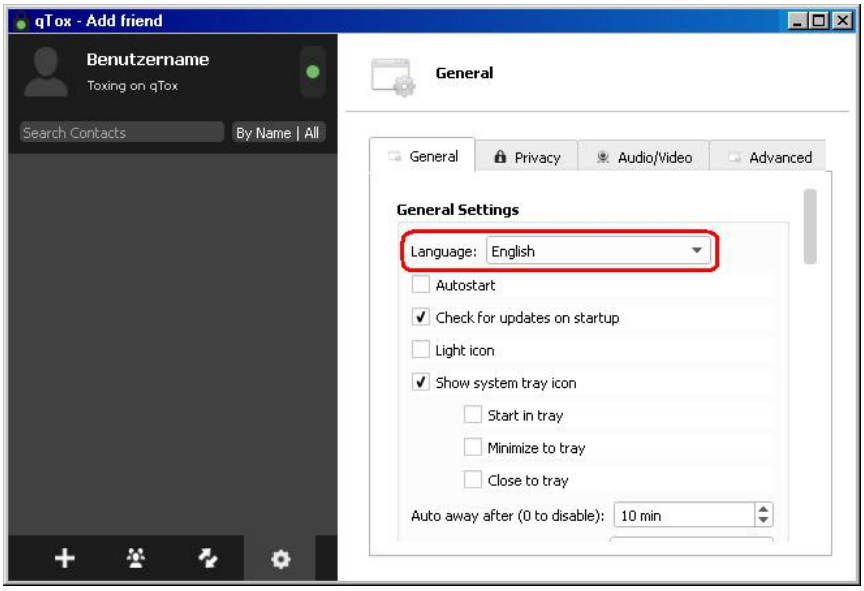
Es sollte ein starkes Passwort gewählt werden - je größer die Basis der möglichen Zeichen (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen), je zufälliger diese Zeichen gewürfelt werden und je mehr Stellen das Passwort hat, desto stärker das Passwort.

Konfiguration von qTox

Im Hauptmenü wählt man in den Einstellungen, die man jederzeit durch Klick auf das Zahnrädchen erreicht, zunächst die Registerkarte *General*. Bei *Language* lässt sich die Sprache umstellen ind man auf *English* klickt und die Sprache *Deutsch* wählen.

Hier lässt sich nun auch einstellen, ob man qTox bei jedem Systemstart mitstarten lassen möchte, ob man regelmäßig nach Updates suchen möchte, ob in der Systemleiste ein Icon angezeigt werden soll, ob qTox bei Programmstart zunächst nur in diesem Icon oder mit einem Fenster starten soll, ob qTox beim Minimieren in die Systemleiste statt in die Taskleiste minimiert werden soll, ob bzw. nach welcher Zeit der Abwesenheit qTox den

Status *Abwesend* anzeigen soll und ob geteilte Dateien automatisch angenommen werden sollen. Aus Sicherheitsgründen sollten Dateien nie automatisch angenommen werden!



Auf der Registerkarte *Privatsphäre* kann man die Speicherung des Chat-Verlaufes deaktivieren. Die Speicherung verschlüsselter Chats ist als Mannings-Bug bekannt geworden. Außerdem kann man die Schreibbenachrichtigungen für Chats deaktivieren.

Auf der Registerkarte *Audio/Video* kann man die Audio- und Videoeinstellungen konfigurieren und testen.

Auf der Registerkarte *Erweitert* kann man qTox in eine portable Programmversion umwandeln, die man auf dem USB-Stick mitnehmen kann.

Kontakt aufnehmen

Wenn Anton und Beatrice Tox für die Kommunikation nutzen wollen, müssen sie die Tox-ID austauschen. Das könnte in folgenden Schritten ablaufen:

1. Anton schickt seine Tox-ID oder ToxMe-Adresse irgendwie an Beatrice.

2. Beatrice sendet eine Freundschaftsanfrage an diese Tox-ID.

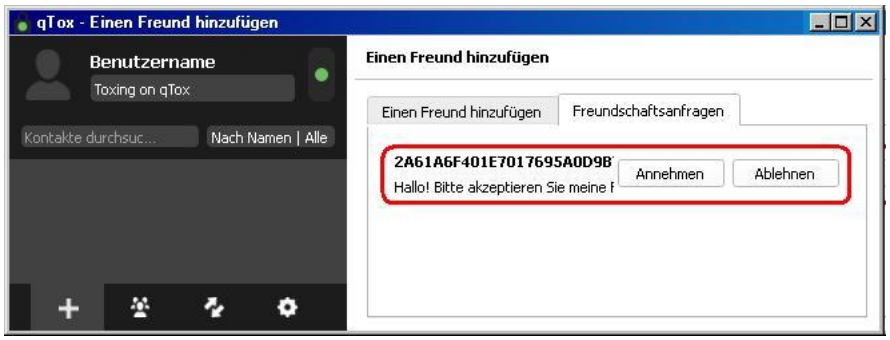
3. Anton akzeptiert die Freundschaftsanfrage von Beatrice.

Um eine Freundschaftsanfrage zu senden, benötigt man die 72-stellige Tox-ID des Kontakts oder eine ToxMe-ID, die über einen sicheren Kanal ausgetauscht werden muss. Die eigene Tox-ID findet man, wenn man sich das eigene Profil anzeigen lässt. Dort könnte man auch eine ToxMe-ID auf einem öffentlichen Server erstellen.

Eine ToxMe-ID ist wie einen E-Mail Adresse aufgebaut und damit leichter zu verstehen und fehlerfreier zu übertragen. Anhand dieser ToxMe Adresse kann qTox die 72-stellige ID des Kontakts auf einem ToxMe-Server finden (z. B von ToxMe.io). Die ToxMe-Server sind also mit einem Telefonbuch vergleichbar und dienen nur der Vereinfachung des Austausches der Adressen.

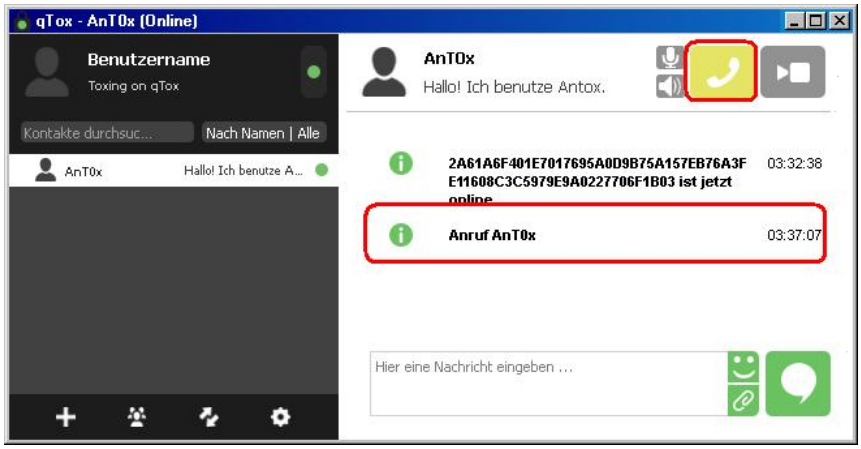
Zusammen mit der Freundschaftsanfrage wird eine Nachricht gesendet. Anhand dieser Nachricht kann der Empfänger den Anfragenden erkennen.

Erhält man eine Freundschaftsanfrage eines anderen Benutzers, so wird oben links im Programmfenster ein grünes Feld mit der Aufschrift *1 neue Freundschaftsanfrage* angezeigt. Durch Klick auf diese grüne Schaltfläche werden weitere Infos zur Freundschaftsanfrage angezeigt - etwa die ID, eventuell auch den Benutzernamen und/oder einen Begrüßungstext. Man hat nun die Wahl die Freundschaftsanfrage anzunehmen oder abzulehnen. Mit der Annahme der Freundschaftsanfrage werden die nötigen Krypto-Schlüssel ausgetauscht, die für die verschlüsselte Kommunikation benötigt werden.

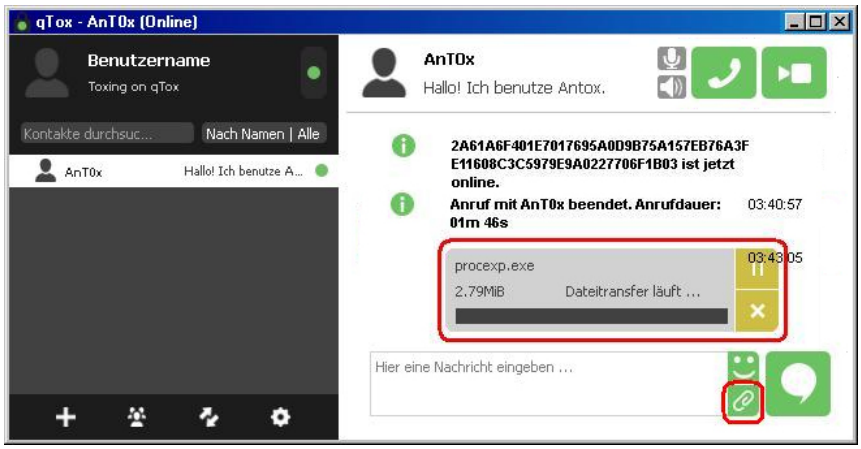


Kontakte anrufen, Dateien schicken oder chatten

Wenn man auf das Profil eines Kontakts klickt, hat man viele Möglichkeiten. Man kann telefonieren und per Video schnattern (Buttons oben rechts)...



...oder chatten und Dateien verschicken (Buttons untern rechts).



9.1.3 Skype???

Der bekannteste Anbieter für Internettelefonie (Voice over IP, VoIP) ist zweifellos **Skype**. Die Installation und das Anlegen eines Account ist einfach. Man benötigt lediglich eine E-Mail Adresse. Skype-Verbindungen sind schwer zu blockieren. Die Client-Software findet fast immer eine Verbindung zum Netz, auch hinter restriktiven Firewalls. Skype bot eine gute Verschlüsselung und kann Verbindungen ins Festnetz herstellen.

Nach der Übernahme von Skype durch Microsoft wurde die zensur-robuste Infrastruktur von Skype umgebaut und die Ende-zu-Ende Verschlüsselung von Skype kompromittiert. Statt einer Peer-to-Peer Infrastruktur nutzt Skype jetzt sogenannte Super-Nodes, die alle in Microsoft Rechenzentren stehen. Die Keys für die Verschlüsselung werden in der Microsoft Cloud hinterlegt und Microsoft nutzt die sich daraus ergebenden Möglichkeiten zum Mitlesen[10] (juristisch korrekt wird in den Datenschutzbestimmungen darauf hingewiesen).

Abhörschnittstellen

Anfang der 90er Jahre des letzten Jahrhunderts wurde das Festnetz in den Industriestaaten digitalisiert und die GSM-Verschlüsselung für Handytelefonate wurde eingeführt. Klassische Abhörmaßnahmen für einen Telefonanschluss waren ohne Kooperation der Telekommuniationsanbieter und ohne vorbereitete Schnittstellen nicht mehr möglich.

Als Antwort auf diese Entwicklung wurden in allen westlichen Industriestaaten Gesetze beschlossen, die die Telekommunikationsanbieter zur Kooperation mit den Strafverfolgungsbehörden und Geheimdiensten verpflichten und Abhörschnittstellen zwingend vorschreiben. In den USA war es der *CALEA Act* [11] von 1994. In Deutschland wurde 1995 auf Initiative des Verfassungsschutz die *Fernmeldeverkehr-Überwachungsverordnung* (FÜV) [12] beschlossen, die 2002 durch die *Telekommunikations-Überwachungsverordnung* (TKÜV) [13] ersetzt wurde.

2005 wurde der CALEA Act durch das höchste US-Gericht so interpretiert, dass er auch für alle VoIP-Anbieter gilt, die Verbindungen in Telefonnetze weiterleiten können. Skype zierte sich anfangs, die geforderten Abhörschnittstellen zu implementieren. Mit der Übernahme von Skype durch Ebay im Nov. 2005 wurde die Diskussion beendet. Heute bietet Skype Abhörschnittstellen in allen westeuropäischen Ländern und zunehmend auch in anderen Ländern wie Indien. In Deutschland sind Abhörprotokolle aus Skype

[10] https://heise.de/-1857620
[11] https://secure.wikimedia.org/wikipedia/en/wiki/Calea
[12] http://www.online-recht.de/vorges.html?FUEV
[13] https://de.wikipedia.org/wiki/Telekommunikations-%C3%9Cberwachungsverordnung

Gesprächen alltägliches Beweismaterial.[14]

Skype ist seit 2011 PRISM Partner der NSA und damit direkt an das Spionagesystem der USA angeschlossen. Mit der Übenahme durch Microsoft 2012 und dem technischen Umbau konnte die von der NSA analysierte Datenmenge aus der Skype verdreifacht werden.[15]

9.2 Instant Messaging

Die Übernahme von WhatsApp durch Facebook zeigt, dass es einfach Sch.... ist, sich das gesamte Adressbuch mit allen Kontakten klauen zu lassen. Irgendwann landet es in den großen Datensammlungen von Google, Microsoft, Facebook oder Yahoo!, die alle als PRISM-Partner der NSA gelistet sind.[16]

In korrektem Juristen-Deutsch könnte man es DSGVO-konform z. B. so formulieren:[17]

> *Wer den Messenger-Dienst WhatsApp nutzt, übermittelt nach den technischen Vorgaben des Dienstes fortlaufend Daten in Klardaten-Form von allen in dem eigenen Smartphone-Adressbuch eingetragenen Kontaktpersonen an das hinter dem Dienst stehende Unternehmen (Facebook).*
>
> *Wer durch seine Nutzung von WhatsApp diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden.*

Wenn man als WhatsApp Nutzer die Telefonnummern mit Bekannten austauscht, dann müsste man also eigentlich um die Zustimmung bitten, Name, Telefonnummer und Freundschaftsstatus an Facebook zu schicken. Das Gespräch könnte so ablaufen:

- Anton: *Du hast doch nichts dagegen, wenn ich Facebook Deinen Namen mit der Telefonnummer schicke und das wir Freunde sind - oder?*
- Beatrice: *Eyhh man, alles ok - mache ich doch auch.?*

Anforderungen an einen guten Messenger

Unter Berücksichtigung der massiven Überwachung von Instant Messaging, welche durch E. Snowden bekannt gemacht wurde, und des Crypto War 3.0 ergeben sich folgende Anforderungen an einen guten Messenger Dienst:

1. Sichere Ende-zu-Ende Verschlüsselung nach dem aktuellen Stand der Technik, die durch unabhängige Experten evaluiert werden kann. Die Auswertung von 160.000 Überwachungsberichten aus dem Snowden-Fundus[18] zeigt, dass Geheimdienste die Messenger Kommunikation massiv überwachen.
2. Sichere Transportverschlüsselung (SSL/TLS) für die notwendige Kommunikation der Apps mit den Servern und zwischen den Servern. Dabei sollten alle Best Practice Empfehlungen umgesetzt werden inklusive Certificate Pinning u.ä.
3. Der Account sollte frei wählbar und nicht an eine Telefonnummer gebunden sein. Telefonnummern sind im Gegensatz zu E-Mail Adressen ein eindeutiges Identifizierungsmerkmal und nicht so einfach austauschbar wie (Wegwerf-) E-Mail Adressen.

[14] http://www.lawblog.de/index.php/archives/2010/08/17/skype-staat-hort-mit
[15] https://heise.de/-1916340
[16] https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/whatsapp-will-infos-mit-facebook-teilen-12995
[17] https://www.lareda.hessenrecht.hessen.de/bshe/document/LARE190000030
[18] http://apps.washingtonpost.com/g/page/world/communication-breakdown/1153/

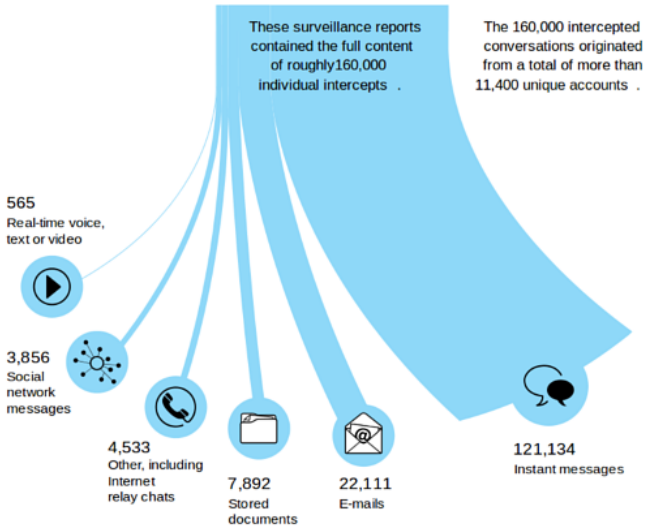


Abbildung 9.2: Auswertung von 160.000 Überwachungsberichten

Das ermöglicht die Verknüpfung verschiedener Accounts bei unterschiedlichen Messaging und die Zuordnung zu einer Person. Außerdem schützt die Weitergabe eines Pseudonyms statt Telefonnummer gegen Stalking.

4. Es sollte keine unerwünschten Uploads (Datenklau) ohne ausdrückliche Zustimmung durch den Nutzer geben. Der Dienst sollte auch komplett ohne Datenklau nutzbar sein und nur optional Daten wie das Adressbuch abgreifen.

5. Eine Google-freie Installation (beispielsweise via F-Droid) sollte möglich sein.

6. Die Nutzung auf dem Desktop PC sollte möglich sein. Oft lässt es sich auf dem PC oder Laptop mit Tastatur/Bildschim besser arbeiten als mit einem Smartphone.

7. Die Infrastruktur sollte dezentral verteilt sein und nicht von einem einzelnen Betreiber kontrolliert werden. Dezentrale Infrastruktur sind nur schwer von Regierungen durch Gesetze kompromittierbar, um Geheimdiensten die Überwachung zu ermöglichen wie z. B. mit BlackBerry in Indien oder in Kanada, Skype weltweit oder die Gesetze zu Backdoors für alle Messenger in Russland oder Australien.

   Im Gegensatz zu einigen Open Source Dogmatikern bin ich nicht der Meinung, dass die dezentrale Infrastruktur freier Messenger gegen die Installation von Backdoors auf den Servern schützt. Während bei Threema oder Signal App immer wieder angezweifelt wird, ob dort wirklich die auditierte bzw. veröffentlichte Software auf den Servern läuft, werden die Open Source Admin von Jabber oder Matrix Servern per Definition zu Heiligen erklärt, die niemals nie etwas anderes installieren würden als die offizielle Serversoftware und nie neugierig Metadaten beschnüffeln würden.

   Für diese Glorifizierung der Open Source Admins gibt es keinen Grund. Als wir vor einigen Jahren noch Jabber/XMPP mit OTR-Verschlüsselung verwendeten, haben wir gehofft, das die Admins der Server nicht mit dem Modul *mod_otr*[19] - *Man in the middle module for Off-the-Record* spielen oder es zumindest nicht gegen uns anwenden. Man musste vertrauen, so wie man Threema oder Signal App vertrauen muss.

   Die Gründe für Vertrauen sind sehr individuell. Manch einer sagt sich: *Ich vertraue dem Admin, weil es ein Bekannter ist.* und ein anderer denkt *Ich vertraue dem Admin nicht, weil es ein Bekannter ist und die Neugier und Verführung zu einer kleinen Schnüffelei, die niemand bemerken würde, unter Bekannten größer ist.* (Stichwort Love-INT o.ä.)

[19] https://www.ejabberd.im/mod_otr

8. Es wäre schön, wenn die Bedienung so einfach wäre, dass auch meine Tante und ihre Kaffeekranz Freundinnen ohne lange Erklärungen damit umgehen können.

Einen idealen Messenger, der alle Bedingungen erfüllt, gibt es nicht. Man muss abwägen, was wichtig ist und welche Schwerpunkte man bei den Anforderungen setzt.

Multi-Device-Support und Ende-zu-Ende Verschlüsselung

Multi-Device-Support ist ein heutzutage ein Standardfeature für Messenger. Man möchte via PC und Laptop online sein, um eine vernüftige Tastatur und einen großen Bildschirm zu nutzen, und man möchte via Smartphone unterwegs erreichbar sein. Dieses Feature erschwert es aber, eine sichere Ende-zu-Ende Verschlüsselung zu realisieren.

Ein potenter Angreifer kann den Multi-Device-Support der Messenger Protokolle nutzen, um ein weiteres Gerät im Namen des Opfers zu registrieren. Damit können alle Unterhaltungen mitgelesen werden, evtl. sind auch Ende-zu-Ende verschlüsselte Chats betroffen (wie bei OMEMO).

Das BKA hat diesen Angriff mehrmals erfolgreich gegen Telegram Nutzer eingesetzt. Das Team von Prof. Fedderath demonstrierte es[20]: die Behörden müssen nur die Telefonnummer des zu belauschenden Account in der Telegram Web-App eingeben und die SMS zur Authorisierung des Zugriffs abfangen. Dann konnten die unverschlüsselten Gruppenchats unbeobachtet mitgelesen werden. (Die verschlüsselten Chats von Telegram können damit nicht geknackt werden, da die Verschlüsselung MTProto nicht Multi-Device fähig ist, sondern für jedes Gerät einen eigenen verschlüsselten Chat erstellt.)

Außerdem hat das BKA durch Registrierung eines zusätzlichen Gerätes für den WhatsApp Account von Magomed Ali-C (ein Terrorverdächtiger aus dem Umkreis von Anis Amri) die Ende-zu-Ende verschlüsselten Chats mitlesen können. Dafür brauchte das BKA allerdings kurzeitig einen unbeobachteten Zugriff auf das entsperrte Handy von Magomed Ali-C, um das zusätzliche Gerät zu aktivieren. (Das würde auch mit Signal App u.a. funktionieren.)

Im Iran wurden seit 2014 wesentlich elegantere Angriffe staatlicher Hacker auf Telegram und WhatsApp eingesetzt. Mit der Zusendung eines bösartigen Dokumentes wurden die Smartphones der Opfer kompromittiert und dann die Account Credentials von WhatsApp oder Telegram ausgelesen. Mit diesen Credentials konnten die Angreifer ein weiteres Gerät im Namen des Opfers registrieren und den Multi-Device Support exploiten, um die Chats mitzulesen. (Auch mit diesem Angriff war das Mitlesen von *Geheimen Chats* bei Telegram nicht möglich sondern nur das Mitlesen von normalen Chats und Gruppenchats. Bei WhatsApp wurde damit auch die E-2-E Verschlüsselung ausgehebelt.)

Das Audit der OMEMO Verschlüsselung für Jabber/XMPP beschreibt einen möglichen Man-in-the Middle Angriff auf die Verschlüsselung, der ebenfalls die Multi-Device Fähigkeiten des Protokolls ausnutzt. Ein Angreifer (Eve) veranlasst Alice, ein neues Gerät mit einem eigenen Key für Bob in die Liste aufzunehmen. Alice sendet in Zukunft alle Nachricht verschlüsselt mit den Schlüsseln für Bob+Eve. Eve kann die Nachrichten mitlesen ohne die Krypto brechen zu müssen. Um unentdeckt zu bleiben, entfernt Eve ihre Geräte-ID, bevor sie die Nachricht an Bob weiterleitet (Abb: 9.3). Diese Manipulation ist bei OMEMO möglich, weil die Nachrichten nicht kryptografisch authentifiziert werden. (Hat man das einfach vergessen?)

Bei OMEMO kann man diesen Angriff verhindern, wenn beide Kommunikationspartner oder alle Kommunikationspartner in einem Gruppenchat die Schlüssel gegenseitig verifizieren. In der Praxis ist das kaum machbar. OMEMO wirbt damit, die sichere Axolotl

[20] https://www.youtube.com/watch?v=wBaj0LxcnY8

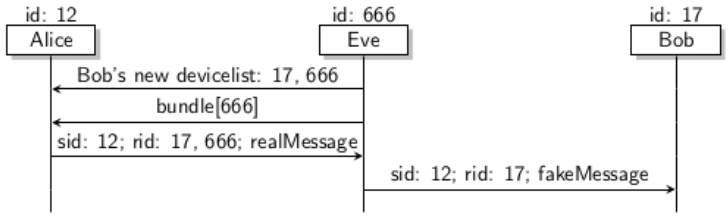


Abbildung 9.3: Man-in-the-Middle Angriff auf OMEMO Verschlüsselung

Verschlüsselung von Signal für Jabber/XMPP zu implementieren. Allerdings hat OMEMO die Verschlüsselung durch die eigene Erweiterung geschwächt. Man sollte also skeptisch bleiben, wenn ein Messenger damit wirbt, die Axolotl Verschlüsselung von Signal einzusetzen. Das Gesamtkonzept kann erheblich weniger Sicherheit bieten, als bei Signal App.

Ein kleiner Test von Riot ([matrix]) zeigte ebenfalls erhebliche Hürden in der Usability beim Schutz gegen das Einschleusen eines bösartigen Gerätes. (Wobei man noch hinzufügen muss, dass beide Teilnehmer in dem Chat als Krypto-Experten gelten und wirklich verstanden haben, wie sichere Krypto funktionieren könnte.)

- Anton: *Ok - habe Riot installiert und bin drin!*
- Beatrice: *War doch ganz einfach - oder?*
- Anton: *Aber der Chat ist unverschlüsselt. Sollte das nicht E-2-E sein?*
- Beatrice: *Du musst die E-2-E Verschlüsselung erst aktivieren.*
- Anton: *Habe ich in den Einstellungen aktiviert.*
- Beatrice: *Nee - DU musst es für JEDEN Chat einzeln aktivieren.*
- Anton: *Wie? Wo? Finde nix.*
- Beatrice: *Chat Settings, ganz runter scrollen, unten die letzte Option.*
- Anton: *Ok - hab's gefunden.*
- Beatrice: *Ist halt BETA, kann man noch verberssern.*
- Anton: *Hmmm - sehe gerade, dass Du hier mit 6 Geräten chattest!!! 2x Linux, 3x Ubuntu und ein seltsames Phone. Bist Du sicher, dass die alle von Dir sind - oder...???*
- Beatrice: *Kann schon sein, keine Ahnung - ich nutze Riot schon länger...*
- Anton: *Arrrghhhh...*

Es ist eine alte Weisheit, dass eine Kommunikation erst dann wirklich vertrauenswürdig ist, wenn man gegenseitig die Schlüssel verifiziert hat und sicherstellt, dass nur diese verifizierten Schlüssel verwendet werden. Die meisten Messenger bieten irgendwie eine Möglichkeit, bei einem Treffen die Schlüssel zu verifizieren, allerdings ist das nicht immer DAU-kompatibel.

Außerdem kann man als Schutzt gegen diese Angriffe bei den meisten Multi-Device fähigen Messengern in den Einstellungen eine zweistufige Bestätigung für das Hinzufügen weiterer Geräte aktivieren. Dann muss man ein zusätzliches Passwort für die Freischaltung eines neuen Gerätes eingeben. Man muss diese Feature aber selbst aktivieren, auch oder gerade dann, wenn man kein zweites Gerät verwenden möchte.

Anmerkung: Die Krypto-Protokolle OTR (Jabber/XMPP) und MTProto (Telegram) sind nicht Multi-Device fähig und von derartigen Angriff nicht betroffen.

Link Previews in Messengern

Einige Messenger bieten ein Link Preview, wenn man eine URL in das Eingabefeld tippt oder kopiert. Man kann den hübschen Preview versenden oder vor dem Versand löschen.

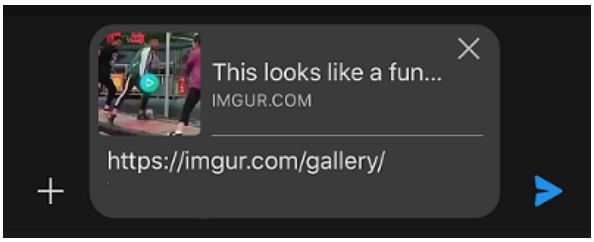


Abbildung 9.4: Link Preview in einem Chat in Signal App

Voraussetzung für einen Link Preview ist, das die Webseite im HTML Header die Open Graph Metatags enthält. Anhand dieser Metatags wird der Preview generiert:

```
<HTML>
  <HEAD>
    ...
    <meta property="og:title" content="Ein Beispiel">
    <meta property="og:description" content="Das ist nur ein sinnloses Beispiel">
    <meta property="og:image" content="https://beispiel.tld/images/preview01.png">
    ...
```

Um einen Link Preview zu generieren, kontaktiert der Messaging Client den Webserver und versucht die Webseite zu laden, sobald eine URL im Eingabefeld erkannt wird. Wenn die Webseite im Header die Open Graph Tags enthält, wird ein Preview generiert und evtl. das Bild herunter geladen. Den Ablauf kann man sehr unterschiedlich implementieren:

- WhatsApp hat die einfachste Implementierung gewählt. Der WhatsApp Messenger kontaktiert den Webserver direkt und hinterlässt damit Einträge in den Logs. Anhand der IP-Adresse kann damit die Verknüpfung zu einer Person erfolgen, wenn man beispw. den Link zu einer Facebook Seite versendet und dabei gleichzeitig bei Facebook eingeloggt ist. (Aber WhatsApp Nutzer stört das wahrscheinlich nicht.)

- Signal App generiert Link Previews nur für Webseiten, die via HTTPS erreichbar sind. Signal App kontaktiert den Webserver ebenfalls direkt und tarnt sich als *WhatsApp*.

  In den Datenschutz Einstellungen von Signal kann man die Previews abschalten.

- Telegram hat eine mittelmäßige Lösung implementiert. Die Link Previews werden auf dem Telegram Server generiert. Das verhindert Implikationen für die Privatsphäre wie bei WhatsApp, da nur der Telegram Server die Webseiten kontaktiert und das Abrufen der Informationen keinem Nutzer individuell zugeordnet werden kann.

  Bei unverschlüsselten Chats kann man das als brauchbare Lösung betrachten. Bei geheimen Chats, die Ende-zu-Ende verschlüsselt sind, sollte der der Telegram Server aber keine Informationen über die Inhalte der Chats sammeln können. Deshalb sollte man die Link Previews für geheime Chats abschalten. Die Option findet man in den Einstellungen unter *Privatsphäre und Sicherheit - Dateneinstellungen*.

- Matrix/Riot macht es ähnlich wie Telegram. Bei unverschlüsselten Chats werden die Link Previews vom Matrix Server generiert. Dieses Feature kann in den Einstellungen von Riot deaktiviert werden. Bei Ende-zu-Ende verschlüsselten Chats sollen laut Spezifikation keine Link Previews generiert werden.

9.2.1 Messenger Threema

Threema ist ein privacy-freundlicher Messenger aus der Schweiz. Chats, Gruppenchats und Audiotelefonie werden standardmäßig verschlüsselt. Im Gegensatz zu Signal oder Telegram wird nicht die Telefonnummer als Kennung verwendet sondern eine zufällige ID.

Das Erstellen von Channels und Bots (die bei Telegram populär sind) ist nur mit dem kostenpflichtigen Zusatzfeature Threema/Broadcast[21] möglich, was den Missbrauch reduziert. Die Channels und Bots können aber von allen Threema Nutzern abonniert werden.

Die Software ist seit Dez. 2020 Open Source und wurde mehrfach auditiert[22]. Die Finanzierung erfolgt durch geringe, einmalige Kosten beim Download der App. Außerdem gibt es mit Threema Work eine Lösung für sichere Unternehmenskommunikation, mit der weitere Einnahmen für die Firma erwirtschaftet werden. Die Server stehen in der Schweiz.

Threema bietet horizontale Anonymität (Anonymität gegenüber Kommunikationspartnern). Man kann seine Threema-ID mit einem Link *https://threema.id/<8-stellige-ID>* in einem Blog o.ä. veröffentlichen, ohne die eigene Identität zu kompromittieren und gleichzeitig anderen eine Möglichkeit zur anonymen Kontaktaufnahme zu geben.

Bei Threema speichert der Client alle Informationen zu Kontaktlisten, Mitgliedschaften in Gruppenchats usw. lokal. Die Server haben keine Informationen. Wenn man das Smartphone wechselt, ist es wichtig, dass man ein Backup der lokalen Daten erstellt und auf dem neuen Smartphone einspielt. Wenn man das nicht macht, beginnt man komplett neu an mit einem neuen Account und verliert alle Kontakte und Gruppenmitgliedschaften.

Das Backup wird mit einem Passwort verschlüsselt und kann auf dem Threema Server gespeichern werden oder auf einem beliebigen WebDAV Server. Wenn man das Backup auf einem eigenen WebDAV Server speichern möchte, muss man dort ein Verzeichnis für Threema Safe anlegen (beispielsweise *threema-safe*) und ein Unterverzeichnis *backups*. In dem Threema Safe Verz. ist die Datei *config* mit folgendem Inhalt anzulegen:

```
{
   "maxBackupBytes": 524288,
   "retentionDays": 180
}
```

Dann kann man auf dem Smartphone ein Threema Safe Backup erstellen und als Experte die eigene WebDAV Adresse des Threema Safe Verzeichnisses angeben inklusive Login Credentials für den WebDAV Server (Abb. 9.5).

Der Name der Backupdatei ist die mit dem Backup Passwort verschlüsseltze Threema-ID. Auch wenn das Backup auf dem Threema Server rumliegt, ist nicht erkennbar, zu welchem Account das Backup gehört. Trotzdem kann die Datei beim Restore eindeutig gefunden werden. Dieses Konzept ist bisher unter Messengern einmalig.

Im Webshop[23] von Threema gibt es eine Google-freie Version für Android, die keine Bibliotheken von Google enthält und keine Google Server für Push Notifications nutzt. Statt dessen fragt diese Version alle 15min beim Server von Threema nach neuen Nachrichten und benötigt daher ein wenig mehr Energie vom Akku.

Threema war in mehreren Jahre die populärste kostenpflichtige App im Apple App Store und hat mehrere Millionen Nutzer. Es ist einer der sichersten Messenger. Die Umsetzung der Designziele (Whitepaper) und aller Sicherheitsempfehlungen für Smartphone Apps gemäß Stand der Technik wurde durch zwei Audits bestätigt.

[21] https://broadcast.threema.ch/de
[22] https://threema.ch/de/faq/code_audit
[23] https://shop.threema.ch/

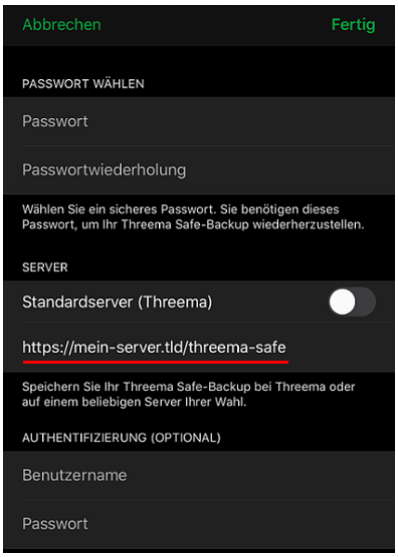


Abbildung 9.5: Eigenen WebDAV Server für Threema Backup auswählen

9.2.2 Messenger Signal App

Signal App wird von Security-Experten aufgrund der guten Ende-zu-Ende Verschlüsselung empfohlen. M. Marlspike entwickelte mit *Axolotl* die Ende-zu-Ende Verschlüsselung, die inzwischen zum Quasi-Standard für KryptoMessenger wurde.

> *I'm not really into advertising for stuff here but the recent update of TextSecure made a gigantic impression on me. The application works well, is uber user friendly, and looks just great.* (Collin R. Mulliner)

> *For the record - @moxie writes crypto software that blinds the #NSA & #GCHQ. He is their nightmare. Usable crypto developer with a backbone!* (J. Appelbaum)

Neben der Verschlüsselung setzt Signal auch konzeptuell neue Standards für Messenger. Alle Nachrichten, Kontaktlisten, Mitgliedschaften in Gruppenchats, persönliche Daten wie das Profilfoto usw. werden lokal in der Signal App gespeichert. Die Server speichern keine Informationen sondern transportieren nur verschlüsselte Nachrichten und Status-Informationen zu den Empfängern, ohne die Absender zu kennen (Sealed Sender).

Aus Sicherheitsgründen kann man Signal App nur mit einem Smartphone nutzen. Mehrere Smartphones mit dem gleichen Account sind nicht möglich. Zusätzlich kann man bis zu 5 Desktop Clients mit dem Account verbinden. Um Signal-Desktop mit einem Account zu verbinden, muss man den QR-Code von der Desktop App mit dem Smartphone scannen.

Signal bietet verschlüsselte **Audio- und Videotelefonie** (nicht im Desktop Client). Videokonferenzen (Group Calls) mit bis zu 5 Teilnehmern sind möglich. Für eine Konferenz erstellt man eine Gruppe mit den Teilnehmern und tippt auf das *Group Call* Symbol.

Für brisante Nachrichten, bei denen man verhindern möchte, dass Dritte sie durch Nachlässigkeit beim Umgang mit dem Smartphone zur Kenntnis nehmen könnten, bietet Signal App **selbstlöschende Nachrichten**. Wenn diese Option für einen Chat aktiviert wird, werden die danach geschriebenen Nachrichten eine einstellbare Zeit nach dem Lesen auf beiden Seiten automatisch gelöscht.

Der Messenger Signal entstand aus TextSecure, einer App zum verschlüsselten Versenden von SMS. Diese Wurzeln beeinflussen noch heute die Konzepte von Signal. Eine

SMS wird üblicherweise an einen Kontakt aus dem Adressbuch versendet. Natürlich kann man auch eine Telefonummer eingeben, aber das macht man eher selten. Ähnlich arbeitet Signal App. Die (verschlüsselten) Nachrichten werden an Kontakte gesendet, die über die Telefonnummer addressiert werden. Die Namen als Bezeichner und die Telefonnummern als Adressen der Kontakte holt sich Signal primär aus dem Adressbuch.

Beim Zugriff auf das **Adressbuch** bemüht sich Signal um einen Kompromiss zwischen einfacher Benutzbarkeit und Privatsphäre. Wenn man nach neuen Kontakten sucht, werden die Hashwerte der Telefonnummern aus dem Adressbuch zu den Servern hochgeladen und dort niemals gespeichert. Ein Blogartikel erklärt das Verfahren.[24]

Wenn man sein Smartphone verliert oder wechselt, dann verliert man auch alle Daten, die Signal App gespeichert hat. Es werden alle Daten nur lokal auf dem Smartphone gespeichert und nicht auf den Server. Deshalb braucht man ein Backup.

Das **Backup-Konzept** von Signal App ist dreistufig:

1. Das Adressbuch auf dem Smartphone dient als primäres Backup für den den *Social Graph* (Liste der Kontakte). Mit einem Backup vom Adressbuch hat man sofort alle Kontakte in Signal wieder hergestellt (außer Gruppenchats). Signal ist primär ein Messenger für private Kontakte, deren Telefonummern man im Adressbuch hat.

2. Optional kann man mit der Signal-PIN als zweite Backupstufe die Mitgliedschaften in Gruppen, Profilbild, Einstellungen und Daten neuer Funktionen wie Kontakte ohne Telefonnummer verschlüsselt auf den Signal Servern ablegen, um sie auf einem anderen Smartphone wiederherzustellen. Die Einstellungen für die Signal-PIN findet man in der Sektion *Datenschutz*.

   Ein Blogartikel erläutert die Voodoo Magie, wie aus einer einfachen, numerischen PIN ein starker Schlüssel für die Verschlüsselung abgeleitet wird. Man kann beim Festlegen der PIN aber auch eine alphanumerisches Passphrase als PIN wählen.

   Die Erinnerungsfunktion soll dabei helfen, die PIN auswendig zu lernen. Wenn man PIN bzw. Passpahrase in eine Passwortspeicher wie KeypassXC speichert, dann kann man die Erinnerungsfunktion auch deaktivieren.

   Außerdem kann eine Registrierungsperre für die Übernahme des Account auf ein anderes Smartphone aktiviert werden. Nach Ansicht der Entwickler reichen 7 Tage aus, um alle Kontakt zu informieren, dass man einen neuen Account verwendet.

   In den Einstellungen in der Sektion *Erweitert* kann man die Signal-PIN wieder deaktivieren.

3. Ein vollständiges Backup inklusive aller Chatinhalte kann man unter Android nur lokal auf einer SD-Karte speichern und auf ein neues Smartphone übertragen.

Für hohe Sicherheitsanforderungen bietet Signal App einige zusätzliche Optionen in der Sektion *Datenschutz* in den Einstellungen:

- Die *Bildschirmsperre bei Inaktivität* kann dagegen schützen, dass ein Angreifer bei kurzeitigem Zugriff auf das entsperrte Smartphone eine Signal Desktop Instanz initialisiert, um die Kommunikation mitzulesen. (Das BKA hat einen vergleichbaren Angriff bei WhatsApp gegen einen Terrorverdächtigen bereits aktiv eingesetzt.)

- Die Anrufe (Audio und Video) können immer über einen Signal Proxy geleitet werden, um dem Kommunikationspartner nicht die eigene IP-Adresse zu verraten.

- Die Anzeige der Signal Anrufe in der Call History kann abgeschaltet werden, damit die Metadaten über Signal Anrufe nicht in der Cloud von Google landen.

[24] https://signal.org/blog/private-contact-discovery/

Signal App für Android verwendet keine Google Services für Push Notifications bei neu eintreffenden Nachrichten. Aus Sicht der Privatsphäre ist das erfreulich, bringt aber bei einigen Nutzern das Problem, dass sie keine Notifications bei neuen Nachrichten erhalten sondern immer in der App nachschauen müssen, ob es etwas Neues gibt. Um dieses Problem zu vermeiden, müssen folgende Vorraussetzungen erfüllt sein:

- Die Signal App muss auch Hintergrund aktiv bleiben dürfen und sollte nicht durch Stromsparmaßnahmen abgeschossen werden.
- Für die Signal App müssen im Hintergrund Internetaktivitäten erlaubt sein.

Ein Support Artikel erläutert die Einstellungen für verschiedene Android Phones.[25]

Es gibt aber auch Nachteile:

- Die Telefonnummer wird als Account Kennung verwendet. Daher ist Siganl App in erster Linie für die Kommunikation mit Freunden empfehlenswert, denen man ohne Bedenken auch Telefonnummer geben würde ohne Stalking zu befürchten.
- Die Server der Infrastruktur stehen alle in den USA. Eine Freigabe der Serverkomponente für den Aufbau einer dezentrale Serverstruktur mit unterschiedlichen Betreibern wird abgelehnt.

Signal App ist kostenlos. Betrieb und Entwicklung werden von der Signal Foundation finanziert, die dafür Spendengelder sammelt. Großspenden kamen u.a. von WhatsApp Gründer Brian Acton (50 Mio. Dollar) und von der Shuttleworth Foundation. Der Quellcode ist offen bei Github verfügbar.[26]

Signal-Desktop installieren und verwenden

Um Signal als Messenger zu verwenden, benötigt man zwingend ein Smartphone, auf dem man die Signal App installiert und seinen Hauptaccount mit der Telefonummer registriert. Auf bis zu fünf Desktop PCs oder Laptops können zusätzliche Clients eingerichtet werden, die mit allen Funktionen parallel zum Smartphone genutzt werden können.

Installation

- Für **Windows** gibt es auf der Download Seite[27] eine EXE-Datei, die man nach dem Download startet, um die Anwendung Signal-Desktop zu installieren.

Signal-Desktop verwenden

Beim ersten Start von Signal-Desktop zeigt das Hauptfenster einen QR-Code, den man mit der Signal App auf dem Smartphone scannen muss, um den Desktop-Client mit seinem Account zu verbinden. Die Daten werden lokal gespeichert, so das die Aktivierung nur einmalig nötig ist. Das ist einerseits bequem, andererseits gibt es einem Angreifer aber auch mehr Möglichkeiten.

Man muss die Signal App auf dem Smartphone öffnen, in den *Einstellungen* den Menüpunkt *Gekoppelte Geräte* öffnen und ein Gerät hinzufügen. Mit der Kamera scannt man den QRCode, um Signal-Desktop mit dem Account auf dem Smartphone zu verbinden.

Nach dem Scan des QRCode fragt das Smartphone nach der PIN für die Registrierungssperre, die man hoffentlich in den Datenschutzeinstellungen aktiviert hat.

Anschließend gibt man dem Siganl-Desktop noch einen Namen. Unter diesem Namen wird die Desktop App in der Liste der *Gekoppelte Geräte* auf dem Smartphone angezeigt.

[25] https://support.signal.org/hc/de/articles/360007318711-Problembehebung-bei-Benachrichtigungen
[26] https://github.com/WhisperSystems
[27] https://signal.org/de/download/

Hier kann man ein Gerät auch wieder rauswerfen, wenn man es nicht mehr verwendet.

Dann kann man Signal parallel auf dem Desktop und dem Smartphone nutzen. Das Hauptfenster (Abb: 9.6) ist spartanisch und bietet nicht alle Funktionen wie auf dem SMartphone. Man kann chatten, Dateien senden oder verschlüsselt telefonieren. Als erstes könnte man an als Test sich selbst eine kleine Nachricht schicken.

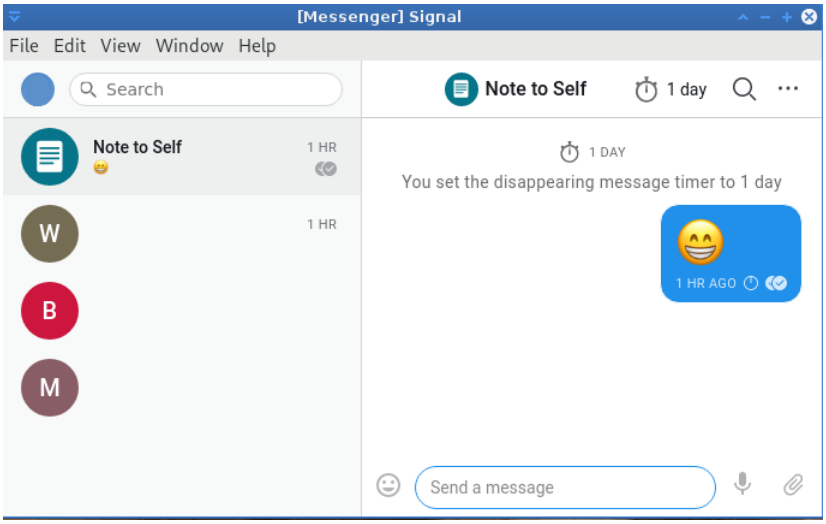


Abbildung 9.6: Hauptfenster von Signal-Desktop

Daten löschen, wenn der Account nicht mehr auf dem PC verwendet wird

Wenn man den Signal Account nicht mehr auf dem Desktop PC oder Laptop verwenden möchte, sollte man unbedingt alle auf der Festplatte gespeicherten Daten löschen. Signal-Desktop bietet in den Einstellungen mit einem dicken roten Button die Möglichkeit, diese Daten sicher zu entfernen.

9.2.3 Messenger Telegram

Telegram ist ebenfalls kostenlos nutzbar. Entwicklung und Betrieb wurden bisher aus dem Vermögen von Pavel Durov finanziert. Aber das Vermögen von P. Durov ist nicht unendlich und 2021 wird Telegram versuchen, Einnahmen zu erwirtschaften, um die Unabhängigkeit zu sichern. Es soll eine eigene Werbeplattform aufgebaut werden und für die Einblendung von Werbung in Channels genutzt werden (private Kommunikation soll werbefrei bleiben). Außerdem soll es kostenpflichtige Zusatzfeatures geben.

Telegram bietet viele Social Features und ist als eine Art *zensurresistentes Twitter mit Black Market Features* populär geworden, beispw. bei den Protesten in Hongkong und Belarus 2020. Als Messenger für private Kommunikation ist es eher ungeeignet. Bei der Sicherheit für private Chats ist sogar WhatsApp inzwischen besser geworden als Telegram.

Die Registrierung erfolgt mit einer Telefonnummer und erfordert ein Smartphone. Standardmäßig werden Chats und Gruppenchats nicht Ende-zu-Ende verschlüsselt und Telegram arbeitet als Cloud Messenger. Die Nachrichten liegen auf den Telegram Servern. Der Betreiber hat Zugriff auf die Chat History und kann Anfragen von Behörden beantworten. Telegram verkauft es als Privacy Feature, dass Anfragen von Behörden aus einigen Ländern ignoriert werden, aber darauf kann man sich nicht dauerhaft verlassen.

Für 1:1 Chats kann eine Ende-zu-Ende Verschlüsselung aktiviert werden (nicht für Gruppenchats). Diese *geheimen Chats* werden nicht in der Cloud gespeichert sondern nur

auf dem Smartphone (unverschlüsselt). Diese Verhalten ist seit Jahren als *Mannings Bug* bekannt und ein Security Bug, da ein Angreifer mit Zugriff auf das Smartphone die *geheimen Chats* auslesen kann. E-2-E verschlüsselte Chats sind auch verschlüsselt zu speichern!!!

Für besonders brisante Nachrichten in geheimen Chats bietet Telegram *selbstlöschende Nachrichten*, die nach einer einstellbaren Zeit nach dem Lesen gelöscht werden.

Die Audio- und Videotelefonie mit Telegram ist immer Ende-zu-Ende verschlüsselt. Zur Verifizierung der Verschlüsselung werden oben rechts vier Emojis angezeigt. Wenn beide Seiten die gleichen Emojis sehen, ist die Verschlüsselung sicher.

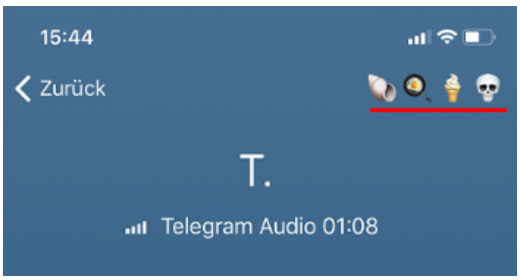


Abbildung 9.7: Verifizierung der Verschlüsselung für Audio- und Videotelefonie

Den Zugriff auf das *Adressbuch* zum Finden von neuen Kontakten kann unter *Privatsphäre - Dateneinstellungen* deaktiviert werden und das ist DRINGEND empfehlenswert.

Wenn man den Zugriff auf das Adressbuch erlaubt, werden zusammen mit der Telefonnummer auch die Namen aus dem Adressbuch auf die Telegram Server hochgeladen. Über eine API können Dritte diese Informationen abfragen und es könnte evtl. peinlich sein, wenn Dritte erfahren, dass man unter der Bezeichnung *Schnuckelchen* gespeichert wurde. A. Navalny hat diese Funktion im Dez. 2020 in einem Interview demonstriert. Er hat die Telefonnummer eines Co-Travellers bei einem Telegram Bot eingegeben und als Antwort wurde u.a. *FSB Vladimir Alexandrovich Panyaev* angezeigt - echt peinlich.

Eine inverse Suche nach Telefonnummern um den Inhaber einer Nummer zu ermitteln, ist auch in Telefonbüchern möglich. Allerdings findet man dort nur Personen bzw. Firmen, die gefunden werden möchten. Gegen die inverse Suche bei Telegram gibt es wenig Schutz und es betrifft nicht nur Telegram Nutzer sondern alle, die ein Telefon oder Smartphone benutzen und einen Telegram Nutzer kennen, der sein Adressbuch hochgeladen hat.

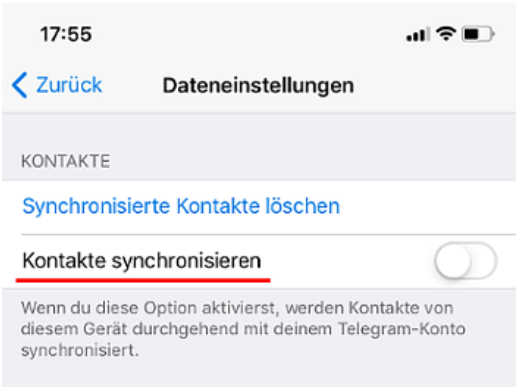


Abbildung 9.8: Deaktivierung des Upload der Kontakte in Telegram

Nach der Registrierung kann man ein *Pseudonym* erstellen und muss nur dieses Pseudonym an Kommunikationspartner weitergegeben. Die Zuordnung des Pseudonyms zum Account bzw. zur Telefonnummer wird auf den Telegram Servern gespeichert. Im Gegensatz zu Threema bietet ein Pseudonym keine Anonymität gegenüber dem Betreiber.

In den Einstellungen zur Privatsphäre kann man die Anzeige der eigenen Telefonnummer beim Gegenüber verbieten. Das schützt gegen Stalking auf anderen Kanälen und kann ein bisschen Anonymität gegenüber Kommunikationspartnern oder in Gruppenchats bieten. Da Telegram bei Terrorismusverdacht mit Behörden kooperiert, ist ein Pseudonym kein Sicherheitsfeature für politische Aktivisten, die mit staatlicher Verfolgung rechnen.

> *If Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities.*

Wenn der Angreifer eine Vermutung hat, zu welcher Gruppe von Personen ein Pseudonym gehört, könnte er bis zu 1.000 Telefonnummern im Adressbuch eingeben. Wenn die Telefonnummer im Adressbuch steht, wird sie auch in Chats unter dem Pseudonym angezeigt und über die Adressbuch-API kann der Angreifer den Namen herausfinden (s.o.)

Nach der Registrierung sollte man die zweistufige Bestätigung für das Hinzufügen neuer Geräte aktivieren. Es wurden bereits mehrfach staatliche Angriffe nachgewiesen, welche die Multi-Device Unterstützung ausnutzten, um unbemerkt Chats mitzulesen, die nicht Ende-zu-Ende verschlüsselt waren. Die zweistufige Registrierung aktiviert man in den Einstellungen unter *Privatsphäre und Sicherheit*. Es wird ein zusätzliches Passwort für die Registrierung von Desktop Clients für den Accout festgelegt.

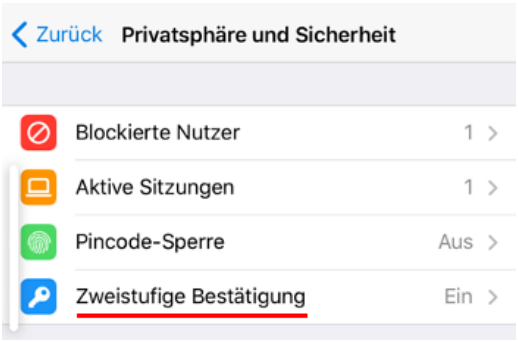


Abbildung 9.9: Zweistufige Bestätigung für neue Geräte aktivieren

Telegram Kanäle sind eines der besondern Social Media Features des Messengers. Man kann diese Kanäle nutzen, um einem breiten Publikum seine Meinung vorstellen oder um Millionen Follower bei Protesten zu informieren. Im Gegensatz zu Twitter ist man dabei nicht auf 200 Zeichen beschränkt und man kann auch anonym gegenüber Dritten bleiben.

- In Russland werden auf diesem Weg immer wieder Informationen über Korruption in unterschiedlichen Behörden publiziert.
- 2020 wurden diese Kanäle bei den Protesten in Hongkong gegen China und in Weißrussland gegen den Wahlbetrug genutzt, um Millionen Anhänger zu mobilieren.
- In Deutschland nutzen rechtsextreme Gruppen und viele Anhänger von Verschwörungstheorien dieses Medium, nachdem sie bei Facebook und Twitter wegen Verbreitung von Hass oder Fake News rausgeflogen sind.

Die Beispiele zeigen wieder einmal den Dual-Use Charakter von Kommunikationsmitteln. Einerseits wünschen sich politische Aktivisten ein Kommunikationsmedium, das nicht

staatlich kontrollierbar ist. Anderseits wird dieses Medium dann auch von Gruppen genutzt, die ... ähmm, also ... - oft jenseits der Legalität agieren?

Für die steigende Verbreitung der Telegram Kanäle als Social Media Tool zur Mobilisierung von (mehr oder weniger großen) Massen gibt es mehrere Gründe. Einerseits wird Telegram von Mio. Menschen für die tägliche Kommunikation genutzt und sie sind mit dem Tool vertraut. Anderseits ist Telegram sehr zensurresistent (technisch und inhaltlich).

- Aufgrund von Anti-Zensur Features kann der Dienst technisch kaum blockiert werden, wie die russische Rozkomnandsor bei einem Versuch lernen musste.

- Der Messenger unterliegt nicht dem NetzDG, das den Betreiber zur Löschung (politisch) unliebsamer Inhalte verpflichten würde wie Facebook, Twitter oder TikTok. Telegram kooperiert lediglich freiwillig bei der Verherrlichung von Terrorismus (IS).

Die Freiheit ist aber nicht grenzenlos. Im Okt. 2020 musste Telegram auf Druck von Apple zähneknirschend drei Kanäle der belarussischen Opposition schließen, in denen über 1.000 Name von Lukaschenkos Staatsdienern veröffentlicht wurden, die brutal gegen Protestler vorgegangen waren und in Gefägnissen gefoltert haben sollen. Apple hatte gedroht, die Telegram App wegen Doxxing aus dem AppStore zu entfernen. (Die Listen enthielten aber auch Fehler, Namen von irrtümlich beschuldigten Personen, die angeblich anhand von Videos identifziert wurden aber für den Tatzeitpunkt ein harmloses Alibi nachweisen konnten.)

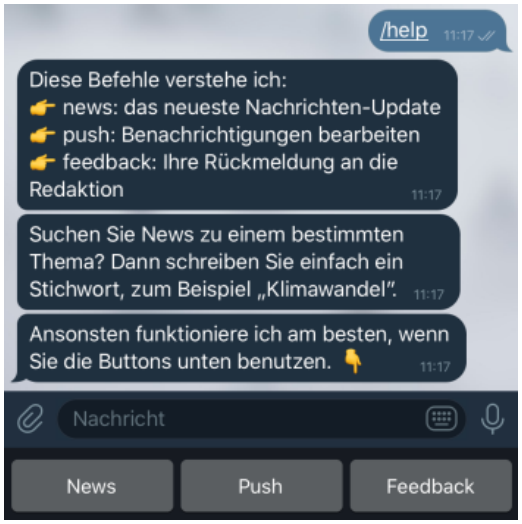
Telegram Bots sind ein weiteres, populäres Feature des Messengers. Ein Bot ist ein Chatpartner, der auf simple Kommando reagieren kann oder automatisiert Informationen liefert. Es ist keine grandiose, neue Erfindung, das gab es schon im letzten Jahrhundert bei IRC, aber aktuell sind Bots vor allem bei Telegram wieder populär geworden.

Ein einfaches simples Beispiel ist der Bot der ARD Tagesschau:

1. Einen Bot findet man über die Suche nach Kontakten in der Telegram App oder als Link auf Webseiten und man startet einen Chat, wie mit anderen Chatpartnern.

2. */start* ist das erste Kommando, das jeder Bot kennt und bei Beginn des Chats ausführt. Es zeigt meist eine kurze Einführung und am unteren Rand ein paar Buttons für weitere Kommandos.

3. */help* ist ein weiteres Kommando, das jeder Bot kennen muss und dass man ihm immer schicken kann, wenn man nicht weiter weiß.



Der Bot der ARD Tagesschau ist ein sehr einfaches Beispiel. Es gibt wesentlich ausgefeiltere Bots, die komplette Shopsysteme emulieren inklusive Auswahl aus den Angeboten, Bewertung der Verkäufer, Bezahlung usw. In diesen Shops kann man auch Dinge finden, die nach dem Betäubungsmittelgesetz illegal sind, gefälschte Dokumente oder Waffen... man muss nur lange genug suchen und darf natürlich nicht auf Fakes hereinfallen. Es bildet sich ein neues Darknet ähnlich wie bei den illegalen Marktplätzen auf Tor Onion Services, welches allerdings auch zukünftig von der Policy der Telegram Betreiber abhängig ist.

Die Sicherheit illegaler Handelsplätze für Drogen oder Waffen ist bei Telegram wesentlich geringer als im Darknet (beispw. Tor Onion Services), da ein zentraler Ansprechpartner als Betreiber existiert, der unter Umständen auch mit der Strafverfolgung kooperiert. Im Okt. 2020 wurden mehrere Chat Kanäle der Drogenszene mit mehr als 8.000 Nutzern vom

BKA übernommen. Die Chatverläufe konnten analysiert werden, es gab mehrere Festnahmen und das BKA hat eine Informationsseite in den übernommenen Gruppen anzeigen lassen. Zumindest der letzte Schritt wäre ohne Kooperation des Betreibers nicht möglich.

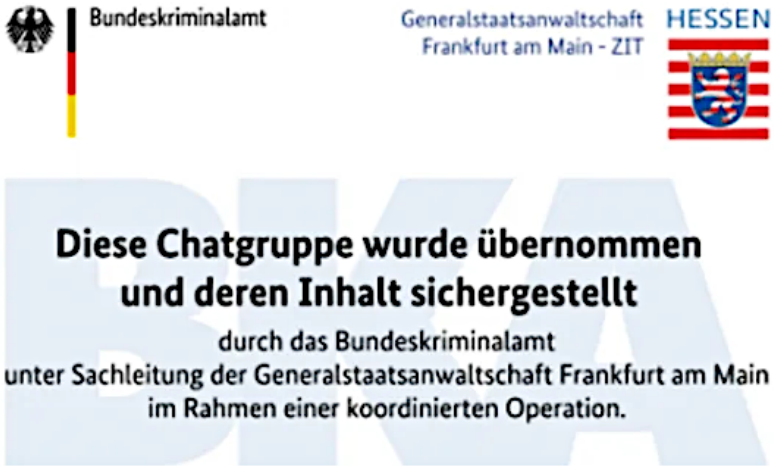


Abbildung 9.10: Informationsseite des BKA in Telegram in übernommen Chat Kanälen

9.2.4 Chatten mit Jabber/XMPP

Jabber/XMPP hat mich und andere Nerds seit vielen Jahren begleitet. Die Software ist OpenSource und ein weltweites Netz von tausenden Servern stellt sicher, dass Jabber nicht juristisch durch gesetzliche Vorgaben kompromittiert werden kann. Übergriffe auf die Privatsphäre durch Datendiebstahl (z.B. Adressbücher) hat es bei Jabber/XMPP nie gegeben und der Account kann frei gewählt werden, unabhängig von Telefonnummern.

Bei der Ende-zu-Ende Verschlüsselung gibt es mehrere Alternativen:

1. Off-the-Record (OTR) wurde 2001 mit dem Ziel entwickelt, möglichst einfach einsetzbar zu sein. OTR ist nicht Multi-Device fähing und verschlüsselt nur direkte Chats. Gruppenchats und Dateitransfer werden nicht verschlüsselt.

2. OpenPGP wurde bereits bei der Verschlüsselung von E-Mail behandelt. Die Erstellung und Austausch der Schlüssel ist etwas komplizierter als bei OTR und OMEMO. Die Vertrauenswürdigkeit der Verschlüsselung muss aber nicht extra verifiziert werden, da sie durch das Vertrauen in die OpenPGP-Schlüssel gegeben ist. OpenPGP verschlüsselt ebenfalls nur direkte Chats.

   Bei OpenPGP gibt es zwei Standards. Die meisten Jabber Clients implementieren XEP-0027, der inzwischen für obsolet erklärt wurde, da er einige Sicherheitslücken enthält. Der neuer XEP-0373 ist bisher noch als experimentell gekennzeichnet und wird nur von sehr wenigen Jabber Clients unterstützt.

3. OMEMO (OMEMO Multi-End Message and Object Encryption, XEP-384) ist eine relativ neue Ende-zu-Ende Verschlüsselung für Jabber/XMPP. Sie basiert auf Axolotl Ratchet, das von WhisperSystems für Signal App entwickelt wurde. Sie bietet wie OTR einen automatischen Schlüsseltausch, Forward Secrecy und Deniability. Zusätzlich bietet OMEMO verschlüsselte Offline-Messages und verschlüsselten Dateitransfer via HTTPUpload. Mit XEP-391 gibt es einen Standard für den verschlüsselten Jingle Dateitransfer, der bisher aber nur von wenigen Clients umgesetzt wird.

Im Vergleich zu den im Punkt Sicherheit führenden Messengern hinkt Jabber/XMPP bei der Umsetzung moderner Sicherheitsfeature hinterher. Die Ursachen dafür liegen in der förderalen Serverstruktur und der Community-basierten Entwicklung. Gerade diese

beiden Punkte sind für Open Source Dogmatiker die Pluspunkte von Jabber/XMPP und werden vehement verteidigt, ohne die Nachteile bezüglich Sicherheit zu erwähnen.

Einige Bespiele für kryptografische Schwächen bei Jabber/XMPP:

1. Certificate Pinning für die TLS Transportverschlüsselung zwischen Apps und Servern ist seit Jahren Bestandteil der Sicherheitsempfehlungen für die Entwicklung von Smartphone Apps, um Angriffe auf die TLS Verschlüsslung zu verhindern, bereits 2009 in der wiss. Arbeit *Certified Lies - Detecting and Defeating Government Interception Attacks against SSL* beschrieben wurden.

   Threema und Signal App nutzen CA-Pinning, um diese Angriffe zu verhindern.

   Bei Jabber/XMPP ist es aufgrund der förderalen Infrastruktur nicht möglich Certificate Pinning einzuführen. Im Gegensatz zur Threema oder Signal ist Jabber/XMPP damit weiterhin anfällig für man-in-the-middle Angriffe auf die TLS Verschlüsselung mit gefakten TLS Zertifikaten. (Einige Jabber Client wie ChatSecure oder CoyIM speichern die zuletzt verwendeten SSL Zertifikate der Server und warnen bei unerwarteten Änderungen, um diese Schwäche teilweise zu kompensieren. Die Warnungen muss man allerdings verstehen und nicht einfach ohne Nachdenken auf Ok klicken.)

2. Alle Kontaktlisten, Mitgliedschaften in Gruppenchats und persönliche Informationen wie Profilfotos u.ä. (VCards) werden bei Jabber/XMPP unverschlüsselt auf den Servern gespeichert, damit man von unterschiedlichen Geräten mit unterschiedlichen Clients darauf zugreifen kann (siehe: RFC 6121). Neben den Techies (Admins der Server) haben auch Behörden darauf Zugriff. Die im Rahmen des *Gesetzentwurfes zur Bekämpfung von Rechtsterrorismus und Hasskriminalität* vorgelegten Anpassungen am Telemediengesetz sollen es jedem Dorfpolizisten ohne richterliche Prüfung erlauben, diese Daten abzurufen.

   Bei Threema und Signal App werden diese Daten ausschließlich auf den Clients gespeichert. Die Server Betreiber haben keine Informationen über Kontaktlisten, Mitgliedschaften in Gruppenchats, Profilfotos o.ä. Das schränkt die Flexibilität bei der Verwendung unterschiedlicher Geräte ein zugunsten der Sicherheit.

3. Signal App und Threema haben ein Sicherheitskonzept, bei dem die Ende-zu-Ende Verschlüsselung der gesamten Kommunikation inkl. Audio- und Videotelefonie sowie Gruppenchats fester Bestandteil und durch Audits bestätigt ist.

   Bei Jabber/XMPP sind bisher alle Versuche einer Ende-zu-Ende Verschlüsselung unvollständig und können nicht sicherstellen, dass die gesamte Kommunikation zwischen zwei oder mehreren Partnern sicher verschlüsselt wird.

   - Teilweise werden XEPs zur Verschlüsselung durch die Community-basierte Entwicklung nur langsam umgesetzt und es dauert mehrere Jahre, bis man davon ausgehen kann, dass sie von einer Mehrheit der Clients unterstützt werden. Die Implentierung von OTR in Jabber Client Gajim war nach 15 Jahren noch immer experimentell und wurde dann zugunsten von OMEMO ganz fallen gelassen.
   - Teilweise sind die Standards selbst unvollständig und umfassen nicht die Verschlüsselung des gesamten möglichen Datenaustausch zwischen zwei oder mehreren Nutzen, wie beispielsweise auch bei OMEMO (XEP-384). Es gibt bisher keinen Standard, der die Ende-zu-Ende Verschlüsselung der gesamten Kommunikation bei Jabber/XMPP als Zielstellung definiert hat.
   - Teilweise liegt es auch an mangelder konzeptueller Vorarbeit. Es wird einfach erstmal irgendwas verschlüsselt - wird schon ok sein. Das Audit von OMEMO bemängelt gleich im ersten Absatz, dass es kein Angreifermodell gibt, gegen das die OMEMO Verschlüsselung schützen soll und keine Anforderungen beschrieben wurden. Damit ist es unmöglich, OMEMO qualifiziert zu auditieren, weil man ohne Zielvorgaben nicht prüfen kann, ob sie erfüllt werden.

4. Das Audit von OMEMO zeigte, das nicht-verifizierte Verbindungen anfällig für Man-in-the-Middle Angriffe sind, die den Multi-Device Support von OMEMO ausnutzen. Ein Man-in-the-Middle kann ein zusätzliches Gerät im Namen des Opfers registrieren und dann die verschlüsselten Chats mitlesen, ohne dass das Opfer es bemerkt. In Auswertung des Audits wurde die Möglichkeit der Verifikation von Schlüsseln eingeführt, die den Multi-Device Support (ursprünglich ein Killerfeature von OMEMO) wieder einschränkt. (Ob die gegenseitige Verifikation der Fingerprints der Schlüssel für eine größere Gruppe von Nicht-IT-Nerds praktisch umsetzbar ist - naja...)

   Threema und Signal App sind gegen vergleichbare Angriffe robust, da man ein zusätzliches Gerät für einen Nutzer nur mit physischen Zugriff auf das Smartphone mit dem Hauptaccount des Nutzers hinzufügen kann. Eine gegenseitige Verifizierung der Schlüssel ist möglich, aber wesentlich weniger wichtig.

Man sollte daraus nicht die Schlussfolgerung ziehen, dass Jabber/XMPP unbrauchbar ist. Wer Spaß daran hat, kann es weiterhin verwenden, wenn der Sicherheitslevel ausreichend ist. Bei der Diskussion über Alternativen sollte man aber nicht dogmatisch auf Open Source und förderale Strukturen bestehen, ohne die Mängel in der Kryptografie einzugestehen.

9.2.5 Messenger basierend auf [matrix]

[matrix] ist eine moderne Alternative zu Jabber/XMPP. Die Serverkomponenten (Matrix) sind Open Source und es ist der Aufbau einer förderalen Infrastruktur möglich. Jeder Interessierte kann einen eigenen Server betreiben, der mit allen anderen Accounts auf anderen Servern kommunizieren kann. Es gibt mehrere Client-Apps, wobei Element.io (früher: Riot) die größte Verbreitung hat.

Nach der Installation einer Client App kann man einen Account erstellen. Den Account kann man auf einem beliebigen Server entsprechend den eigenen Preferenzen frei wählen, unabhängig von der Telefonnummer. Diesen Server nennt man im Matrix Jargon den Homeserver. Über Identitätsserver kann man den Account auf Wunsch mit einer Telefonnummer oder E-Mail Adresse verbinden, so dass man leichter gefunden wird. . Überwiegend wird dafür der Server *vector.im* verwendet, der damit eine zentrale Funktion übernimmt.

Zentrales Konzept beim Chatten via [matrix] sind die *Räume*. Man kann sich auf seinem Homeserver neue *Räume* einrichten und dort erstmal Selbstgespräche führen. Wenn man eine zweite Person in den Raum einlädt und diese Person die Einladung annimmt, kann man chatten, Dateien austauschen oder telefonieren. Wenn man mehrere Personen in den *Raum* einlädt, hat man einen Gruppenchat. Innerhalb des *Raumes* lassen sich Rechte vergeben, wer administrieren darf, wer neue Mitglieder einladen darf usw.

Konzeptuell ist [matrix] ein Multi-Cloud Messenger. Im Gegensatz zu Threema oder Signal App, die keine Daten auf den Servern speichern, werden bei [matrix] alle Kontaklisten, Mitgliedschaften in Gruppenchats und persönlichen Informationen auf dem Homeserver gespeichert. Außerdem werden Räume inklusive der Nachrichteninhalte für unbegrenzte Zeit auf allen Matrix Servern in Kopie gespeichert, die an der Kommunikation beteiligt sind.

Im Gegensatz zu anderen Messengern wirbt [matrix] nicht damit, dass Nutzer die volle Kontrolle über ihre Kommunikation behalten. Der Vorteil ist laut [matrix] Werbung:

> *There is no single point of control or failure in a Matrix conversation which spans multiple servers: the act of communication with someone elsewhere in Matrix shares ownership of the conversation equally with them.*

Neben den Techies (Admins der beteiligten Server) und Hackern (April 2019: *Matrix.org chat server hacked, chat history lost*) haben auch Behörden im Rahmen von Auskunftsersuchen darauf Zugriff. Mit Umsetzung des im Dez. 2019 vorgelegten Gesetzentwurfes

zur Bekämpfung von Rechtsterrorismus und Hasskriminalität könnte jeder Dorfpolizist ohne richterliche Prüfung die Daten von dem bevorzugten Server abrufen, der sich juristisch in seiner Reichweite befindet. Sollten die Inhalte der Nachrichten Ende-zu-Ende verschlüsselt sein, können trotzdem detaillierte Metadaten der Kommunikation für die Kommunikationsanalyse abgerufen werden. (Wer, wie häufig, mit wem...?)

Nach der Rechtssprechung des BVerfG unterliegen Nachrichten nicht mehr dem Telekommunikationsgeheimnis nach §10 GG, wenn der Empfänger die Nachricht gelesen hat und die Gelegenheit hatte, sie zu löschen. Auf dem eigenen Homeserver kann man Nachrichten löschen, indem man eine Nachricht antippt und den Menüpunkt *Entfernen* wählt. Der Homeserver wird diesen Löschwunsch auch an alle anderen Server weitergeben, die Kopien der Nachricht gespeichert haben. Die Dokumentation von Matrix weist aber darauf hin, das damit nur ein Wunsch des Nutzers zum Ausdruck gebracht wird. Es kann nicht sichergestellt werden, dass die anderen Server diesen Wunsch auch befolgen. Im [matrix] Werbe-Slang:

> *This means that every server has total self-sovereignty over its users data...*

Open Source Enthusiasten argumentieren oft, dass man bei förderalen Systemen problemlos einen eigenen Server aufsetzen kann, wenn man keinen vertrauenswürdigen Server findet. Bei Matrix/Riot ist dieses Argument falsch. Man muss nicht nur dem eigenen Server vertrauen sondern auch den Admins aller anderen Server, die an einer Kommunikation beteiligt sind, da alle beteiligten Server eine komplette Kopie der Kommunikation speichern.

Im F-Droid Store gibt es eine Google-freie Version von Riot für Android, die keine Google Services für Push Notifications nutzt. Statt dessen wird ein Hintergrundprozess für die Synchronisation der Nachrichten verwendet, der ein bisschen mehr Energie vom Akku benötigt. In den Einstellungen kann man einen individuellen Kompromiss zwischen der Häufigkeit der Aktualisierung und Energieverbrauch konfigurieren.

Hinsichtlich Sicherheit könnte man noch anmerken, dass Certificate Pining als Schutzmaßnahme gegen Man-in-the-Middle Angriffe auf die TLS Verschlüsselung bei [matrix] aus den gleichen Gründen nicht möglich ist, wie bei Jabber/XMPP. Mit einer förderalen Infrastrutur, wo jeder Interessierte Admin einen eigenen Server betreiben kann, ist es unmöglich, diese Sicherheitsempfehlung umzusetzen. Im Gegensatz zu Threema oder Signal App ist der Riot damit weiterhin anfällig für Angriffe, die 2009 in der wiss. Arbeit *Certified Lies - Detecting and Defeating Government Interception Attacks against SSL* beschrieben wurden.

Die Ende-zu-Ende Verschlüsselung ist Teil des Sicherheitskonzeptes von [matrix] und standardmäßig aktiviert. Für eine hohe Sicherheitsansprüche gibt es folgende Optionen:

1. Verifikation der Kommunikationspartner: Die Verifizierung der Partner soll sicherstellen, dass man wirklich mit dem gewünschten Gegenüber verbunden ist, und erfolgt durch Scannen von QR-Codes bei einem persönlichen Treffen oder mit Emoji, die man über einen getrennten Kommunikationskanal (out-of-band) prüfen muss.

2. Cross-Signing mehrerer Geräte: Wenn man selbst mehrere Geräte verwendet, sollte man das Cross-Signing aktivieren. Dabei werden Signaturschlüssel und Key Backup auf dem Homeserver abgelegt und mit einem zusätzlichen Passwort verschlüsselt, das sich von dem Account Passwort unterscheiden sollte. Alternativ kann man den Schlüssel für das Cross-Signing herunter laden und lokal speichern. Die Signaturschlüssel werden verwendet, um eigene, neue Geräte zu signieren und das in die Vertrauensbasis bestehender Verifikationen einzuschließen.

   Verifizierte Kommunikationspartner müssen nicht mehr jedes einzelne Gerät verifizieren, wenn man Cross-Signing aktiviert. Man entscheidet selbst , welche Geräte vertrauenswürdig sind und verifiziertes Vertrauen wird auf neue Geräte übertragen.

Nach einer Verifizierung der Kommunikationspartner und der eigenen Geräte sollte man zusätzlich die Kommunikation mit nicht-verifizierten Geräten verbieten, damit man sicherheitsmäßig von der Verifizierung profitiert.

Neben den Smartphone Clients, deren Krypto-Implementierung jemand im Rahmen eines Audits nach Vorliegen der finalen Version untersuchen könnte, gibt es eine Browserversion als Desktop Client oder für den Einsatz auf einem Webserver. Aufgrund konzeptueller Schwächen kann man bereits ohne Prüfung der finalen Version sagen, das eine Webversion nicht für hohe Sicherheitsansprüche geeignet ist:

- Das Webserver-basierte Chat Clients für die Sicherheitsansprüche politischer Aktivisten, Menschrechtsaktivisten o.ä. generell nicht geeignet sind, hat Patrick Ball 2012 in einem Essay bei Wired am Beispiel von Cryptocat dargelegt.[28]

- riot-web speichert die privaten kryptografischen Schlüssel für die Ende-zu-Ende Verschlüsselung im HTML5 Storage des Browsers. Im *HTML5 Security Cheat Sheet*[29] wird vom OWASP empfohlen, keine sensitiven Informationen im HTML5 Storage zu speichern, da es kein sicherer Speicher ist und diese Daten leicht kompromittiert werden könnten, beispielsweise z. B. mit XSS-Angriffen.

  In der Dokumentation wird darauf hingewiesen, dass man das Web-GUI nicht auf dem gleichen Server installieren sollte wie den Matrix Server, da ein Angreifer mit XSS-Angriffen die Matrix-API kompromittieren könnte. Man findet aber keine Warnung dazu, dass auch die privaten Schlüssel für Ende-zu-Ende Verschlüsselung mit den gleichen Angriffen kompromittiert werden könnten.

9.2.6 Einige weitere Messenger (unvollständig)

Es gibt sehr viele Messenger. Man kann nicht alle kennen und vergleichen. Einige kleine Bemerkungen zu Messengern, die nicht empfohlen werden:

Wire wird in erster Linie als Collaboration Plattform für Unternehmen vermarktet. Das hauptsächlich in Berlin arbeitenden Entwicklerteam gehört juristisch zur Wire Swiss GmbH, die zu 100% der Wire Group Holdings Inc. in Dover (USA) gehört.

Die Software ist Open Source, Client Apps gibt es für Smartphones und PCs. Accounts kann man ohne Angabe einer Telefonnummer anlegen und dann auf bis zu 8 Geräte mit Smartphones oder PCs unabhängig von der Telefonnummer nutzen. Für die Inhalte der Kommunikation wird mit Proteus eine Ende-zu-Ende Verschlüsselung verwendet, die standardmäßig aktiv ist. Verschlüsselte Telefonie ist auch möglich.

Wire speichert die Metadaten der Kommunikation dauerhaft unverschlüsselt in der europäischen Amazon Cloud, also im direkten Zugriffsbereich US-amerikanischer Dienste. Die gesetzlich Grundlage für den Zugriff liefert der *Clarifying Lawful Overseas Use of Data Act*. Laut Wire ist diese Speicherung technisch nötig. Im Privacy Statement findet man keinen Hinweis auf diese Mini-VDS und keine Hinweis, wie lange die Metadaten gespeichert werden.

Vor einigen Jahren war Wire der neue deutsche Shooting Star unter den Krypto-Messengern, aber die Versprechungen auf förderale Infrastruktur der Server wurden auf unbekannte Zeit verschoben und Vorteile gegenüber WhatsApp sind gering. Als einziges Argument kann man noch anerkennen, das die Telefonbücher nicht an Datensammler weitergegeben werden. Das reicht nicht mehr für eine Empfehlung.

Facebook Messenger ist keine Alternative zu WhatsApp. Man kann zwar eine Ende-zu-Ende Verschlüsselung aktivieren, aber trotzdem kann Facebook bei Bedarf die verschlüsselten Chats mitlesen. Dabei wird nicht die Krypto gebrochen sondern auf Anforderung eine unverschlüsselte Kopie der Nachricht an Facebook gesendet.

[28] http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/
[29] https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html

Delta-Chat vergewaltigt das E-Mail Protokoll. Die Chat Nachrichten werden per E-Mail ausgetauscht und Delta-Chat verwendet dafür einen vorhandenen E-Mail Account.

Die Verschlüsselung erfolgt mit OpenPGP und der Schlüsselaustausch per Autocrypt. Warum Autocrypt kein sicherer Schlüsseltausch ist, kann man im Kapitel *E-Mail Verschlüsselung mit OpenPGP* nachlesen. Diese Verschlüsselung bietet nur geringe Sicherheit, konzeptuell bedingt nur *Some Protection Most of the Time*. Mit anderen Worten: sie wird genau dann nicht funktionieren, wenn man sie gebraucht hätte, also wenn sich ein ernsthafter Angreifer für die Inhalte der Chats interessiert.

Ende-zu-Ende Verschlüsselung soll gegen Belauschen durch die Provider schützen. Der oder die Provider sind die Angreifer, gegen den Ende-zu-Ende Verschlüsselung schützen soll. OpenPGP mit Autocrypt funktioniert aber nur, wenn die E-Mail Provider der Chat Teilnehmer vertrauenswürdig sind. Damit wird die Verschlüsselung obsolet.

Bei der E-Mail Kommunikation fallen viele Metadaten beim Provider an.

E-Mail ist das am häufigsten genutzte Medium für Textnachrichten. Als Realitätscheck ein Vergleich mit den genannten Messenger Diensten:

- Die Grundlage für die seit vielen Jahren hohe Nutzung von E-Mail bilden offene Protokolle, die eine förderale Serverlandschaft von vielen Anbietern auf Basis von Open Source Software erlauben.
- E-Mails werden in der Regel unverschlüsselt gesendet. Die großen E-Mail Provider wie Google oder Microsoft lesen ungeniert mit. Auch wenn man selbst einen privacy-freundlichen E-Mail Provider nutzt, ist man nicht gegen das Mitlesen nicht geschützt, weil:

  Google has most of my emails, because it has all of yours.
- Die zusätzliche Installation und Konfiguration von OpenPGP für die Ende-zu-Ende Verschlüsselung ist kompliziert. Es gibt keine Ende-zu-Ende Verschlüsselung mit *Forward Secrecy* für E-Mails.
- Der Austausch von Schlüsseln für OpenPGP oder S/MIME muss per Hand erfolgen, es gibt keinen vertrauenswürdigen Automatismus. Außerdem müssen die Schlüssel per Hand verifiziert werden.
- Die Sicherheit der Transportverschlüsselung (SSL/TLS) zwischen den Mailservern schwankt von *nicht vorhanden* bis *möglicherweise verschlüsselt, wenn keiner angreift*. Garantierte TLS-Verschlüsselung und Certificate Pinning in Form von DANE/TLSA gibt es erst in kleinen Ansätzen bei sehr wenigen Mailprovidern.

Schlussfolgerung: Trotz der Mängel haben die oben genannten Alternativen zu WhatsApp wie Signal oder Threema erhebliche Vorteile gegenüber E-Mails hinsichtlich der Verschlüsselung. Deshalb stehen Messenger im Crypto War 3.0 generell im Focus bei der Forderung nach Backdoors, während (bisher) keine Backdoors für verschlüsselte E-Mails gefordert werden.

Kapitel 10

Anonymisierungsdienste

Anonymisierungsdienste verwischen die Spuren im Internet bei der Nutzung herkömmlicher Webdienste. Die verschlüsselte Kommunikation verhindert auch ein Belauschen des Datenverkehrs durch mitlesende Dritte. Diese Dienste sind für den anonymen Zugriff auf Websites geeignet und ermöglichen auch unbeobachtete, private Kommunikation via E-Mail, Jabber, IRC...

Die unbeobachtete, private Kommunikation schafft keine rechtsfreien Räume im Internet, wie Demagogen des Überwachungsstaates immer wieder behaupten. Sie ist ein grundlegendes Menschenrecht, das uns zusteht. Nach den Erfahrungen mit der Diktatur Mitte des letzten Jahrhunderts findet man dieses Grundrecht in allen übergeordneten Normenkatalogen, von der UN-Charta der Menschenrechte bis zum Grundgesetz.

Anonymisierungsdienste sind ein Hammer unter den Tools zur Verteidigung der Privatsphäre, aber nicht jedes Problem ist ein Nagel. Das Tracking von Anbietern wie DoubleClick verhindert man effektiver, indem man den Zugriff auf Werbung unterbindet. Anbieter wie z. B. Google erfordern es, Cookies und JavaScript im Browser zu kontrollieren. Anderenfalls wird man trotz Nutzung von Anonymisierungsdiensten identifiziert.

10.1 Warum sollte man diese Dienste nutzen?

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

1. **Profilbildung:** Nahezu alle großen Suchmaschinen generieren Profile von Nutzern, Facebook u.a. Anbieter speichern die IP-Adressen für Auswertungen. Nutzt man Anonymisierungsdienste, ist es nicht möglich, diese Information sinnvoll auszuwerten.

2. **Standortbestimmung:** Die Anbietern von Webdiensten können den Standort des Nutzers nicht via Geolocation bestimmen. Damit ist es nicht möglich:

   - die Firma identifizieren, wenn der Nutzer in einem Firmennetz sitzt.
   - bei mobiler Nutzung des Internet Bewegungsprofile zu erstellen.

3. **Belauschen durch Dritte:** Die verschlüsselte der Kommunikation mit den Servern des Anonymisierungsdienstes verhindert ein Mitlesen des Datenverkehrs durch Dritte in unsicheren Netzen. (Cafes, WLANs am Flughafen oder im Hotel, TKÜV...)

4. **Rastern:** Obwohl IP-Adressen die Identifizierung von Nutzern ermöglichen, sind sie rechtlich in vielen Ländern ungenügend geschützt. In den USA können sie ohne richterliche Prüfung abgefragt werden. Die TK-Anbieter genießen Straffreiheit, wenn sie die nicht vorhandenen Grenzen übertreten. Wenig verwunderlich, dass man

IP-Adressen zur tagtäglichen Rasterfahndung nutzt. Facebook gibt täglich 20-30 IP-Adressen an US-Behörden, AOL übergibt 1000 Adressen pro Monat...

5. **Zensur:** Der Datenverkehr kann vom Provider oder einer restriktiven Firewall nicht manipuliert oder blockiert werden. Anonymisierungsdienste ermöglichen einen unzensierten Zugang zum Internet. Sie können sowohl die "Great Firewall" von China und Mauretanien durchtunneln sowie die in westeuropäischen Ländern verbreitet Zensur durch Kompromittierung des DNS-Systems.

6. **Repressionen:** Blogger können Anonymisierungsdienste nutzen, um kritische Informationen aus ihrem Land zu verbreiten ohne die Gefahr persönlicher Repressionen zu riskieren. Für Blogger aus Südafrika, Syrien oder Burma ist es teilweise lebenswichtig, anonym zu bleiben. Iran wertet Twitter-Accounts aus, um Dissidenden zu beobachten

7. **Leimruten:** Einige Websites werden immer wieder als Honeypot genutzt. Ein Beispiel sind die Leimrute des BKA. In mehr als 150 Fällen wurden die Fahndungseiten von LKAs oder des BKA als Honeypot genutzt und die Besucher der Webseiten in Ermittlungen einbezogen [1]. Surfer wurden identifiziert und machten sich verdächtig, wenn sie sich auffällig für bestimmte Themen interessierten.

8. **Geheimdienste:** Sicherheitsbehörden und Geheimdienste können mit diesen Diensten ihre Spuren verwischen. Nicht immer geht es dabei um aktuelle Operationen. Die Veröffentlichung der IP-Adressbereiche des BND bei Wikileaks ermöglichte interessante Schlussfolgerungen zur Arbeitsweise des Dienstes. Beispielsweise wurde damit bekannt, dass der BND gelegentlich einen bestimmten Escort Service in Berlin in Anspruch nimmt.

9. **Belauschen durch den Dienst:** Im Gegensatz zu einfachen VPNs oder Web-Proxys schützen 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.

[1] http://heise.de/-1704448

10.2 Tor Onion Router

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

Tor nutzt ein weltweit verteiltes Netz von 6.000-7.000 aktiven Nodes. Aus diesem Pool werden jeweils 3 Nodes für eine Route ausgewählt. Die Route wechselt regelmäßig in kurzen Zeitabständen. Die zwiebelartige Verschlüsselung sichert die Anonymität der Kommunikation. Selbst wenn zwei Nodes einer Route kompromittiert wurden, ist eine Beobachtung durch mitlesende Dritte nicht möglich. Da die Route durch das Tor Netzwerk ständig wechselt, müsste ein großer Teil des Netzes kompromittiert worden sein, um einen Nutzer zuverlässig deanonymisieren zu können.

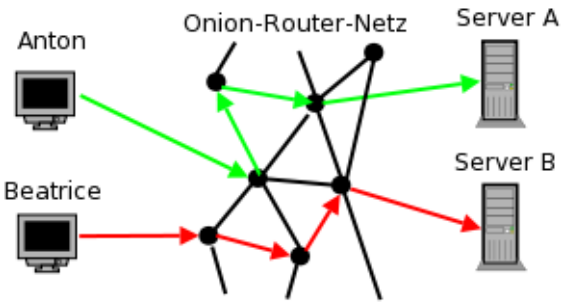


Abbildung 10.1: Das Prinzip von Tor Onion Router

Tor ist neben Surfen auch für IRC, Instant-Messaging, den Abruf von Mailboxen oder Anderes nutzbar. Dabei versteckt Tor nur die IP-Adresse! Für die sichere Übertragung der Daten ist SSL- oder TLS-Verschlüsselung zu nutzen. Sonst besteht die Möglichkeit, dass *Bad Exit Nodes* die Daten belauschen und an Userkennungen und Passwörter gelangen.

Der Inhalt der Kommunikation wird 1:1 übergeben. Für anonymes Surfen bedarf es weiterer Maßnahmen, um die Identifizierung anhand von Cookies, der HTTP-Header, ETags aus dem Cache oder JavaScript zu verhindern. Das TorBrowserBundle ist für anonymes Surfen mit zu nutzen.

Verschiedene Sicherheitsforscher demonstrierten, dass es mit schnüffelnden *Bad Exit Nodes* relativ einfach möglich ist, Daten der Nutzer zu sammeln.

- Dan Egerstad demonstrierte, wie man in kurzer Zeit die Account Daten von mehr als 1000 E-Mail Postfächern erschnüffeln kann, u.a. von 200 Botschaften.[2]

- Auf der Black Hack 2009 wurde ein Angriff auf die HTTPS-Verschlüsselung beschrieben. In Webseiten wurden HTTPS-Links durch HTTP-Links ersetzt. Innerhalb von 24h konnten mit einen Tor Exit Node folgende Accounts erschnüffelt werden: 114x Yahoo, 50x GMail, 9x Paypal, 9x Linkedin, 3x Facebook.[3]

  2012 haben mehrere russische Extis-Nodes diesen Angriff praktisch umgesetzt.

- Die Forscher um C. Castelluccia nutzten für ihren Aufsatz *Private Information Disclosure from Web Searches (The case of Google Web History)* einen schnüffelnden Tor Exit Node, um private Informationen von Google Nutzern zu gewinnen.[4]

[2] http://www.heise.de/security/news/meldung/95770
[3] http://blog.internetnews.com/skerner/2009/02/black-hat-hacking-ssl-with-ssl.html
[4] http://planete.inrialpes.fr/projects/private-information-disclosure-from-web-searches/

- Um reale Zahlen für das Paper *Exploiting P2P Applications to Trace and Profile Tor Users* zu generieren, wurden 6 modifizierte Tor Nodes genutzt und innerhalb von 23 Tagen mehr als 10.000 User deanonymisiert.[5]

Man kann davon auszugehen, dass die Geheimdienste verschiedener Länder ebenfalls im Tor-Netz aktiv sind und sollte die Hinweise zur Sicherheit beachten: sensible Daten nur über SSL-verschlüsselte Verbindungen übertragen, Warnungen nicht 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 Onion Services* bieten Möglichkeiten, anonym und zensurresistent zu publizieren.

Finanzierung von TorProject.org

Formal ist TorProject.org unabhängig. Über 20 Jahre hing das Projekt an der Finanzierung durch die US-Regierung und erst durch diese langjährige Finanzierung durch das US-Verteidigungsministerium, US-State-Department, Broadcasting Board of Governors (BBG ist ein Spin-Off der CIA, das auch Medien wie Voice of America, Radio Free Europe oder Radio Liberty beaufsichtigt) und andere US-Behörden konnte das Projekt zum erfolgreichen, größten Anonymisierungsprojekt werden.[6]

Seit 2015 bemüht TorProject.org sich darum, die Finanzierung zu diversifizieren und den Anteil der US-Regierung zu senken. Dieser Anteil sank von 85% (2015) auf 39% (2019).

Für die verbleibenden 61% der insgesamt 4,6 Mio. Dollar wurden 2020 folgende Geldgeber genannt:

- 15,4% von einer Behörde des schwedischen Außenministeriums
- 13,4% von der Mozilla Foundation
- 6,2% von der US-amerikanischen Stiftung Media Democracy Fund
- 4,1% von der Organisation Handshake Open Source Pledge
- 11,9% Einzelspenden

Tor ist eine Triple-Use-Technik

Anonymisierungsdienste und Kryptografie allgemein sind Triple-Use-Techniken. Am Beispiel von Tor Onion Router kann man es deutlich erkennen:

1. Ganz normal Menschen nutzen Tor, um ihre Privatsphäre vor kommerziellen Datensammlern sowie staatlicher Überwachung und Repressalien zu schützen. Dieses Szenario der Nutzung steht häufig im Mittelpunkt der Diskussion unter Privacy Aktivisten, ist aber meiner Meinung nach die kleinste Nutzergruppe.

2. Kriminelle nutzen in großen Umfang Tor, um verschiedenste Formen der Kommunikation geheim zu halten. Beispielsweise verwenden Botnetze Tor, um die Kommunikation mit den C&C Servern geheim zu halten. Das bekannteste Beispiel ist das Mevade.A Botnet. Im Sommer 2013 waren zeitweise 80-90% der Tor Clients Mevade.A Bots, wie man in Bild 10.2 sehen kann.

   Außerdem nutzen Drogenhändler u.a. die Technik der Tor Onion Sites (Tor Hidden Services), um ihre Waren anzubieten. Im Rahmen der Operation Onymous konnte das FBI mehr als 400 Drogenmarkplätze abgeschalten werden. Das FBI hatte dabei technische Unterstützung von der Carnegie Mellon Unversity bei der Deanonymisierung von Tor Onion Sites.

[5] http://hal.inria.fr/inria-00574178/en/
[6] https://surveillancevalley.com/blog/fact-checking-the-tor-projects-government-ties

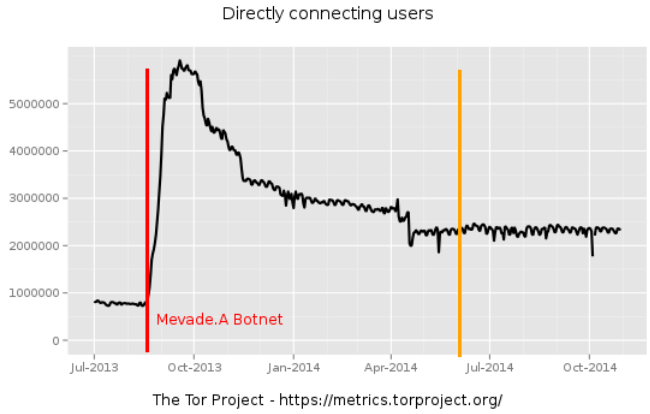


Abbildung 10.2: Mevada.A Botnetz von metrics.torproject.org

Die Nutzung von Anonymisierungsdiensten durch Kriminelle betrifft nicht nur Tor. Im Jahresbericht 2015 befürchten die Analysten von Europol, dass Kriminelle zukünfig das Invisible Internet Project (I2P) oder OpenBazaar statt Tor Onion Sites nutzen könnten, was die Verfolgung erschweren würde.

3. Die Geheimdienste nutzen Tor in erheblichen Umfang, um Kommunikation geheim zu halten. Außerdem ist Tor eine Waffe im Arsenal der CIA und des US-Cybercommand.

   Im Frühjahr 2014 auf dem Höhepunkt der Ukraine-Krise wurde beispielsweise ein Botnetz in Russland hochgefahren, dass der russischen Gegenseite ernsthafte Probleme bereitet hat. In Bild 10.3 sieht man den Anstieg der Tor Nutzer in Russland (aber nicht international), der typisch für ein aktiviertes Botnetz ist. Die russische Regierung hat offiziell 4 Mio. Rubel für einen Exploit geboten um die beteiligten Tor Nodes zu deanonymiseren.

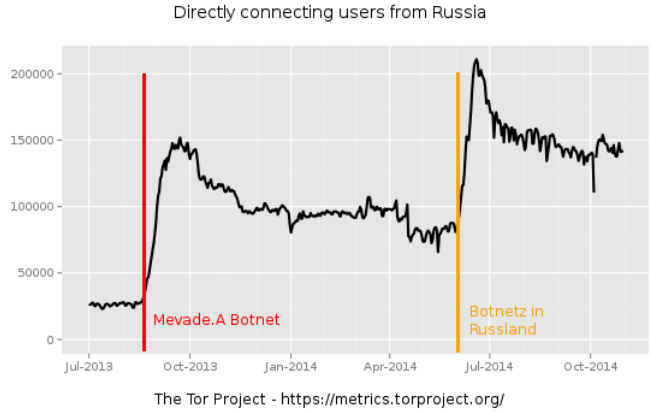


Abbildung 10.3: Botnetze mit Tor in Russland von metrics.torproject.org

Vom Journalisten Y. Levine veröffentlichte FOIA Dokumente zeigen, das insbesondere die CIA Tor aktiv als Werkzeug bei Kampagnen zur Destabilisierung unbequemer Länder nutzt:

> *The documents showed Tor employees taking orders from their handlers in the federal government, including hatching plans to deploy their anonymity tool in countries that the U.S. was working to destabilize: China, Iran, Vietnam, Russia.*

Die Nutzung von Tor ist meiner Meinung nach ein **Spiegel der gesellschaftlichen Probleme** und nicht der Technik selbst anzulasten.

1. Das in der UN-Menschenrechtscharta und der Europäische Menschenrechtskonvention deklarierte Recht auf unbeobachtet, pivate Kommunikation ist durch die staatlich organisierte Massenüberwachung und kommerzielle Datensammlungen praktisch abgeschafft. Bundesinnenminister Friedrich empfiehlt Selbstschutz, weil die technischen Möglichkeiten zur Ausspähung nun einmal existieren (die Bankrotterklärung der Politik), und Tor ist ein Technik zum Selbstschutz.

2. Kriminaltät wie Wirtschaftskriminalität, Eigentumsdelikte, Drogenkriminalität... oder ganz allgm. *Handlungen im Widerspruch zu geltenden Gesetzen* sind gesellschaftliche Phänomene, für die man nicht den technischen Hilfsmitteln die Schuld geben kann.

3. Im Rahmen der erneuten Eskalation des *Kalten Krieges* wird jede Technik hinsichtlich Brauchbarkeit als Waffe geprüft. Tor war von Anfang ein Projekt der US-Army und wird deshalb von der US-Regierung finanziert. Auf der Webseite von TorProject.org wird diese Nutzung ausdrücklich beworben. Diese Verwendung sollte auch denen klar sein, die sich als freiwillige Unterstützer an der Finanzierung eines Tor Node beteiligen oder selbst einen Tor Node betreiben.

Durch diese unterschiedlichen Interessen entstehen skurrile Situationen, wenn das FBI der Carnegie Mellon Unversity 1 Mio. Dollar zur Verfügung stellt, um Tor Onion Services für die Operation Onymous zu deanonymisieren[7], die Univerität die wiss. Ergebnisse auf der BlackHat Konferenz aber nicht publizieren darf[8], um die US-Cyberoperationen in Russland nicht zu gefährden, und die Entwickler bei TorProject.org auf Vermutungen angewiesen sind[9], um die Bugs zu fixen, damit sie politischen Aktivisten wie Wikileaks eine vertrauenswürdige Infrastruktur bereit stellen können.

10.2.1 Security Notes

Die Sicherheit von IP-Anonymisierern wie Tor Oinion Router ergibt sich nicht alleine aus der Qualität der Software und der Kryptografie. Durch Fehler bei der Nutzung oder durch falsche Konfiguration kann die Anonymität komplett ausgehebelt werden.

- Wer in seinem Standardbrowser nur die Proxy-Einstellungen anpasst um Tor zu verwenden, ist auch nicht sicher anonym. Eine Deanonymisierung ist mit WebRTC oder Java-Applets möglich. Cookies und andere Trackingfeatures können langfristig ebenfalls zu einer Deanonymisierung des Surfverhaltens führen.

- Viele Messenger verwenden *Interactive Connection Establishment* (ICE) für den Aufbau einer direkten Verbindung zwischen Clients für Audio- und Videochats. ICE ist Bestandteil von WebRTC und libjingle (XMPP). Dabei werden dem Kommunikationspartner alle verfügbare IP-Adressen (auch die öffentliche IP des Routers) zugeschickt und via UPnP Protokoll wird versucht, einen direkten Tunnel durch den Router zu bohren. Mit einem Audio- oder Videoanruf kann man also deanonymisiert werden.

- Einige nicht-anonyme Peer-2-Peer Protokolle wie BitTorrent übertragen die IP-Adresse des eigenen Rechners zusätzlich in Headern des Protokoll-Stacks ähnlich wie bei ICE. Damit ist es ebenfalls möglich, User zu deanonymisieren. Eine wiss. Arbeit zeigte, wie 10.000 BitTorrent Nutzer via Tor deanomisiert werden konnten.

- Der Assistent zur Einrichtung eines E-Mail Account in Thunderbird umgeht die Proxyeinstellungen beim Abrufen der Autoconfig Datei mit den Servereinstellungen und sendet dabei die eigene E-Mail Adresse an den Provider. Der E-Mail Provider erhält damit die echte IP-Adresse zusammen mit der E-Mail Adresse und man ist deanonymisiert, bevor man die erste E-Mail geschrieben oder empfangen hat.

[7] https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users
[8] https://web.archive.org/web/20140705114447/http://blackhat.com/us-14/briefings.html
[9] https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/

- Durch Software aus fragwürdigen Quellen können Backdoors zur Deanonymisierung geöffnet werden. Eine Gruppe von ANONYMOUS demonstrierte es, indem sie eine modifizierte Version des Firefox Add-on TorButton zum Download anboten, dass wirklich von einigen Tor-Nutzern verwendet wurde. Dieses Add-on enthielt eine Backdoor, um die Nutzer von einigen Tor Hidden Services mit kinderpronografischem Material zu identifizieren. Die Liste der damit deanonymisierten Surfer wurde im Herbst 2011 im Internet veröffentlicht.

Schlussfolgerungen:

- TorProject empfiehlt für anonymes Surfen ausdrücklich das TorBrowserBundle. Das ist eine angepasste Version des Browser Mozilla Firefox zusammen mit dem Tor Daemon. Nur diese Konfiguration kann als wirklich sicher nach dem aktuellen Stand der Technik gelten. Die vielen Sicherheitseinstellungen dieser Softwarekombination kann man nur unvollständig selbst umsetzen.
- Für alle weiteren Anwendungen sind die Anleitungen der Projekte zu lesen und zu respektieren. Nur die von den Entwicklern als sicher deklarierten Anwendungen sollten mit Tor genutzt werden.
- Verwenden Sie ausschießlich die Originalsoftware der Entwickler.

10.2.2 Anonym Surfen mit dem TorBrowserBundle

Das TorBrowserBundle enthält einen modifizierten Firefox als Browser sowie den Tor Daemon und ein Control Panel. Die Webseite stellt das TorBrowserBundle für verschiedene Betriebssysteme und in unterschiedlichen Sprachen zur Verfügung.

HINWEIS: es ist empfehlenswert, die **englische Version des TorBrowsers (en-US)** herunter zu laden. In den letzten Jahren gab es immer wieder aufgrund von Bugs im TBB die Möglichkeit, Hinweise auf die Lokalisierung des Browser zu fimden, z.B via Javascript *date.tolocale()* Funktion (Bug #5926) oder via Informationen aus dem HTTP Accept-Language Header (Bug #628) oder via *ressource://* URI (Bug #8725). Wenn man die deutsch lokalisierte Version des TorBrowsers nutzt, gibt man möglicherweise einen Hinweis auf eine deutsche Herkunft, und das möchte man beim anonymen Surfen natürlich vermeiden.

Neben der stabilen Version des TorBrowserBundle bietet TorProject.org auch eine Alpha-Version mit neuen Features zum Testen an. Diese Versionen enthalten manchmal Features, die man sich als Anwender sehr wünscht. Für den produktiven Einsatz empfehlen wir aber trotzdem, die stabile Version zu nutzen und zu warten, bis die Entwickler die neuen Features als ausreichend getestet einstufen und in die stabile Version übernehmen. Neben den möglichen Problemen der Stabilität ist auch die höhere Anonymität ein Grund für diese Empfehlung, da die Anonymitätsgruppe mit der stabilen Version größer ist.

Installation

Das Archiv ist nach dem Download zu entpacken, keine Installation nötig. Unter Windows öffnet man nach dem Download das selbstentpackende Archiv mit einem Doppelklick im Dateimanager und wählt ein Zielverzeichnis. Nach dem Entpacken startet man alle Komponenten mit einem Doppelklick auf **Start Tor Browser.exe** im Dateimanager.

Wenn die Downloadseite für das TorBrowserBundle gesperrt ist, dann findet man unter GetTor[10] alternative Downloadmöglichkeiten. Man kann z.B. per Jabber/XMPP oder E-Mail eine Nachricht mit dem gewünschten Betriebssystem (windows, linux, osx) an den Account *gettor@torproject.org* schicken und bekommt eine Liste alternativer Downloadlinks.

Beim ersten Start öffnet sich zuerst das Control Panel. Hier kann man bei Problemen Einstellungen zur Umgehung von Firewalls konfigurieren (z.B. wenn eine Firewall nur

[10] https://gettor.torproject.org/

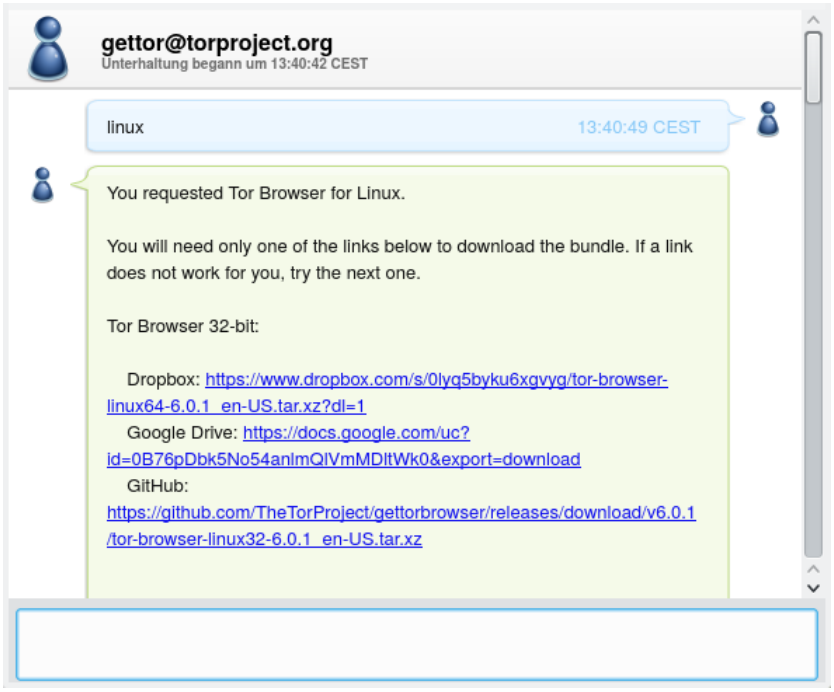


Abbildung 10.4: Alternative Downloadlinks via Jabber/XMPP abrufen

Verbindungen zu bestimmten Ports passieren lässt) oder man kann den Tor Daemon mit Klick auf den Button *Verbinde* ohne weitere Konfiguration starten.

Größe des Browserfensters

Der TorBrowser startet mit einer festgelegten Größe des Browserfensters. Die Fensterbreite sollte ein Vielfaches von 200px sein (max. 1000px) und die Höhe ein Vielfaches von 100px. Die Fenstergröße wird gleichzeitig als Bildschirmgröße via JavaScript bereitgestellt. Da die innere Größe des Browserfensters und die Bildschirmgröße als Tracking-Feature genutzt werden, sollte man die voreingestellte Größe des Browserfensters nicht(!) ändern.

Sicherheitseinstellungen

Die folgenden Beispiele für erfolgreiche Angriffe beziehen sich auf FBI, weil es darüber Berichte gibt. Es sind aber nur Beispiele (nicht nur NSA und FBI haben fähige Hacker). *Rule 41 of the US Federal Rules of Criminal Procedure*[11] erlaubt seit Dez. 2016 dem FBI das massenweise Hacken von Tor- und VPN-Nutzern unabhägig davon, in welchem Land die Tor-Nutzer sich befinden.

1. 2016 wurde auf der Tor Mailingliste[12] ein Javascript Bug gepostet, den das FBI aktiv mit Exploits ausnutzte, um einen Trojaner zu installieren, der Tor Nutzer deanonymisiert. Der Einsatz wurde auf der vom FBI beschlagnahmten Onion Site Giftbox nachgewiesen.[13]

2. 2015 verwendete das FBI einen Zero-Day-Exploit im TorBrowser, um einen Trojaner zu installieren und die Tor-Nutzer damit zu deanonymisieren. Welcher Lücke im Firefox dabei ausgenutzt wurde, ist nicht bekannt. Mozilla und TorProject.org haben

[11] https://blog.torproject.org/blog/day-action-stop-changes-rule-41
[12] https://lists.torproject.org/pipermail/tor-talk/2016-November/042639.html
[13] https://motherboard.vice.com/en_us/article/9a3mq7/tor-browser-zero-day-exploit-targeted-dark-web-child-porn-site-giftbox

Abbildung 10.5: Start des TorBrowser

sich bemüht, aber die Informationen zur ausgenutzten Lücke wurden unter Hinweis auf die Nationale Sicherheit als geheim eingestuft.[14]

3. Im Sommer 2013 wurden tausende Tor-Nutzer mit dem FBI-Trojaner *Magneto* infiziert. Der Exploit zur Installation des Trojaners nutzte einen JavaScript Bug im Tor-Browser aus. Der installierte Trojaner sendete die IP-Adresse, die MAC-Adresse und den Namen des Rechners an einen FBI Server, um Tor-Nutzer zu deanonymisieren.[15]

4. Aus den Snwoden Dokumenten geht hervor, dass die NSA das TorBrowserBundle auf Basis von Firefox 10 esr über einen Bug in E4X, einer XML Extension für JavaScript, automatisiert angreifen und Nutzer deanonymisieren konnten.[16]

Die Tor-Entwickler haben den Tradeoff zwischen einfacher Benutzbarkeit und Sicherheit in den Default-Einstellungen zugunsten der einfachen Benutzbarkeit entschieden. Es wird aber anerkannt, dass diese Einstellungen ein Sicherheitrisiko sind. In den FAQ steht:

> *There's a tradeoff here. On the one hand, we should leave JavaScript enabled by default so websites work the way users expect. On the other hand, we should disable JavaScript by default to better protect against browser vulnerabilities (not just a theoretical concern!).*

Beim Start wird man darauf hingewiesen, dass man die Sicherheitseinstellungen anpassen kann. TorBrowser startet standardmäßig mit dem niedrigsten Sicherheitslevel *Standard*, um das Surferlebnis möglichst wenig einzuschränken. Bei Bedarf kann man den Sicherheitslevel erhöhen.

Für sicherheitsbewuste Nutzer ist der umgekehrten Weg empfehlenswert. Man kann standardmäßig im höchsten Sicherheitslevel *Safest* surfen und wenn es ein Login bei einer Webseite erfordert, auf den mittleren Level *Safer* wechseln. Fast alle Websites, die einen Login erfordern (E-Mail Provider u.ä.), kann man mit dem Level *Safer* problemlos nutzen.

[14] https://motherboard.vice.com/read/the-fbi-is-classifying-its-tor-browser-exploit
[15] http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi
[16] http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

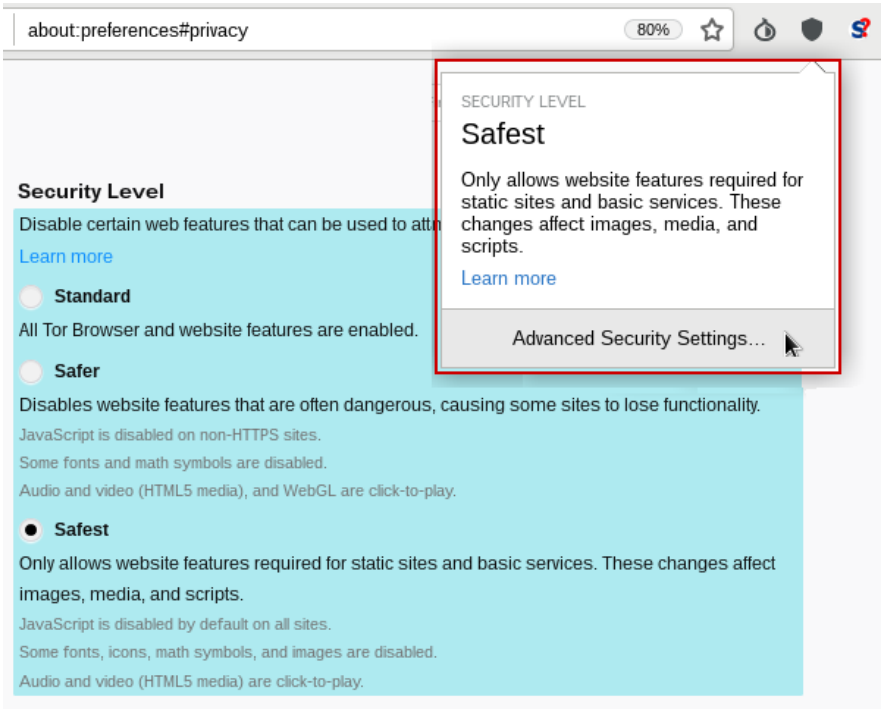


Abbildung 10.6: Sicherheitslevel im TorBrowser anpassen

Um den Sicherheitslevel anzupassen, klickt man auf das Symbol mit dem Schild (2. Symbol rechts neben der URL-Leiste) und in dem ausklappenden Menü auf *Advanced Security Settings*. Im Browser wird dann die Seite mit den Einstellungen geöffnet.

Wenn man den Sicherheitslevel auf *Standard* verringert, könnten bösartige Exit Nodes unschöne Dinge in den HTML Code von Webseiten einfügen, die über unverschlüsselte HTTP-Verbindung geladen werden. Das ist nicht empfehlenswert. Neben der NSA und dem FBI betreiben auch andere Geheimdienste bösartige Tor Exit Nodes. Ein Leak von Daten des russischen Geheimdienstleisters Systec zeigte, dass auch der FSB diese Methode nutzt. Die Überwachungsdichte und die Aggressivität der Angreifer ist im Tor Netzwerk viel höher, als im normalen Internet. Daher sollte man auch die erforderlichen Schutzmaßnahmen deutlich höher ansetzen, als bei einem normalen Browser.

HTTPS Security

sslstripe Angriffe durch Bad Tor Exit Nodes, die 2009 auf der Black Hack Konferenz demonstriert wurden, sind auch 2020 noch ein aktuelles Problem.

Als Schutz gegen diese Angriffe enthält der TorBrowser das Add-on HTTPSEverywhere, welches anhand von Regeln die Umschreibung von HTTP Adressen auf HTTPS für viele populäre Webseiten erzwingt (aber nicht für alle Webseiten, die HTTPS unterstützen).

Konzeptuell bietet die Verwendung von Regeln, die von Servern herunter geladen werden, einige Angriffsmöglichkeiten, die den Entwicklern von HTTPSEverywhere bewusst sind. Ein Angreifer könnte bösartige Regeln einfügen und z. B. *www.privacy-handbuch.de* auf die Seite *https://www.privacy-handbuch-boese.de* umleiten oder unauffälliger auf… Deshalb warnt HTTPSEverywhere vor Regelsätzen von Dritten (Abb: 10.7).

Aber sind die Regelsätze der Default Downloadserver der EFF.org vertrauenswürdig? Selbst wenn man der Qualität bei den Maintainern der Regelsätze vertraut, kann man nie

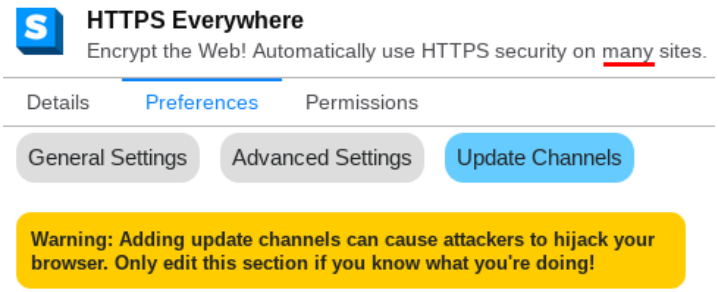


Abbildung 10.7: HTTPSEverywhere: Sicherheitswarnung vor Regelsätzen von Unbekannten

zu 100% ausschließen, dass ein Hacker an diesem Punkt ansetzt und etwas manipuliert...

Alternative: Seit Firefox 78.5 ESR funktioniert der HTTPS-only-Mode zufriedenstellend gut. Damit wird bei Eingabe URL eine Umschreibung auf HTTPS für alle Webseiten erzwungen, die TLS Verschlüsselung unterstützen. Außerdem wird mmixed contentäuf Webseiten, die via HTTPS geladen wurden, komplett blockiert. Wenn kein Upgrade auf eine HTTPS Verbindung möglich ist, wird eine Warnung angezeigt und man könnte die unverschlüsselte HTTP Seite trotzdem aufrufen, wenn man es wirklich will und das Risiko akzeptiert.

Man könnte daher das Add-on HTTPSEverywhere in der Add-on Verwaltung deaktivieren (also: deativieren(!) und nicht entfernen, sonst ist es nach dem nächsten Update vom TorBrowser wieder aktiv) und unter *about:config* folgende Optionen aktivieren:

```
dom.security.https_only_mode                    = true
security.mixed_content.upgrade_display_content = true
```

Ein Trackingdienst kann nicht erkennen, ob der Nutzer *https://www.privacy-handbuch.de* eingegeben hat oder ob die verkürzte Eingabe von *privacy-handbuch.de* durch den HTTPS-only-Mode umgeschrieben wurde. Aber es ergibt sich ein kleiner Unterschied zum Verhalten des originalen TorBrowsers, da die Entwickler bei TorProject.org entschieden haben, für *passive mixed content* (Bilder, CSS, Fonts...) auf HTTPS Webseiten kein Upgrade auf HTTPS zu versuchen und es nicht blockieren. Daraus ergibt sich aber kein individuelles Trackingmerkmal, da auch andere Nutzer diese Einstellungen nutzen.

AdBlocker und Trackingprotection

Der TorBrowser enthält keinen AdBlocker und alle Trackingprotection Features von Firefox sind vollständig deaktiviert. Es ist das Konzept vom TorBrowser, Werbung und Trackingscripte nicht zu blockieren sondern durch Anonymität die Privatspäre zu gewährleisten.

- Das Anonymitätskonzept des TorBrowser verhindert, dass Nutzer individuell erkannt und beim Surfen verfolgt werden können.
- Viele Webseiten finanzieren sich durch Werbung. TorProject.org möchte in diesem Punkt keine Konfrontation, um die Akzeptanz des Browsers nicht zu belasten.

Es ist empfehlenswert, dem Konzept von TorProject.org zu folgen. Ein AdBlocker ist leicht erkennbar und unterschiedliche Filterlisten können als Merkmal für das Fingerprinting dienen. Es ist nahzu unmöglich, eine Anonymitätsgruppe mit identischen Filterlisten aufzubauen.

Cookies und EverCookies

Um Tackingcookies und EverCookies muss man sich beim TorBrowser keine Gedanken machen. Das von den Entwicklern umgesetzte Sicherheitskonzept *Cross-Origin Identifier*

Unlinkability schützt zuverlässig gegen Tracking und Deanonymisierung mit Cookies oder EverCookies ohne das Surferlebnis nennenswert zu beeinträchtigen.

- Für jede aufgerufene Domain wird automatisch ein Surf-Container erstellt. Dieser Container enthält in einer abgeschotteten Umgebung alle Daten, die von einer Website lokal im Browser gespeichert werden (Cookies, HTML5-Storage, IndexedDB, Cache, TLS Sessions...). Diese Daten bilden dann den sogenannten *Context*.
- Der Zugriff auf Daten in einem anderen *Context* bzw. anderen Surf-Container ist nicht möglich. Somit werden in den verschiedenen *Contexten* unterschiedliche Tracking Markierungen gesetzt, wenn man unterschiedliche Domains aufruft.
- Beim Neustart oder wenn man den Menüpunkt *Neue Identität* der Zwiebel in der Toolbar wählt, werden alle Container gelöscht. Für eine *Neue Identität* wird außerdem eine neue Route durch das Tor Netzwerk mit einem anderen Tor Exit Node genutzt.

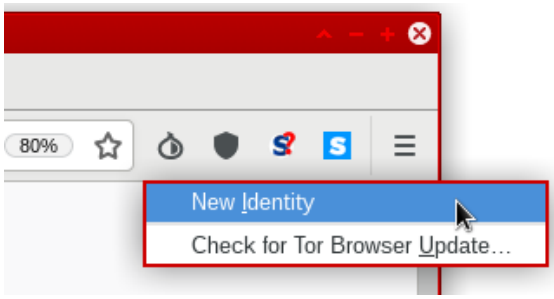


Abbildung 10.8: Neue Identät im TorBrowser wählen

Man sollte dem Anonymitätskonzept des TorBrowser folgen und gelegentlich alle Cookies und andere lokalen Daten löschen, indem man auf die Zwiebel neben der URL-Leiste klickt und *Neue Identität* wählt. Insbesondere nach einem Login auf einer Webseite ist es empfehlenswert, die Spuren zu beseitigen.

PDFs und andere Dokumente

Auf der Downloadseite des TorBrowserBundles findet man unten einige Sicherheitshinweise[17], unter anderem zu PDFs und anderen Dokumenten:

> ***Don't open documents downloaded through Tor while online***
>
> *You should be very careful when downloading documents via Tor (especially DOC and PDF files) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP!*
>
> ***If you must work with DOC and/or PDF files, we strongly recommend either using a disconnected computer**, downloading the free VirtualBox and using it with a virtual machine image with networking disabled, or using Tails.*

PDFs und andere Office Dokumente können Tracking Wanzen enthalten, die beim Öffnen des Dokumentes von einem Server geladen werden. Wenn man sie in einem PDF-Reader öffnet, während man online ist, dann kann man deanonymisiert werden. Standardmäßig öffnet TorBrowser PDFs im eigenen Viewer PDF.js. Damit sollte man zwar nicht deanonymisiert werden können, aber der Server kann zumindest das Öffnen des Dokumentes registrieren, auch nicht schön. Außerdem gibt es immer wieder Bug in Mozillas PDF.js, die für einen Exploit genutzt werden können (z. B. mfsa2015-69 vom Juli 2015).

[17] https://www.torproject.org/download/download

Um nicht immer daran denken zu müssen, mit der rechten Maustaste auf einen PDF-Link zu klicken und *Speichern unter...* zu wählen, kann man die Einstellung im TorBrowser für PDF-Dokumente zu ändern und auf *Speichern* setzen.

Die via Tor herunter geladenen Dokumente kann man in einem besonderen Ordner speichern. Dann behält man den Überblick und weiss, dass man diese Dokumente nur öffnen darf, wenn man den Netzwerkstecker gezogen hat oder die WLAN-Verbindung ausgeschaltet wurde.

Hinweis: Man kann eine PDF Datei von Wanzen säubern, indem man die heruntergeladenen Dateien auf einem Rechner ohne Internetverbindung in einem PDF-Viewer öffnet und in eine neue PDF-Datei ausdruckt. Dabei werden sichtbare Fotos neu gerendert und unsichtbar eingebettete Wanzen entfernt.

10.2.3 Tor Onion Services

Das Tor Netzwerk ermöglicht nicht nur den anonymen Zugriff auf herkömmliche Angebote im Web sondern auch die Bereitstellung anonymer, zensurresitenter und schwer lokalisierbarer Angebote auf den Tor-Nodes. Der Zugriff auf die Tor Hidden Services (Neu: Tor Onion Services) ist nur über das Tor Netzwerk möglich. Eine kryptische Adresse mit der Top-Level Domain .onion dient gleichzeitig als Hashwert für ein System von Schlüsseln, welches sicherstellt, dass der Nutzer auch wirklich mit dem gewünschten Dienst verbunden wird. Die vollständige Anonymisierung des Datenverkehrs stellt sicher, dass auch die Betreiber nur sehr schwer ermittelt werden können.

Es gibt zwei Versionen für Tor Onion Services:

Onion Services v2 werden derzeit standardmäßig verwendet. Diese Onion Service verwenden kryptografische Funktionen, die teilweise veraltet sind. Es wird SHA1 verwendet, DH-Schlüsseltausch und Public Key Kryptografie auf Basis RSA mit 1024 Bit langen Schlüsseln. Die Onion Adressen sind 16 Zeichen lang:

```
vwakviie2ienjx6t.onion
```

Onion Services v3 stehen ab Tor Version 3.2 zur Verfügung (Stable Release v3.2.9 Jan. 2018). Die Onion Services V3 verwenden aktuelle kryptografischen Funktionen (SHA3, ECDHE mit ed25519 und Public Key Kryptografie auf Basis elliptischer Kurven mit curve25519). Die Onion-Adressen sind mit 56 Zeichen wesentlich länger:

```
4acth47i6kxnvkewtm6q7ib2s3ufpo5sqbsnzjpbi7utijcltosqemad.onion
```

Für den Übergang sollten Administratoren beide Versionen der Onion Services für einen Dienst bereitstellen, um einen sanften Wechsel zu ermöglichen.

Tor Onion Services als sichere Alternative

Es gibt mehrere Angebote im normalen Web, die zusätzlich als Tor Hidden Service bzw. als Tor Onion Site anonym und unbeobachtet erreichbar sind. Wenn man Tor nutzt, sollte man diese Onion Services den normalen Webadressen vorziehen, da dann keine Gefahr durch Bad Tor Exit Nodes besteht.

- Die **Suchmaschine** *DuckDuckGo* ist auch als Tor Onion Site unter der Adresse http://3g2upl4pq6kufc4m.onion zu finden und die Suchmaschine Metager unter http://b7cxf4dkdsko6ah2.onion. Für Firefox gibt es bei Mycroft Add-ons für die Suchleiste, das diese Tor Onion Services nutzen.
- Die folgenden Webseiten können als Tor Onion Sites aufgerufen werden:
  - Invidio.us bietet einen tracking-freien Zugang zu Youtube Videos und ist unter der Onion Adresse kgg2m7yk5aybusll.onion erreichbar.

  - TorProject.org ist unter http://expyuzz4wqqyqhjn.onion erreichbar. Weitere Onion Sites von TorProject.org findet man auf der Übersichtsseite zu dem Thema: https://onion.torproject.org bzw. http://yz7lpwfhhzcdyc5y.onion.
  - Das Debian Projekt bietet eine Tor Onion Site für die Hauptseite unter http://sejnfjrq6szgca7v.onion und weitere Tor Onion Sites für einige Projekte an. Eine Übersicht findet man unter https://onion.debian.org bzw. http://5nca3wxl33tzlzj5.onion.
  - Wikileaks Submission Plattform ist unter http://wlupld3ptjvsgwqw.onion zu finden und einen sicheren Webchat unter http://wlchatc3pjwpli5r.onion.
  - Heise.de bietet einen sicheren Briefkasten auf Basis von Secure Drop für Tippgeber (sogenannte Whistleblower) unter http://sq4lecqyx4izcpkp.onion.
  - Das BKA (Bundeskriminalamt) bietet u.a. ein Kontaktformular und Fahndungsinformationen anonym unter http://h5zalmg25nhz3iqp.onion.
  - ...

- **Mastodon** als Twitter Alternative gibt es als Tor Onion Service bei:
  - Sergal.org unter http://izeljfc5nxetw7dm.onion oder als Onion Service v3:

    `5gdvpfoh6kb2iqbizb37lzk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion`

- Die folgenden **E-Mail Provider** bieten POP3, IMAP und SMTP als Tor Onion Service:
  - mailbox.org: unter kqiafglit242fygz.onion und als Onion Service v3 unter:

    `xy5d2mmnh6zjnroce4yk7njlkyafi7tkrameybxu43rgsg5ywhnelmad.onion`
  - Riseup.net: unter zsolxunfmbfuq7wf.onion[18] und als Onion Service v3 unter:

    `5gdvpfoh6kb2iqbizb37lzk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion`
  - ProtonMail ist unter als Onion Site erreichbar.

- Die folgenden **Jabber-Server** sind als Tor Onion Service erreichbar:
  - jabber-germany.de unter dbbrphko5tqcpar3.onion[19]
  - Mailbox.org unter kqiafglit242fygz.onion und als Onion Service v3 unter:

    `xy5d2mmnh6zjnroce4yk7njlkyafi7tkrameybxu43rgsg5ywhnelmad.onion`
  - systemli.org unter x5tno6mwkncu5m3h.onion[20]
  - Riseup.net unter 4cjw6cwpeaeppfqz.onion[21] und als Onion Service v3 unter:

    `jukrlvyhgguiedqswc5lehrag2fjunfktouuhi4wozxhb6heyzvshuyd.onion`
  - securejabber.me unter giyvshdnojeivkom.onion[22] und als Onion Service v3:

    `sidignlwz2odjhgcfhbueinmr23v5bubq2x43dskcebh5sbd2qrxtkid.onion`
  - jabber.otr.im unter 5rgdtlawqkcplz75.onion[23]
  - jabber.so36.net unter s4fgy24e2b5weqdb.onion[24]
  - creep.im unter creep7nissfumwyx.onion[25]
  - Draugr.de unter jfel5icoxf3nmftl.onion[26]

[18] https://help.riseup.net/en/tor
[19] https://www.jabber-germany.de
[20] https://www.systemli.org/en/service/xmpp.html
[21] https://help.riseup.net/en/tor
[22] https://securejabber.me
[23] https://www.otr.im/chat.html
[24] https://www.so36.net/services/xmpp
[25] https://creep.im
[26] https://www.draugr.de/neues/Tor_Hidden_Service

  - Trashserver.net unter m4c722bvc2r7brnn.onion[27]
  - Jabber.cat unter sybzodlxacch7st7.onion[28] und als Onion Service v3 unter:

    `7drfpncjeom3svqkyjitif26ezb3xvmtgyhgplcvqa7wwbb4qdbsjead.onion`
  - dismail.de unter l2epd2e4g2hx3tdf.onion[29] oder als Onion Service v3:

    `4colmnerbjz3xtsjmqogehtpbt5upjzef57huilibbq3wfgpsylub7yd.onion`
  - tchncs.de unter duvfmyqmdlyvc3mi.onion[30]

- Das **SILC-Netz** des CCC Dresden ist unter t3oisyiugzgvxph5.onion erreichbar.
- Das **Freenode IRC-Netzwerk** kann als Tor Onion Service unter der Adresse p4fsi4ockecnea7l.onion (Port: 6667) genutzt werden (nur mit registriertem Nick!)
- **HKP-Keyserver** für OpenPGP Schlüssel sind unter folgender Adresse erreichbar:

  `hkp://zkaan2xfbuxia2wpf7ofnkbz6r5zdbbvxbunvp5g2iebopbfc4iqmbad.onion`

Tor Onion Services für E-Mail Kommunikation

Für unbeobachtete Kommunikation gibt es folgenden Dienste, die ausschließlich aus Tor Hidden Service genutzt werden können:

- *Mail2Tor* ist ein weiterer E-Mail Dienst, der von Unbekannten als Tor Hidden Service unter der Adresse http://mail2tor2zyjdctd.onion betrieben wird. Accounts sind kostenlos, E-Mail können ebenfalls ins normale Internet gesendet und von dort empfangen werden.
- *TorBox* ist ein kostenfreier Hidden-only E-Mail Service und unter Adresse http://torbox3uiot6wchz.onion erreichbar. Es können keine E-Mails ins normale Internet gesendet oder von dort empfangen werden.

Hinweis: Einige Tor Hidden E-Mail Provider bieten ein Gateway ins normale Web, um E-Mails auch mit Nutzern aus dem normalen Internet austauschen zu können. Diese Gateways bieten aber nur eine schlechte TLS Konfiguration, die Transportverschlüsselung zu den Mailservern der normalen E-Mail Provider ist durchgehend sehr schlecht. Deshalb würde ich Tor Hidden Mail Provider nur für Kommunikation mit Onion-Adressen nutzen und für den Kontakt mit normalen E-Mail Adressen ein sicheren Provider aus dem normalen Netz.

Debian GNU/Linux Hidden Software Repository

Für Debian GNU/Linux gibt es einen Mirror der Repositories als Tor Hidden Service unter der Adresse *vwakviie2ienjx6t.onion*. Außerdem gibt es den Apt-Transport-Tor, der die Nutzung des Hidden Service mit den ganz normalen Tools zur Softwareverwaltung ermöglicht. Um die Software des Systems anonym und von Dritten unbeobachtet zu verwalten und zu aktualisieren ist ab Debian *jessie* nur das Paket *apt-transport-tor* zu installieren:

```
> sudo apt install apt-transport-tor
```

Anschließend editiert man die Datei */etc/apt/sources.list* und ersetzt die Server für Debian Paketquellen nach folgendem Muster:

[27] https://trashserver.net/technik
[28] https://jabber.cat/deutsch.html
[29] https://dismail.de/info.html
[30] https://tchncs.de/xmpp

```
deb tor+http://vwakviie2ienjx6t.onion/debian jessie
deb tor+http://vwakviie2ienjx6t.onion/debian jessie-updates main
deb tor+http://sgvtcaew4bxjd7ln.onion/debian-security jessie/updates main

# deb tor+http://vwakviie2ienjx6t.onion/debian jessie-backports main
```

Zukünftig nutzen alle Tools zur Softwareverwaltung (aptitude, Synaptic, KPackekit, ...) den Tor Hidden Service für die Installation und Aktualisierung der Software.

Neben Debian bietet natürlich auch TorProject.org das Repository für alle unterstützten Distributionen als Onion Site an. Um den tor Daemon regelmäßig zu aktualisieren, kann man folgendes Repository nutzen:

```
deb tor+http:://sdscoq7snqtznauu.onion/torproject.org <DISTRIBUTION> main
```

<DISTRIBUTION> ist dabei durch den Codenamen der Distribution zu ersetzen, den man mit dem folgenden Kommando ermitteln kann:

```
> lsb_release -c
Codename:  yakkety
```

Sonstiges

Ansonsten kenne ich kaum etwas, dass ich weiterempfehlen möchte. Meine "Sammlung" an reinen Tor Hidden Services enthält:

- 34x Angebote, die kinderpornografischen Schmutz zum Download anbieten (ausschließlich und teilweise zusätzlich zu anderen Inhalten). Das BKA hat eine etwas umfangreichere Liste mit 545 Seiten (Stand: 2012).[31]
- 3x Angebote zum Thema *Rent a Killer*. Ein Auftragsmord kostet offenbar nur 20.000 Dollar (wenn diese Angebote echt sind).
- Ein Angebot für gefakete Ausweisdokumente (aufgrund der mit Photoshop o.ä. bearbeiteten Screenshots der Beispieldokumente auf der Webseite halte ich das Angebot selbst für einen Fake).
- Mehrere Handelsplattformen für Drogen. (Das FBI kannte über 400 Plattformen zu diesem Thema.)
- Einige gähnend langweilige Foren & Blogs mit 2-3 Beiträgen pro Monat.
- Einige Index-Seiten mit Listen für verfügbare Hidden Services wie das legendäre *HiddenWiki* oder das neuere *TorDirectory*. In diesen Index Listen findet man massenweise Verweise auf Angebote mit Bezeichnungen wie *TorPedo*, *PedoVideoUpload*, *PedoImages*. Nach Beobachtung von ANONYMOUS sollen 70% der Besucher des *HiddenWiki* die Adult Section aufsuchen, wo dieses Schmutzzeug verlinkt ist.

In dem Paper *Cryptopolitik and the Darknet* (2016) haben sich die Autoren D. Moore und T. Rid empirisch mit den Tor Onion Sites beschäftigt. Von den 2723 besuchten Onion Sites waren 1547 Onion Sites auf kriminelle, illegale Aktivitäten ausgerichtet.[32]

Fake Onion Sites

Für Tor Onion Sites gibt es kein Vertrauens- oder Reputationsmodell. Es ist unbekannt, wer einen Tor Hidden Services betreibt und es ist damit sehr einfach, Honeypots aufzusetzen. Die kryptischen Adressen sind nur schwer verifizierbar. Das Problem von *Anonymität und Reputation* ist im Kapitel *Nachdenken* ausführlicher beschrieben.

[31] http://heise.de/-2124930
[32] http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085

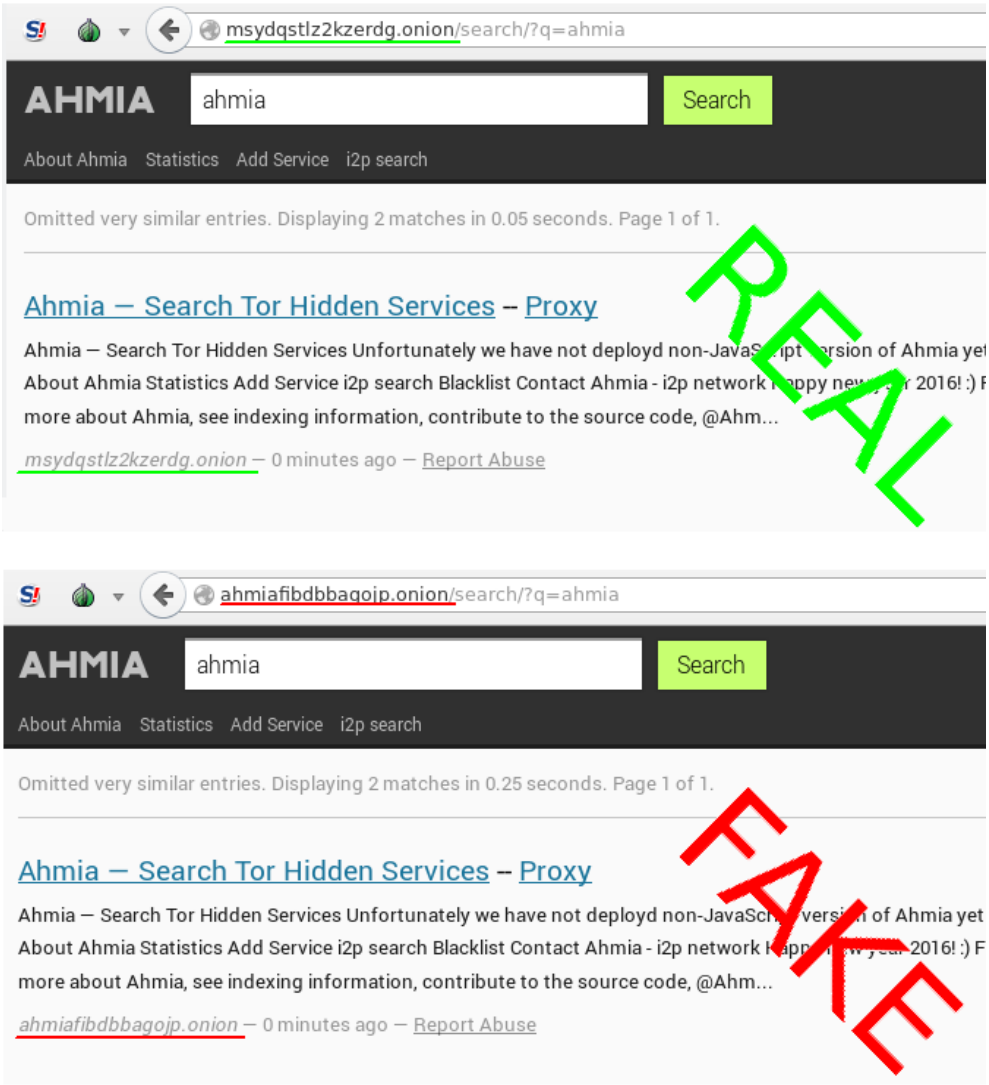


Abbildung 10.9: Original und Fake Onion Site der Suchmaschine Ahmia.fi

Juha Nurmi (Betreiber der Hidden Service Suchmaschine Ahmia.fi) veröffentlichte bereits zwei Warnungen im Juni 2015[33] und Januar 2016[34] mit 300 Fake Onion Sites, die den originalen Onion Sites täuschend ähnlich sehen. Diese Fake Sites leiten des Traffic der originalen Sites durch, modifizieren die Daten geringfühig oder erschnüffeln Login Credentials.

Auch Suchmaschinen mit Hidden Service Adressen wie DuckDuckGo (Tor) und Ahmia.fi waren betroffen, wie die Sceenshots in Bild 10.9 zeigen. Die Fake Site sieht dem Original täuschend ähnlich, die Besucher werden mit den Suchergebnissen aber auf andere Fake Onion Sites gelenkt.

Teilweise sind die Adressen der Fake Sites den Originalen sehr ähnlich:

```
REAL: http://torlinkbgs6aabns.onion
FAKE: http://torlinksb7apugxr.onion

REAL: http://valhallaxmn3fydu.onion
FAKE: http://valhalla4qb6qccm.onion
```

[33] https://lists.torproject.org/pipermail/tor-talk/2015-June/038295.html
[34] https://lists.torproject.org/pipermail/tor-talk/2016-January/040038.html

```
REAL: http://vendor7zqdpty4oo.onion
FAKE: http://vendor7eewu66mcc.onion
```

Schlussfolgerung: Man sollte den kryptischen Hidden Service Adressen nur vertrauen, wenn man sie aus einer vertrauenswürdigen, verifizierten Quelle bekommt. Die Ergebnislisten einer Suchmaschine für Onion Sites sind dabei nur begrenzt zuverlässig, da die Betreiber der Fake Onion Sites natürlich auch SEO-Techniken nutzen, um vor den Orginalen platziert zu werden.

10.2.4 Anonyme E-Mail Accounts

Es ist wenig sinnvoll, einen bisher ganz normal genutzten E-Mail Account plötzlich anonym zu nutzen. Es haben sich in den letzten Monaten genug Daten angesammelt, die die Identifizierung des Nutzers ermöglichen. Der erste Schritt sollte also die Einrichtung eines neuen E-Mail Accounts sein, der ausschließlich via Tor Onion Router genutzt wird.

Dieser neue E-Mail Account sollte NICHT für den tagtäglichen E-Mail Kleinkram genutzt werden sondern nur für eine bestimmte Aufgabe, die Anonymität erfordert. Anhand der Kommunikationdaten ist anderenfalls eine Deanonymisierung möglich, beispw. wenn die Bank oder ein Onlinehändler E-Mails mit der vollen Anrede und Adresse senden. Anonyme Kommunikation und Alltagskommunikation sollten immer streng getrennt sein.

Bei der anonymen Nutzung von E-Mail Accounts sind bestehen zwei Anforderungen:

1. Anonymität: Es dürfen keine Lücken bei Anonymisierung bestehen.
2. Sicherheit: Verschlüsselung mit OpenPGP sollte möglich sein.

Derzeit gibt es keinen E-Mail Client, der für die Nutzung mit Tor von TorProject.org überprüft und für gut befunden wurde. Die eigenmächtigen Nutzung einer Anwendung mit Tor als SOCKS5 Proxy ohne qualifizierte Prüfung durch Experten ist nicht ratsam, wie Thunderbird oder diverse Jabber Clients zeigen. Anonymität ist damit nicht gesichert.

Mit dem TorBrowser das Webinterface des E-Mail Providers nutzen

Eine Alternative ist die Nutzung des Webinterfaces eines E-Mail Providers mit dem TorBrowser. Dabei sollte der E-Mail Provider einen Tor Onion Service anbieten oder vergleichbare Lösungen, um die Gefahren durch Bad Exit Nodes zu reduzieren.

Die Verwendung eines Browsers erschwert die Verschlüsselung der E-Mails mit OpenPGP. Man könnte irgendwie versuchen, die Inhalte der E-Mails mit Copy/Paste zu verschlüsseln und entschlüsseln, wie bei Webformularen beschrieben, aber das macht kein Spaß. Besser wäre es, wenn der E-Mail Provider OpenPGP im Webinterface unterstützt.

Die im Kapitel E-Mail allgm. empfohlene Nutzung von POP3 zum Abrufen der E-Mail und lokale Speicherung ist damit unmöglich. Die Mails müssen auf dem Server des Providers verwaltet werden und sollten daher möglichst verschlüsselt gespeichert werden.

Da die GUIs der Mailprovider sehr intensiv mit Javascript arbeiten, muss man den mittleren Sicherheitslevel *Safer* im TorBrowser aktivieren, damit alles funktioniert.

- **Empfehlung:** ProtonMail bietet mit https://protonirockerxow.onion einen Tor Onion Service, Verschlüsselung mit OpenPGP im Webinterface und verschlüsselte Speicherung von E-Mails und Adressbuch. Man kann kostenfreie Accounts nutzen.
- Mit kleinen Einschränkungen könnte man auch mailbox.org für die anonyme Nutzung mit dem TorBrowser empfehlen, wenn man die angebotenen Features aktiviert:

  - Der Tor Node von mailbox.org kann ähnlich wie ein Onion Service mittels MapAddress Konfiguration verwendet werden. Im Installationsverzeichnis des TorBrowsers die Datei "Browser/TorBrowser/Data/Tor/torrcmmit einem Texteditor öffnen und folgende Einträge am Ende hinzufügen:

    ```
    MapAddress mailbox.org mailbox.org.85D4088148B1A6954C9BFFFCA010E85E0AA88FF0.exit
    MapAddress *.mailbox.org *.mailbox.org.85D4088148B1A6954C9BFFFCA010E85E0AA88FF0.exi
    ```

  - OpenPGP Verschlüsselung kann im Webinterface aktiviert werden. Allerdings ist mailbox.org Guard nicht für hohe Sicherheitsanforderungen geeignet sondern bietet nur hinreichende Sicherheit, wie mailbox.org in den FAQ schreibt.
  - Das verschlüsselte Postfach sorgt für die verschlüsselte Speicherung der E-Mail Inhalte auf dem Server. Das Feature muss in den Einstellungen aktiviert werden.
  - Ein verschlüsseltes Adressbuch gibt es nicht. Deshalb sollte die man die automatische Sammlung von Adressen in den Einstellungen deaktivieren. Die Optionen findet man in den Einstellungen unter *Email*.
  - Anonyme Bezahlung ist per Cash (Brief oder Überweisung) möglich.

- Es gibt weitere E-Mail Provider, die die Voraussetzungen erfüllen. Die Liste ist nicht abschließend sondern soll einige Hinweisen geben, worauf man achten kann.

Thunderbird 68.x und Tor Onion Router???

Thunderbird 68.x ist nicht für anonyme E-Mails geeignet. Das Add-on TorBirdy ist nicht kompatibel mit Thunderbird 68+ und niemand hat die Gefahren der neuen Features von Thunderbird 68.x in Kombination mit Tor Onion Router analysiert, siehe Bugticket 31341.

> *Alas, I think it might be a while until torbirdy gets an update – it involves somebody looking at Thunderbird 68 to see what new privacy invasive problems they put into it.*

Man kann in Thunderbird einen Proxy verwenden und die nötigen Einstellungen für Tor Onion Router eintragen, aber das reicht nicht. Eine Sicherheitsanalyse der Features von Thunderbird 2011zevon igte einige Gefahren auf, die zur Deanonymisierung führen können. Mit dem Add-on TorBirdy, das maßgeblich von Jacob Appelbaum initiert wurde, konnten diese Risiken gebannt werden. Für Thunderbird 68.x wäre eine neue Analyse nötig und eine neue, angepasste Version des Add-on TorBirdy, die es nicht gibt.

E-Mail Accounts mit der Tor Live-DVD TAILS verwalten

Die Tor Live-DVD TAILS ermöglicht die Verwendung von Thunderbird zur Verwaltung anonymer E-Mail Accounts. Die Live-DVD enthält einen modifizierten Thunderbird, der die Features von dem Add-on TorBirdy umsetzt, das seit einiger Zeit nicht mehr weiterentwickelt und nicht an aktuelle Thunderbird Versionen angepasst wird. Außerdem verhindert das Sicherheitskonzept von TAILS Verbindungen ins Netz, die nicht via Tor anonymisiert werden.

Da man Thunderbird nicht bei jedem Start der Live-DVD neu konfigurieren möchte, sollte man die persistente Speicherung der Daten von Thunderbird und GnuPG aktivieren.

1. Zuerst ist der persistente Speicher zu erstellen und zu konfigurieren, so dass die Daten von Thunderbird und GnuPG in dem verschlüsselten Speicher abgelegt werden.

   Den Konfigurator startet man unter **Anwendungen -> TAILS -> Persistenten Speicher**. Es ist ein Passwort für die Verschlüsselung anzugeben und auf den Button **Erstellen** zu klicken. Es wird der freie Platz auf dem TAILS Boot Medium für einen verschlüsselten Container zum Speichern der Daten genutzt.

2. Dann ist die Live-DVD neu zu starten und im Boot Greeter ist der persistente Speicher einzubinden. Dafür ist die Eigabe des Passwortes nötig.

3. Danach kann man Thunderbird starten und den E-Mail Account einrichten.

4. Als E-Mail Provider sind jene zu bevorzugen, die Tor Onion Services für IMAP, POP3 und SMTP anbieten, um die Gefahr durch bösartige Tor Exit Nodes zu minimieren.

E-Mail Accounts mit Whonix verwalten

Whonix ist ein System, das aus zwei virtuellen Computern (VMs) besteht. In der Arbeits-VM sind diverse Internetprogramme installiert und in der zweiten Tor-VM läuft Tor Onion Router. Die Arbeits-VM sendet den gesamten Datenverkehr an die Tor-VM. Von dort wird alles durch das Tor Netzwerk geleitet und anonymisiert.

Die Entwickler empfehlen die Nutzung des TorBrowsers, um E-Mail die Kommunikation im Webinterface eines E-Mail Providers zu verwalten.

Whonix enthält aber auch einen unmodifizierten Thunderbird. Das Konzept von Whonix verhindert, das man durch die vorhandenen Bugs in Thunderbird anhand der IP-Adresse deanonymisiert wird. In Kombination mit einer privacy-freundlichen Konfiguration, wie sie hier im Handbuch für Thunderbird empfohlen wird, könnte man den Thunderbird in Whonix ebenfalls zu Verwaltung von E-Mail Accounts nutzen. Vorteil ist die höhere Sicherheit bei OpenPGP und die Möglichkeit POP3 statt IMAP zu verwenden.

Spam-Blacklisten

Viele große E-Mail Provider sperren Tor-Nodes bei der Versendung von E-Mails via SMTP aus. Sie nutzen Spam-Blacklisten, in denen Tor-Relays häufig als "potentiell mit Bots infiziert" eingestuft sind. Wenn der E-Mail Provider eine dieser DNSBL nutzt, sieht man als Anwender von Tor nur eine Fehlermeldung beim Senden von Mails. Der Empfang funktioniert in der Regel reibungslos.

Um diese Probleme zu vermeiden, sollte man einen privacy-freundlichen E-Mail Provider nutzen, der Sender-IPs aus dem Header der versendeten E-Mails entfernt.

GoogleMail und Anonymisierungsdienste

GoogleMail (oder GMail) mag eine anonyme Nutzung der kostenfreien Accounts nicht. Kurz zusammengefasst kann man sagen, dass Google entweder eine IP-Adresse der Nutzer haben möchte oder die Telefonnummer. Stellungnahme des *Google account security team* zu einer Anfrage der Tor Community:

> *Hello,*
>
> *I work for Google as TL of the account security system that is blocking your access.*
>
> *Access to Google accounts via Tor (or any anonymizing proxy service) is not allowed unless you have established a track record of using those services beforehand. You have several ways to do that:*
>
> *1) With Tor active, log in via the web and answer a security quiz, if any is presented. You may need to receive a code on your phone. If you don't have a phone number on the account the access may be denied.*
>
> *2) Log in via the web without Tor, then activate Tor and log in again WITHOUT clearing cookies. The GAPS cookie on your browser is a large random number that acts as a second factor and will whitelist your access.*
>
> *Once we see that your account has a track record of being successfully accessed via Tor the security checks are relaxed and you should be able to use TorBirdy.*

Hope that helps,
Google account security team

Außerdem werden nach einem Bericht von Wired [35] zukünftig alle E-Mails der GMail Accounts in das NSA-Datacenter in Bluffdale kopiert.

10.2.5 Anonym Bloggen

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

Die einfachste Variante:

- Man braucht einen anonymen Browser, am besten das TorBrowserBundle. Gut geeignet ist beispielsweise TAILS, da diese neben einem fertig konfigurierten Browser für anonymes Surfen auch die nötigen Tools zur Anonymisierung von Bildern und Dokumenten enthalten und keine Spuren auf dem PC hinterlassen.

- Man braucht eine anonyme E-Mail Adresse, die nur in Zusammenhang mit dem Blog verwendet wird (für die Registrierung und als Kontaktadresse). Dabei ist es nicht nötig, einen E-Mail Client zu konfigurieren. Man kann die E-Mails im Webinterface des Providers mit dem TorBrowser lesen.

- Man braucht einen Bloghoster, der anonyme Registrierung oder Registrierung mit Fake-Daten ermöglicht und anonym z. B. mit Paysafecard bezahlt werden kann.

  Wordpress.com ist empfehlenswert oder die kostenfreie Variante von *Twoday.net*. Für politische Aktivitäten ist der Bloghoster *blackblogs.org* geeignet. Um ein Blog bei diesem Hoster zu eröffnen, benötigt man eine E-Mail Adresse von einem Technik Kollektiv. Auf der Policy Seite von blackblogs.org[36] findet man eine die Liste von akzeptierten E-Mail Providern. Diese E-Mail Provider bieten kostenlose Postfächer für politische Aktivisten. Um ein Postfach zu erstellen, muss man seine Gründe darlegen, aber man muss seine Identität nicht aufdecken.

- Registrierung und Verwaltung des Blogs sowie das Schreiben von Artikeln können komplett im Browser durchgeführt werden. Dabei ist stets der Anonymisierungsdienst zu nutzen. Man sollte darauf achten, dass man nicht hektisch unter Zeitdruck schnell mal einen Beitrag verfasst. Dabei können Fehler passieren.

- Im Blog veröffentlichte Bilder und Dokumente sind stets vor dem Upload zu anonymisieren. Vor allem Bilder von Digitalkameras enthalten eine Vielzahl von Informationen, die zur Deanonymisierung führen können. Fotos von Freunden oder Bekannten sollte man nicht veröffentlichen, da durch Freundschaftsbeziehungen eine Deanonymisierung möglich ist.

- Jede Blogsoftware bietet die Möglichkeit, den Zeitpunkt der Veröffentlichung von neuen Artikeln festzulegen. Das sollte man nutzen und neue Artikel nicht sofort veröffentlichen sondern einige Stunden später freigeben, wenn man nicht online ist.

- Stilometrie (Deanonymisierung anhand des Schreibstils) ist inzwischen fester Bestandteil geheimdienstlicher Arbeit. Es ist mit (teil-) automatisierten Verfahren möglich, anonyme Texte einem Autor zuzuordnen, wenn der Kreis der Verdächtigen eingeschränkt ist und genügend Textproben der Verdächtigen vorliegen. Mit Ruhe und Konzentration beim Verfassen von Blogartikeln ist es möglich, seinen individuellen Schreibstil zu verstellen und stilometrische Angriffe zu erschweren.

[35] http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1
[36] https://blackblogs.org/policy/

10.2.6 Anonymes Instant-Messaging

Verschlüsselte Chats und Instant Messaging in Kombination mit Anonymisierunsgdiensten wie Tor sind auch für potente Geheimdienste wie die NSA ein Alptraum. Es gibt keine Metadaten, OTR-Verschlüsselung kann noch nicht gebrochen werden und eine Zuordnung von Traffic zu IP-Adressen wird durch die Anonymisierungsdienste verhindert.

Leider gibt es nur wenige Messenger, die für die Kombination mit Tor geeignet sind:

- Populäre Messenger, die eine Telefonnummer und ein Smartphone für den Hauptaccount erfordern, sind natürlich ungeeignet (trivial).
- Messenger, die Interactive Connection Establishment (ICE) für Audio- und Videochats verwenden, sind auf PCs/Laptops ebenfalls ungeeigent, weil ICE aggresiv versucht, eine Peer-2-Peer Verbindung mit oder ohne Proxy herzustellen und dabei die eigene IP-Adresse dem Kommunikationspartner mitteilt und via UPnP ein Loch in den Router bohren will. Somit kann ein Anruf zur Deanonymisierung führen.

  ICE ist Bestandteil von WebRTC und der libjingle (XMPP, WhatsApp).
- DNS Leaks sind ein häufiges Problem bei Messenger, die nicht ausdrücklich für die Nutzung via Tor Onion Router vorbereitet wurden.

Folgende Anwendungen können für Instant Messaging via Tor genutzt werden:

Briar (nur Android) bringt Tor bereits mit und ist für anonyme Nutzung optimiert.

qTox (PCs/Laptops) bzw. der **TRIfA** Tox Client für Andoid können mit Tor genutzt werden, weil das Protokoll keine verräterischen Informationen überträgt.

Dabei ist darauf zu achten, dass der anonyme genutzte Account erst dann angelegt wird, wenn der Proxy via Tor konfiguriert wurde. Evtl. muss man zuerst einen Dummy Account erstellen, damit man die Einstellungen modifizieren kann und danach den richtigen Account.

UDP und IPv6 Support sind entgegen der Empfehlung bei der Konfiguration von Tor als Proxy zu deaktivieren, da beides von Tor nicht unterstützt wird (Abb: 10.10).

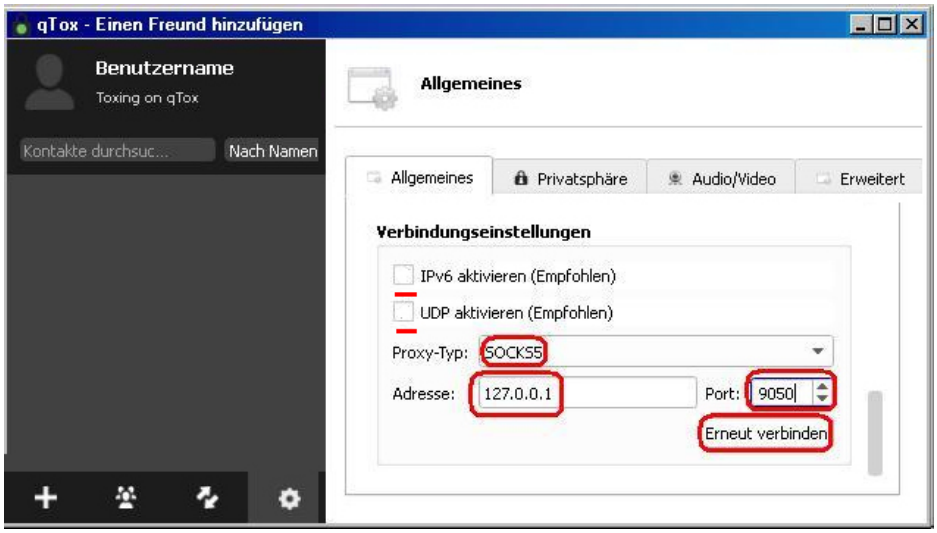


Abbildung 10.10: qTox Proxy Konfiguration für Tor Onion Router

Jabber/XMPP mit Tor zu verwenden, war vor einige Jahren populär. Der XMPP Client muss dabei folgende Anforderungen erfüllen:

1. Es muss ein SOCKS5 Proxy mit Remote DNS Resolving (ohne DNS-Leaks) konfigurierbar sein, um die Daten durch den Anonymisierungsdienst zu schicken.
2. Die Tor Hidden Service Adresse des Jabber Servers muss als *Verbindungsserver* konfigurierbar sein. Wenn Tor Onion Router genutzt wird, empfehlen wir nachdrücklich die Jabber/XMPP Server, die eine Tor Hidden Service Adresse anbieten. Damit vermeidet Gefahren durch bösartige Tor Exit Nodes. Angriffe von bösartigen Tor Exit Nodes auf Jabber/XMPP wurden bereits nachgewiesen.
3. Audio- und Video-Chats mit der *libjingle* dürfen nicht verfügbar bzw. müssen deaktivierbar sein. Audio- und Video-Chats sind nicht via Anonymisierungsdienst möglich. Bei Einladung zu einem Video-Chat versucht das integrierte *Interactive Connectivity Establishment* (ICE) der *libjingle* automatisch, eine Verbindung mit oder ohne Proxy herzustellen, das ist kein Bug sondern ein Feature der ICE Spezifikation. Nutzer können damit deanonymisiert werden.
4. Weitere XMPP Erweiterungen wie z.B. Jingle Dateitransfer können von einem Angreifer unter Umständen auch zur Deanonymisierung genutzt werden.

TorProject.org empfiehlt *CoyIM* für Jabber/XMPP. Dieser Client bietet nur Textchats mit OTR-Verschlüsselung und vermeidet durch Reduktion der Features Probleme bei der Anonymisierung, wie sie mit anderen Jabber/XMPP Clients auftreten.

Allerdings ist OTR als Ende-zu-Ende Verschlüsselung nicht kompatibel mit den meisten anderen Jabber/XMPP Clients, die OMEMO bevorzugen.

10.2.7 Dateien anonym tauschen via Tor

OnionShare[37] ist ein kleines Tool, um in Kombination mit dem TorBrowserBundle Dateien zu tauschen. Es ist eine ideale Ergänzung zu TorMessenger oder Ricochet, denen die Möglichkeit zum Tauschen von Dateien (noch) fehlt.

1. Der Absender benötigt OnionShare und den Tor Daemon des TorBrowserBundles, um die Dateien zum Download bereitzustellen. OnionShare stellt einen Tor Hidden Service bereit, unter dem die Dateien abgerufen werden können.
2. Der oder die Empfänger benötigen nur den TorBrowser, um die bereitgestellten Dateien herunter zu laden. Den Link zum Download bekommen die Empfänger über einen anderen sicheren Kanal, z. B. via TorMessenger oder Ricochet.

Installation von OnionShare:

- Für Windows und MacOS stehen auf der Download Website Setup Dateien zur Installation bereit.
- In den Linux Distributionen Unbuntu und Fedora ist Onionshare enthalten und kann mit dem bevorzugten Tool zur Softwareverwaltung installiert werden.
- Für alle anderen Linux Distributionen muss man OnionShare selbst compileren. Eine Anleitung findet man auf der Webseite.

Nach dem Start von OnionShare kann man im Hauptfenter Dateien zur Liste der gesharten Dateien hinzufügen und den Service starten. Der Tor Daemon des TorBrowserBundle wird genutzt, um den Hidden Service bereitzustellen, das TorBrowserBundle muss also gestartet werden, bevor man die Dateien zum Download freigeben kann.

Wenn die Option *Den Server automatisch anhalten* aktiviert, dann wird der Tor Hidden Service nach dem ersten erfolgreichen Download sofort wieder beendet. Das ist ein Sicherheitsfeature, da es im Tor Netz auch bösartige Nodes gibt, die neue Tor Hidden Services testen und teilweise auch angreifen.[38]

[37] https://onionshare.org
[38] https://www.schneier.com/blog/archives/2016/07/researchers_dis.html

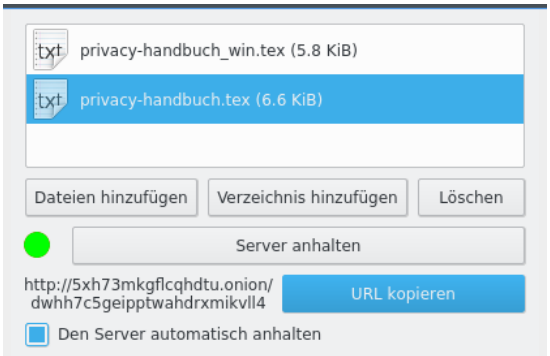


Abbildung 10.11: OnionShare Hauptfenster

Wenn der Service erfolgreich gestartet ist, kann man die Tor Onion URL in die Zwischenablage kopieren und an den oder die Empfänger schicken, am besten via Instant Messenger. Der oder die Empfänger können die Adresse dann im TorBrowser aufrufen und die bereitgestellten Dateien als ZIP-Archiv herunter laden.

1-Click-Hoster

1-Click-Hoster sind eine weitere mögliche Alternative. Mit dem TorBrowserBundle kann man anonym Datieen bei einem 1-Click-Hoster hochladen und den Download-Link veteilen.

- Auf diesen Hostern sind die Uploads nur eine begrenzte Zeit verfügbar (1-4 Wochen):
  - https://1fichier.com (Uploads werden nach 15 Tagen gelöscht)
  - https://www.transferbigfiles.com (bis zu 20GB für registierte Nutzer
  - https://www.filefactory.com (benötigt Javascript und eine E-Mail Addr.)
- Für Langzeit-Hosting kann man folgende Dienste verwenden:
  - https://nofile.io (Verschlüsselung möglich - BETA)
  - https://www.mediafire.com (Registrierung für Uploads nötig)

BitTorrent über einen Anonymisierungsdienst ???

Die naheliegende Variante ist es, BitTorrent über einen Anonymisierungsdienst wie Tor zu nutzen, um die eigene IP-Adresse zu verstecken. Das funktioniert nur begrenzt. Das BitTorrent-Protokoll überträgt die IP-Adresse des Clients auch im Header der Daten und es ist relativ einfach möglich, die Teilnehmer zu 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 [39].

Anonyme Peer-2-Peer Netze

Einige Projekte für anonymes, unbeobachtetes Filesharing:

- **I2P Snark:** Das Invisible Internet Project bietet anonymes Filesharing innerhalb des Netzes. Eine kurze Einführung findet man im Kapitel zum Invisible Internet.
- **GNUnet:** bietet anonymes, zensurresistentes Filesharing ohne zentrale Server. Alle Teilnehmer leiten Daten für andere Teilnehmer weiter und stellen selbst Dateien bereit. Da weitergeleitete Daten nicht von Daten unterscheidbar sind, die von einem

[39] https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea

Teilnehmer selbst stammen, ergibt sich eine hohe Anonymität. Es ist ein echtes GNU-Projekt (bitte nicht mit Gnutella verwechseln). Weitere Informationen auf der Projektwebsite https://gnunet.org.

10.2.8 Tor Bad Exit Nodes

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

Durch einfaches Beschnüffeln wird die Anonymität des Nutzers nicht zwangsläufig kompromittiert, es werden meist Inhalte mitgelesen, die im Web schon verfügbar sind. Erst wenn Login-Daten unverschlüsselt übertragen werden oder man-in-the-middle Angriffe erfolgreich sind, können die Bad Exit Nodes an persönliche Informationen gelangen. Persönliche Daten, bspw. Login Daten für einen Mail- oder Bank-Account, sollten nur über SSL- oder TLS-gesicherte Verbindungen übertragen werden. Bei SSL-Fehlern sollte die Verbindung abgebrochen werden. Das gilt für Surfen via Tor wie auch im normalen Web.

Einige Beispiele für Bad Exits:

1. Die folgenden Nodes wurde dabei erwischt, den Exit Traffic zu modifizieren und JavaScript in abgerufene Websites einzuschmuggeln. Dabei handelte es sich zumeist um Werbung oder Redirects auf andere Seiten. Diese Bad Exit Nodes sind schon lange nicht mehr online, die Liste ist nur als Beispiel gedacht.

`apple`	`$232986CD960556CD8053CBEC47C189082B34EF09`
`CorryL`	`$3163a22dc3849042f2416a785eaeebfeea10cc48`
`tortila`	`$acc9d3a6f5ffcda67ff96efc579a001339422687`
`whistlersmother`	`$e413c4ed688de25a4b69edf9be743f88a2d083be`
`BlueMoon`	`$d51cf2e4e65fd58f2381c53ce3df67795df86fca`
`TRHCourtney1..10`	`$F7D6E31D8AF52FA0E7BB330BB5BBA15F30BC8D48`
	`$AA254D3E276178DB8D955AD93602097AD802B986`
	`$F650611B117B575E0CF55B5EFBB065B170CBE0F1`
	`$ECA7112A29A0880392689A4A1B890E8692890E62`
	`$47AB3A1C3A262C3FE8D745BBF95E79D1C7C6DE77`
	`$0F07C4FFE25673EF6C94C1B11E88F138793FEA56`
	`$0FE669B59C602C37D874CF74AFEA42E3AA8B62C6`
	`$E0C518A71F4ED5AEE92E980256CD2FAB4D9EEC59`
	`$77DF35BBCDC2CD7DB17026FB60724A83A5D05827`
	`$BC75DFAC9E807FE9B0A43B8D11F46DB97964AC11`
`Unnamed`	`$05842ce44d5d12cc9d9598f5583b12537dd7158a`
	`$f36a9830dcf35944b8abb235da29a9bbded541bc`
	`$9ee320d0844b6563bef4ae7f715fe633f5ffdba5`
	`$c59538ea8a4c053b82746a3920aa4f1916865756`
	`$0326d8412f874256536730e15f9bbda54c93738d`
	`$86b73eef87f3bf6e02193c6f502d68db7cd58128`

2. Die folgenden Nodes wurden bei dem Versuch erwischt, SSL-Zertifikate zu fälschen, um den verschlüsselten Traffic mitlesen zu können:

   (a) *LateNightZ* war ein deutscher Tor Node, der 2007 beim man-in-the-middle Anriff auf die SSL-Verschlüsselung erwischt wurde.[40]

   (b) *ling* war ein chinesischer Tor Node, der im Frühjahr 2008 versuchte, mit gefälschten SSL-Zertifikaten die Daten von Nutzern zu ermitteln. Gleichzeitig wurde in

[40] http://www.teamfurry.com/wordpress/2007/11/20/tor-exit-node-doing-mitm-attacks/

China eine modifizierte Version von Tor in Umlauf gebracht, die bevorzugt diesen Node nutzte. Die zeitliche Korrelation mit den Unruhen in Tibet ist sicher kein Zufall [41].

(c) Im Sept. 2012 wurden zwei russische Tor Nodes mit den IP-Adressen 46.30.42.153 und 46.30.42.154 beim SSL man-in-the-middle Angriff erwischt.

(d) Im April 2013 wurde der russische Tor Node mit der IP-Adresse 176.99.10.92 beim SSL man-in-the-middle Angriff auf Wikipedia und auf IMAPS erwischt [42].

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. Im Februar/März 2012 haben mehrere Exit-Nodes in einer konzertierten Aktion die HTTPS-Links in Webseiten durch HTTP-Links ersetzt. Wie man damit erfolgreich die SSL-Verschlüsselung ausgehebeln kann, wurde auf der Black Hack 2009 beschrieben. Die Software für diesen Angriff heisst *ssl-stripe* und ist als Open Source verfügbar.

`Bradiex`	`bcc93397b50c1ac75c94452954a5bcda01f47215`
	`IP: 89.208.192.83`
`TorRelay3A2FL`	`ee25656d71db9a82c8efd8c4a99ddbec89f24a67`
	`IP: 92.48.93.237`
`lolling`	`1f9803d6ade967718912622ac876feef1088cfaa`
	`IP: 178.76.250.194`
`Unnamed`	`486efad8aef3360c07877dbe7ba96bf22d304256`
	`IP: 219.90.126.61`
`idideditttheconfig`	`0450b15ffac9e310ab2a222adecfef35f4a65c23`
	`IP: 94.185.81.130`
`UnFilTerD`	`ffd2075cc29852c322e1984555cddfbc6fb1ee80`
	`IP: 82.95.57.4`

4. Im Oktober 2014 wurde ein Tor Exit Node aufgespürt, der Windows Binaries (z. B. DLLs oder EXE-Dateien) beim Download on-the-fly mit dem Trojaner OnionDuke infizierte, einer Variation der russischen Cyberwaffe MiniDuke. Der Trojaner sammelte Login Daten und spionierte die Netzwerkstruktur der Opfer aus. F-Secure konnten die ersten Infektionen mit OnionDuke auf Oktober 2013 datieren. Der Bad Exit Node wurde gefunden, weil ein Sicherheitsforscher gezielt nach diesem Angriff suchte.[43]

5. Im April 2015 wurden 70 Bad Tor Nodes identifiziert, die den Hidden E-Mail Service angegriffen hatten. Die Betreiber von SIGAINT warnen, dass es den Angreifern gelungen ist, den Hidden Service mit einem man-in-the-middle Angriff zu kompromittieren und möglicherweise Daten inklusive Login Credentials mitzulesen.[44]

> *I think we are being targeted by some agency here. That's a lot of exit nodes.* SIGAINT Admin

Diese 70 Tor Nodes meldeten sich innerhalb eines Monats kurz vor dem Angriff als neue Tor Nodes im Netzwerk an. 31 weitere Nodes stehen noch in dem Verdacht, ebenfalls zu dieser Gruppe zu gehören, aber noch nicht aktiv angegriffen zu haben.

6. Um passiv schnüffelnde Tor Exit Nodes in eine Falle tappen zu lassen, hat Chloe im Juni 2015 einen Honigtopf aufgestellt und 11 passiv schnüffelnde Exit Nodes aufgespürt. Zwei der elf Nodes hatten Guard Status.[45]

[41] http://archives.seul.org/or/talk/Mar-2008/msg00213.html
[42] https://trac.torproject.org/projects/tor/ticket/8657
[43] http://heise.de/-2457271
[44] https://lists.torproject.org/pipermail/tor-talk/2015-April/037549.html
[45] https://chloe.re/2015/06/20/a-month-with-badonions/

7. Im März 2016 haben 14 Bad Exit Nodes in einer konzertierten Aktion versucht, sich als man-in-the-middle in STARTTLS Verschlüsselung einiger Jabber/XMPP Server einzuschleichen.[46] Folgende Jabber Server waren von dem Angriff betroffen:

   - freifunk.im
   - jabber.ccc.de
   - jabber.systemli.org
   - jappix.org
   - jodo.im
   - pad7.de
   - swissjabber.ch
   - tigase.me

8. Tor Exit Nodes aus dem Iran sind generell als Bad Exits markiert. Diese Nodes unterliegen der iranischen Zensur. Außerdem wird beim Aufruf von Webseiten über diese Nodes von der staatlichen Firewall ein unsichtbarer IFrame aus dem Hidden Internet[47] of Iran eingefügt.

   ```
   <iframe src="http://10.10.34.34" style="width: 100%;
      height: 100%" scrolling="no" marginwidth="0"
      marginheight="0" frameborder="0" vspace="0" hspace="0">
   </iframe>
   ```

9. Die Unterlagen des Whistleblowers E. Snowden haben bestätigt, dass NSA und GCHQ passiv schnüffelnde Exit-Nodes betreiben. Die NSA soll damals 10-12 leistungsfähige Tor-Server genutzt haben (aktuelle Angriffe zeigen, dass es inzwischen deutlich mehr sind). Zum Engagement des GSHQ wurden keine Zahlen bekannt.

10. Europol betreibt seit Jahren ein Projekt mit dem Ziel *to provide operational intelligence related to TOR*. Die Formulierung lässt vermuten, dass ebenfalls passiv schnüffelnde Exit-Nodes genutzt werden.

10.2.9 Tor Good Exit Nodes

Im Abschnitt *Tor Bad Exits* sind einige Nodes genannt, denen man nicht trauen sollte. Diese Aufzählung kann nicht abschleißend und vollständig sein.

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

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

- Torservers.net ist eine vertrauenswürdige Organisation, die Exit-Nodes betreibt.
- Die von der Swiss Privacy Foundation betriebenen Server sammeln keine Informationen. Eine Liste der Server findet man unter:
  https://www.privacyfoundation.ch/de/service/server.html.

[46] https://tech.immerda.ch/2016/03/xmpp-man-in-the-middle-via-tor/
[47] http://arxiv.org/abs/1209.6398

- Der CCC betreibt zur Zeit acht Tor Nodes (siehe Liste im TorAtlas unter https://atlas.torproject.org/#search/chaoscomputerclub).
- Der Tor Node *Digitalcourage3ip1* wird vom Verein Digitalcourage e.V. betrieben.[48]
- Die Heinlein Support GmbH betreibt den Tor Node *mailboxorg* und empfiehlt die Konfiguration von MapAdresses in der torrc, so dass dieser Node als Exit Node für alle Mailbox.org Dienste genutzt wird.
- .... bitte selbst die Liste erweitern

Bei der Auswahl der Server sollte man nicht einfach nach dem Namen im TorStatus gehen. Jeder Admin kann seinem Server einen beliebigen Namen geben und den Anschein einer vertrauenswürdigen Organisation erwecken. Die Identität des Betreibers sollte verifiziert werden, beispielsweise durch Veröffentlichung auf einer Website.

Konfiguration in der torrc

In der Tor Konfigurationsdatei */etc/tor/torrc* bzw. für das TorBrowserBundle in *<TorBrowserBundleVerzeichnis>/Browser/TorBrowser/Data/Tor/torrc* kann man die gewünschten Nodes mit folgenden Optionen konfigurieren:

```
StrictExitNodes 1
ExitNodes $9BDF3EEA1D33AA58A2EEA9E6CA58FB8A667288FC,
          $1A1DA6B9F262699A87F9A4F24EF48B50148EB018,
          $31A993F413D01E68117F76247E4F242095190B87,
          $A07FF746D9BA56C3F916BBD404307396BFA862E0,
          $A3279B1AC705C9F3478947598CF0557B81E12DE1,
          $AB176BD65735A99DCCB7889184E62EF0B2E35751,
          $B7BE1D35762155FEB2BC9DAE0A157C706D738FE5,
          $85D4088148B1A6954C9BFFFCA010E85E0AA88FF0,
          $39659458160887CC8A46FAE627EE01EEDAAED07F,
          $0111BA9B604669E636FFD5B503F382A4B7AD6E80,
          $AD86CD1A49573D52A7B6F4A35750F161AAD89C88,
          $DC41244B158D1420C98C66F7B5E569C09DCE98FE,
          $B060482C784788B8A564DECD904E14CB305C8B38,
          $88487BDD980BF6E72092EE690E8C51C0AA4A538C,
          $95DA61AEF23A6C851028C1AA88AD8593F659E60F,
          $95DA61AEF23A6C851028C1AA88AD8593F659E60F,
          $487092BA36F4675F2312AA09AC0393D85DAD6145
```

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 und ist nur ein Beispiel. Für die praktische Nutzung ist sie viel zu klein, um eine hohe Anonymität zu gewährleisten.

[48] https://digitalcourage.de/support/tor

10.3 Finger weg von unseriösen Angeboten

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

10.3.1 Tor-Boxen

Sogenannte Tor-Boxen wie Anonabox oder SafePlug leiten als Router den gesamten Traffic eines Computers oder Heimnetzwerkes oder als Proxy nur den HTTP-Traffic durch Tor. Die Anbieter versprechen eine einfachste Installation und gleichzeitig die Anonymtät des Tor-Netzwerkes. Aber manchmal ist *Einfach* das Gegenteil von *Anonym*.

Anonymes Surfen erfordert in erster Linie eine sichere Browserkonfiguration. Wer mit einem beliebigen Browser (z. B. Internet Explorer, Google Chrome oder Safarie) ohne privacy-freundliche Konfiguration im Internet surft, der kann sich die Nutzung von Tor sparen, damit surft man nicht anonym. Die einzige, von den Tor-Entwicklern empfohlene Variante zum anonymen Surfen ist die Nutzung des TorBrowserBundle.

> *The most crucial problem with a torifying proxy is that it uses a bring-your-own-browser system, as opposed to a hardened browser, and therefore is susceptible to browser-based privacy leaks. This is why it's better to use the Tor Browser Bundle.*
> (Quelle: Blog TorProject.org)

10.3.2 Web-Proxys

Web-Proxys mit HTTPS-Verschlüsselung sind ein probates Mittel, um Zensur im Internet zu umgehen. Sie sind aber als Anonymisierungsdienste unbrauchbar. Mit kruden HTML-Elementen oder JavaScript ist es möglich, die meisten Web-Proxys auszutricksen und die reale IP-Adresse des Nutzers zu ermitteln.

Die folgende Tabelle zeigt eine Liste bekannter Webproxys, die den Anonymitätstest der JonDos GmbH nicht bestehen:

Betreiber	HTML/CSS	JavaScript	Java
Anonymouse	gebrochen	gebrochen	gebrochen
Cyberghost Web		gebrochen	gebrochen
Hide My Ass!		gebrochen	gebrochen
WebProxy.ca		gebrochen	gebrochen
KProxy		gebrochen	gebrochen
Guardster		gebrochen	gebrochen
Megaproxy	gebrochen	nicht verfügbar	nicht verfügbar
Proxify		gebrochen	gebrochen
Ebumna	gebrochen	gebrochen	gebrochen

Einige Webproxys erlauben es, JavaScript mit dem Aktivieren einer Option auf der Startseite zu blockieren. Es ist zwingend notwendig, diese Option zu aktivieren, da alle Webproxys mit Javascript ausgetrickst werden können! Außerdem sollte man JavaScript im Browser deaktivieren, damit keine Scripte in Bildern, Werbebannern o.ä. durch den Proxy geschmuggelt werden können.

CTunnel.com

CTunnel.com ist ein ganz besonderer Web-Proxy, der hier etwas ausführlicher behandelt werden soll. Man verspricht zwar eine anonyme Nutzung des Internet. Die Entwickler haben sich aber große Mühe gegeben, die Nutzung des Dienstes mit deaktiviertem JavaScript unmöglich zu machen. Der gesamte Inhalt der Website ist encoded und wird mit JavaScript geschrieben.

Die IP-Adressen der Nutzer werden bei aktiviertem JavaScript gleich an drei Datensammler verschickt. Neben Google Analytics erhalten auch xtendmedia.com und yieldmanager.com diese Information. Google Analytics ist bekannt, die beiden anderen Datensammler sind ebenfalls Anbieter von Werbung. Die Website enthält keinen Hinweis auf die Datenweitergabe. Zumindest im Fall von Google Analytics besteht jedoch eine Informationspflicht.

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

10.3.3 Free Hide IP

Free Hide IP wird von *Computerbild* als Anonymisierungsdienst angepriesen.

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

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

Als Tool zur Umgehung von Zensur ist der Dienst auch nicht geeignet. Die amerikanischen Proxy-Server setzen das Filtersystem *Barracuda* ein und es werden die Internetsperren des COICA-Zensurgesetzes umgesetzt.

10.3.4 ZenMate

ZenMate will ein VPN-artiger Anonymisierungsdienst sein, der eine einfach zu installierende Lösung für anonymes Surfen verspricht. Man muss auf der Webseite nur einmal kurz klicken, um einen Browser Add-on zu installieren. Es gibt eine kostenlose Version, die nur die IP-Adresse versteckt. Außerdem steht eine Premium Version zur Verfügung, die auch Tracking Elemente blockieren können soll.

Die kostenfreie Version hat Jens Kubiziel schon 2014 getestet. Das Ergebnis kann man einfach zusammenfassen: es funktioniert nicht zuverlässig.Insbesondere wenn man ZenMate zur Umgehung regionaler IP-Sperren verwenden möchte, um Videos zu schauen, die im eigenen Land nicht verfügbar sind, funktioniert die IP-Anonymisierung NICHT.[49]

Abbildung 10.12: ZenMate IP-Leak via Flash

Ich habe mir die Premium Version angeschaut:

- Die Registrierung und später der Login in den Premium Dienst erfordern die Angabe einer E-Mail Adresse, was eindeutig ein identifizierendes Merkmal ist. Das gesamte anonymisierte Surfverhalten von Premium Kunden könnte ZenMate eindeutig dem

[49] https://kubieziel.de/blog/archives/1582-ZenMate-als-Anonymisierungsprogramm.html

Inhaber einer E-Mail Adresse zugeordnen. Vielleicht protokolliert ZenMate wirklich nichts, technisch wäre es aber einfach möglich.

- Die nächste Überraschung war die Verschmutzung der E-Mails zur Zahlungsbestätigung mit Tracking Wanzen. Wenn man die E-Mails von ZenMate genauer untersucht, findet man ein kleines, nicht sichtbares Bildchen, welches mit einer individuellen URL von einem ZenMate Tracking Server geladen wird.

```
<img width="1px" height="1px" alt=""
 src="http=://email.zenmate.com/o/eJyzEOwjAMBdDTkIOqie....">
```

ZenMate versucht also, die Empfänger der E-Mails zu verfolgen und jedes Öffnen der Mails soll registriert werden. In der Privacy Policy[50] von ZenMate wird dieses E-Mail Tracking nicht erwähnt.

- Das versprochene Blockieren von Third Party Tracking in der Premium Version funktioniert ebenfalls nicht. Cookies und moderne HTML5 Tracking Features von Drittseiten werden nicht zuverlässig blockiert, wenn man den Tracking Schutz aktiviert.

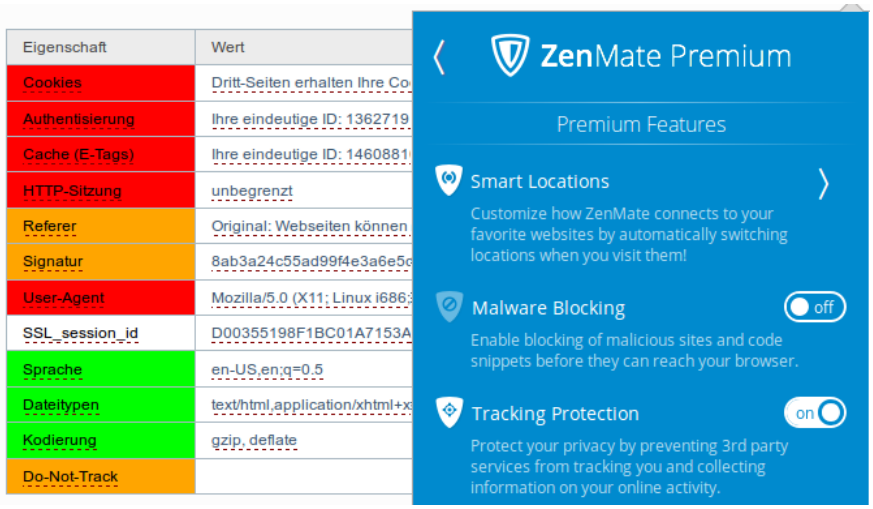


Abbildung 10.13: Tracking Protection in ZenMate funktioniert nicht

Schlussfolgerung: Das ist nur Abzocke mit zweifelhafter Werbung.

10.3.5 5socks.net

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

Eine kurze Recherche brachte folgende Ergebnisse:

1. Fragen wir mal nach 5.socks.net:

```
domain: 5socks.net
IPv4-adress: 174.36.202.143
addr-out: s3d.reserver.ru
whois.nic.mil [0] Undefined error: 0
```

[50] https://zenmate.com/privacy-policy/

```
OrgName: SoftLayer Technologies Inc.
OrgID: SOFTL
Address: 1950 N Stemmons Freeway
City: Dallas
StateProv: TX
PostalCode: 75207
Country: US
```

2. Softlayer Technologies Inc. == Layered Technologies
   http://seo-mannsgarn.de/proxy-ip-vandalismus.htm

3. Zu dieser Firma findet man bei cryptome.info:

```
Layered Technologies Incorporated
[NSA-affiliated IP range]
Frisco TX US
72.232.0.0 - 72.233.127.255
ns2.layeredtech.com [72.232.210.195]
ns1.layeredtech.com [72.232.23.195]
```

Keiner möchte einen NSA-affiliated Anonymisierungsserver nutzen - oder?

10.3.6 BlackBelt Privacy, Cloakfish und JanusVM

Tor Onion Router ist ein populärer Anonymisierungsdienst. Der Hauptnachteil ist die geringe Geschwindigkeit. Die Entwickler von TorProject.org sind sich dieses Problems bewusst und sie arbeiten daran, die Geschwindigkeit ohne Einbußen bei der versprochenen Anonymität zu erhöhen . Daneben gibt es immer wieder ein paar Scharlatane, die mit Voodoo-Methoden eine höhere Geschwindigkeit versprechen. Ich rate davon ab, diese Projekte zu nutzen.

Tor BlackBelt Privacy verspricht durch ein bisschen Voodoo in der Konfiguration eine Erhöhung der Geschwindigkeit bei der Nutzung von Tor. Eine Analyse der Änderungen an der Konfiguration durch Tor Entwickler kommt zu dem Schluss, dass minimale Verbesserungen bei der Geschwindigkeit möglich sein könnten. Allerdings verursachen die 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 ausreichen oder wäre als Ergänzung sinnvoll. Suspect.

Cloakfish ist ein Projekt, welches kommerziellen Zugriff auf das kostenfrei zugängliche Tor-Netz bieten möchte. Eine Client-Software, die als Closed-Source zum Download bereitsteht, soll vor allem SEOs ermöglichen, sich über die Tor-Exit-Nodes mit vielen verschiedenen IP-Adressen im Web zu bewegen. (laut Eigen-Werbung bis zu 15.000 verschieden Adressen pro Monat)

Durch die Verwendung von nur einem Tor-Node wird die Anonymität der Nutzer stark eingeschränkt und nicht die nächste Stufe der Anonymität erreicht, wie ein schnell aufgezogenes Werbe-Blog suggerieren möchte.

Die Tor-Entwickler missbilligen diese Nutzung des Tor-Netzwerkes, da die Load-Balancing Algorithmen von Tor durch diese Software gestört werden. Entgegen der

Behauptung auf der Projekt-Webseite sind die Entwickler von Cloakfish den Tor Developern unbekannt.

Diskussionen zu Cloakfish und verunglückte Beispiele von Postings, die unter falschem Pseudonym Werbung für die Software machen wollen, findet man bei gulli, im Forum der GPF und im Forum von JonDonym. Die Software wird bei den Black SEO intensiv beworben.

JanusVM ist eine VMware Appliance für anonymes Surfen. Die Appliance soll mit openVPN, Tor, Privoxy usw. eine schlüsselfertige Lösung bieten. Roger Dingledine von TorProject.org kommentierte die JanusVM im Dezember 2011 auf der OR-Talk Liste mit folgenden Worten:

> *"Probably has been unsafe to use for years."*

10.3.7 Proxy-Listen

In der Anfangszeit des Internets nutzten Cypherpunks die Möglichkeit, ihre IP-Adresse mit mehreren Proxies zu verschleiern. Der Datenverkehr wird über ständig wechselnde Proxies geleitet, so dass der Webserver ständig eine andere IP-Adresse sieht. Es gibt Tools, die diesen Vorgang automatisieren.

Der Vorteil liegt in der im Vergleich zu Mixkaskaden und Onion-Routern höheren Geschwindigkeit. Der offensichtliche Nachteil ist, dass der Datenverkehr zwischen eigenem Rechner und den Proxies meist unverschlüsselt ist.

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

Kapitel 11

Anonyme Peer-2-Peer Netzwerke

Anonyme Peer-2-Peer Netze nutzen die Infrastruktur des WWW, um in einer darüber liegenden, komplett verschlüsselten Transportschicht ein anonymes Kommunikationsnetz zu bilden. Der Datenverkehr wird mehrfach verschlüssellt über ständig wechselnde Teilnehmer des Netzes geleitet. Der eigene Rechner ist auch ständig an der Weiterleitung von Daten für andere Teilnehmer beteiligt. Das macht die Beobachtung durch Dritte nahezu unmöglich.

Es entsteht ein sogenanntes Darknet im Schatten des normalen Internet, das Google nicht kennt und in dem man sich weitgehend unbeobachtet bewegen kann, wie im Dunkel der Nacht.

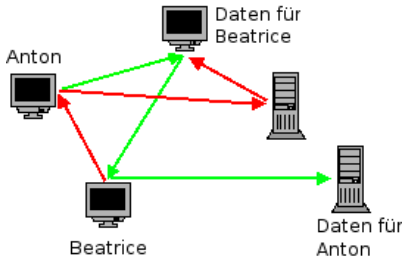


Abbildung 11.1: Prinzip von anonymen Peer-2-Peer Netzen

Hauptverwendungszweck für anonyme Peer-2-Peer Netze ist unbestritten das abmahnsichere Tauschen von Dateien. Unbeobachtete Kommunikation zwischen den Teilnehmern (E-Mail, Chatten...) ist ebenfalls möglich. Außerdem kann man zensurresistent Webseiten publizieren. Da die Nutzung der Angebote mit technischen Hürden verbunden ist, werden sie deutlich weniger besucht als klassische Webseiten.

Invisible Internet Project (I2P)

I2P hat das Ziel, Anonymität sowohl für Konsumenten als auch für Anbieter von Angeboten zu bieten. Dieses Ziel läßt sich nur in einem geschlossenen Netz verwirklichen. Die innerhalb des Invisible Internet bereitgestellten Angebote sind nicht lokalisierbar. Wie im normalen Internet sind die meisten Angebote zentralisiert und Server-basiert.

- Webserver stellen die sogenannten *eepsites* bereit, die Webseiten mit der Toplevel Domain *.i2p*. Es gibt Suchmaschinen für die *eepsites*. Das Äquivalent für Google ist http://eepsites.i2p.
- Als E-Mail Dienst hat sich *SusiMail* etabliert, ein zentraler Mailserver für I2P mit Gateway ins normale Internet. Eine neue Alternative ist das serverlose Projekt *I2P-Bote*.

- Das Äquivalent zum Usenet ist *Syndie*. Es gibt öffentliche und private Diskussionsforen, die auf Syndicationservern gehostet werden.
- Es gibt zwei redundante Server für IRC.
- Für das Filesharing ist mit *I2Psnark* eine Adaption von BitTorrent vorhanden. Der Tracker von *Postman* ist das Äquivalent zur PirateBay im normalen Netz.

Freenet

Freenet bietet Schutz gegen das umfangreichste Angriffsmodell. Freie Kommunikation unter den Bedingungen totaler Überwachung ist das Ziel des Projektes. Es stellt die höchsten Anforderungen an die Nutzer und erzielt die langsamste Downloadgeschwindigkeit.

Im Unterschied zu I2P werden die Inhalte im Freenet redundant über alle Teilnehmer verteilt und verschlüsselt abgelegt. Es gibt keine Server für Webdienste, E-Mail usw. Der Zugriff auf die Inhalte erfolgt nicht über einfache URLs, sondern über komplexe Schlüssel, welche die Adressen der TOR Hidden Services als absolut harmlos erscheinen lassen. Einmal veröffentlichte Inhalte können im Freenet nicht mehr modifiziert werden, auch nicht vom Autor. Es ist jedoch möglich, aktualisierte Versionen zu veröffentlichen. Die Freenet Software stellt sicher, dass immer die aktuellste Version angezeigt wird.

Neben Webseiten gibt es *F-Mail* und mit *Frost* ein Äquivalent zum Usenet. Das Tauschen von Dateien erfolgt direkt im Browser mit einer Oberfläche, die die Freenet Software bereitstellt.

Unabhängig vom *Open Freenet* kann man mit vertrauenswürdigen Freunden ein eigenes Netz Friend-2-Friend Netzwerk konfigurieren, welches sich vollständig der Beobachtung durch unbefugte Dritte entzieht.

Retroschare

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

RetroShare ermöglicht die unbeobachtete Kommunikation in Gruppen, ohne zentrale Dienste im Internet zu nutzen. Die Kommunikation ist durch Dritte sehr schwer kompromittierbar, wenn jeder Teilnehmer die kryptografischen Schlüssel nur an vertrauenswürdige Freunde weitergibt. Wenn man allerdings diese Grundregel missachtet und die eigenen Schlüssel im Internet publiziert, um das private Netzwerk zu vergrößern, dann können sich auch unbefugte Dritte einschleichen.

11.1 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.

Das Projekt bietet einen Java-basierten Client. Dieser Client verschlüsselt den Datenverkehr für alle Internet-Anwendungen, die I2P nutzen. Außerdem stellt er sicher, dass ständig neue Verbindungen zu anderen Rechnern des Netzwerkes aufgebaut werden.

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

11.1.1 Installation des I2P-Routers

Für die Nutzung des Invisible Internet Projects benötigt man den I2P-Router, der als Proxy für verschiedene Anwendungen (Webbrowser, E-Mail Client...) dient und die Weiterleitung der Daten vom und zum I2P-Netz übernimmt. Der I2P-Router ist eine Java-Applikation und steht unter https://geti2p.net/de zum Download bereit.

Windows: Als erstes ist ein Java-Runtime-Environment (JRE) zu installieren. Das Installationsprogramm für Java gibt auf der Webseite www.java.com[1]. Der Installer möchte unbedingt die *Ask-Toolbar* für alle Browser installieren. Das sollte man deaktivieren, braucht man nicht.

Anschließend kann der I2P-Router installiert werden. Die Datei *i2pinstall-0.x.y.exe* von der I2P Downloadseite enthält einen kompletten Installer, der nach dem Start alles Nötige einrichtet. Einfach starten und dem Assistenten folgen. Nach der Installation findet man im Startmenü die neue Gruppe *I2P* (Bild 11.2).

Abbildung 11.2: I2P im Startmenü von Windows

Die beiden Punkte zum Starten von I2P unterscheiden sich nur gering. Im ersten Fall hat man keine störende Konsole auf dem Desktop. *I2P router console* öffnet den Webbrowser, um den Router zu konfigurieren oder abzuschalten mit der Adresse http://localhost:7657.

Nach dem ersten Start braucht der I2P-Router einige Zeit, um sich im Invisible Internet zu orientieren. Zum Warmlaufen sollte man ihm 30 min Zeit lassen. Wenn es danach noch immer nicht so richtig funktioniert, sind die Netzwerkeinstellungen zu prüfen. Die Startseite der Router-Console gibt einige Hinweise.

Den I2P-Router kann man nicht kurz einmal starten, wenn man ihn nutzen möchte. Er sollte möglichst immer laufen, wenn der Rechner online ist. Damit lernt er die verfügbaren Peers und eepsites besser kennen und ist besser in das Netz eingebunden.

[1] https://www.java.com/de/

11.1.2 Konfiguration des I2P-Router

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

Bandbreite anpassen

Der I2P-Router arbeitet am besten, wenn man die Bandbreite an den eigenen Internetanschluss anpasst. Nach dem Start kann man auf der Seite http://localhost:7657/config der Router Konsole die Werte anpassen.

Netzwerkkonfiguration

Auf der Seite http://localhost:7657/confignet der Router Konsole sind die Einstellungen für die Einbindung in das I2P-Netz zu konfigurieren. Dabei gibt es zwei Möglichkeiten:

1. Wenn der eigene Rechner nicht vom Internet erreichbar ist, dann sind folgende Optionen zu aktivieren, damit der I2P-Router korrekt arbeitet:
   - *Versteckter Modus* ist zu aktivieren.
   - Optional kann der *Laptop Modus* aktiviert werden. Dann ändert sich Router-Identifikation bei Änderung der IP-Adresse.
2. Wenn der eigene I2P-Router vom Internet für andere Teilnehmer erreichbar ist, verbessert sich die Performance und Anonymität. In der Netzwerk Konfiguration des I2P-Routers sind dann folgende Optionen zu konfigurieren:
   - UPnP ist aus Sicherheitsgründen auf dem DSL-Router zu deaktivieren. Damit ist klar, dass in der Netzwerkkonfiguration des I2P-Routers das *UPnP Portforwarding* und die *UPnP IP-Adresserkennung* auch zu deaktivieren sind.
   - In den UDP-Einstellungen ist der Port anzugeben, für den die Weiterleitung auf dem DSL-Router konfiguriert wurde.
   - In den TCP-Einstellungen ist ebenfalls der Port zu konfigurieren und die Option *automatisch erkannte IP-Adresse benutzen* zu aktivieren.

   Die Hinweise im Kapitel *Konfiguration des DSL-Routers* erläutern die notwendigen Einstellungen, damit Ihr Rechner vom Internet erreichbar ist. Auf dem DSL-Router ist ein Portforwarding zu Ihrem Rechner zu konfigurieren und die Firewall des Rechners ist anzupassen.

SusiDNS anpassen

Für die Zuordnung von Domainnamen mit der Toplevel Domain .i2p zu einem Service wird SusiDNS verwendet, ein dem DNS im Internet vergleichbares System. Wie in den Anfangszeiten des WWW erhält jeder I2P Router eine komplette Liste der bekannten eepsites: das *addressbook*.

Um neue eepsites oder Services in das addressbook einzufügen, verwendet I2P sogenannte *subscriptions*. Die eine standardmäßig vorhandene subscription wird relativ selten aktualisiert.

Um auf dem Laufenden zu bleiben, kann man weitere subscriptions zu abonnieren. Die Einstellungen für SusiDNS findet man in der Routerkonsole. Subscriptions kann man unter folgender Adresse einfügen: http://localhost:7657/susidns/subscriptions.jsp (Bild 11.3)

Folgende subscriptions bieten aktuelle Neuerscheinungen von eepsites:

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

Abbildung 11.3: subscriptions für SusiDNS

11.1.3 Anonym Surfen mit I2P

Der I2P-Router stellt einen HTTP- und HTTPS-Proxy für den Webbrowser bereit. Die Default-Adressen dieser Proxys sind:

```
          Rechner:  localhost
    HTTP-Proxy Port:  4444
     SSL-Proxy Port:  4445
     FTP-Proxy Port:  4444
  Gopher-Proxy Port:  4444
```

Der Proxy kann genutzt werden, um Webseiten im Invisible Internet aufzurufen (sogenannte *eepsites*, erkennbar an der Toplevel Domain **.i2p**).

JonDoFox nutzen

Das Firefox Profil *JonDoFox* ist für spurenarmes und sicheres Surfen optimiert. Es bietet neben *JonDo* und *Tor* eine *Benutzerdefinierte Proxy Konfiguration*, die man für I2P nutzen kann. Die Einstellungen zeigt Bild 11.4. Der JonDoFox verhindert zuverlässig eine Kompromittierung der Anonymität.

Firefox selbst konfigurieren

Ich würde empfehlen, für das Surfen im Invisible Internet ein separates Firefox-Profil zu erstellen. Dann ist es für spionierende Websites gänzlich unmöglich, im Cache oder in der Historie abgelegte Daten über das anonyme Surfen auszulesen. Den Profil-Manager von Firefox startet man mit folgendem Kommando:

```
> firefox -P
```

In dem sich öffnenden Dialog (Bild 11.5) kann man ein neues Profil anlegen und anschließend die Proxy-Einstellungen konfigurieren. In Zukunft wird Firefox bei jedem Start fragen, welches Profil genutzt werden soll.

Anschließend kann das Profil *I2P-Fox* gestartet werden und die Proxy-Einstellungen sind wie im Bild 11.6 gezeigt zu konfigurieren. Die allgemeinen Hinweise zu Cookies, JavaScript, Plug-ins, HTTPS-Security usw. im Abschnitt *Spurenarm Surfen* gelten auch für I2P. Das Profil *I2P-Fox* ist entsprechend zu konfigurieren.

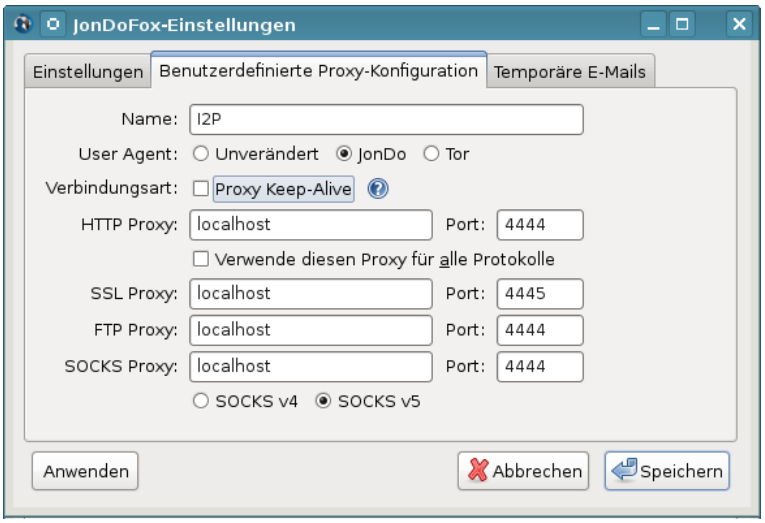


Abbildung 11.4: Benutzerdefinierte Proxy Konfiguration im JonDoFox

Abbildung 11.5: Firefox Profil-Manager

Wichtige Sicherheitseinstellungen für Firefox

Flash und Java Plug-ins sind unbedingt zu deaktivieren, da diese Plug-ins die Proxy Einstellungen umgehen könnten. Um eine Deanonymisierung zu vermeiden, sind für einen aktuellen Firefox außerdem folgende Features unter der Adresse *about:config* zu deativieren:

- WebRTC kann durch UDP-Tunnel die reale IP-Adresse aufdecken (nur Firefox 18 und neuer):

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

- Geolocation-API kann den realen Standort ermitteln:

```
geo.enabled = false
```

- Phishing- und Malware Protection funktioniert für eepsites nicht, da die Webseiten des Darknet nicht in der Google Datenbank enthalten sind:

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

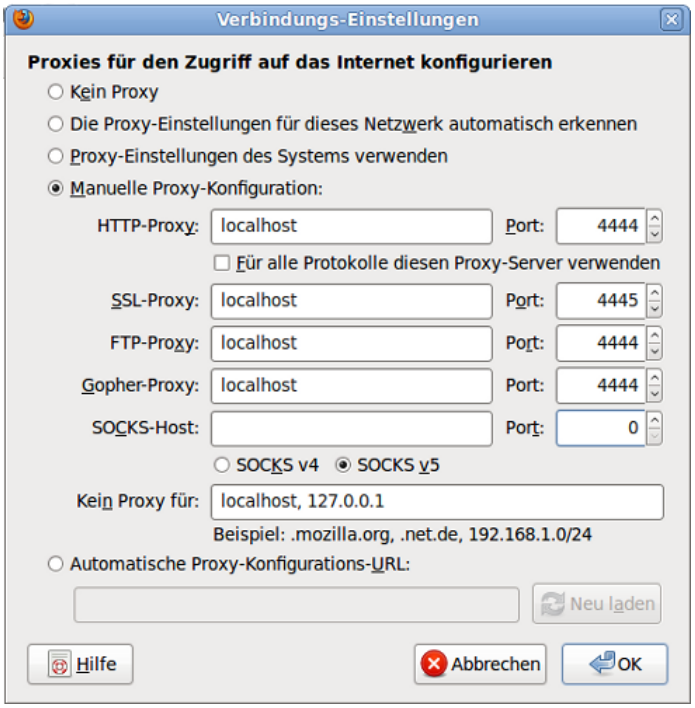


Abbildung 11.6: Firefox Proxy-Einstellungen für I2P

Suchmaschinen für I2P

Um sich in einem Netzwerk zu orientieren, braucht man eine Suchmaschine. Die Webseite plugins.i2p bietet viele *Firefox Search Plugins für I2P*. Wenn man die Webseite http://plugins.i2p/firefox aufgerufen hat, kann man die Suchmaschinen einfach durch Aufklappen der Liste der Suchmaschinen oben rechts im Firefox hinzufügen. Unter dem Trennstrich findet man die neuen Suchmaschinen, die diese Webseite zur Installation anbietet.

Das Äquivalent zu Google im normalen Internet ist im I2P-Netz die Suchmaschine http://eepsites.i2p. Die anderen Dienste in der Liste durchsuchen einzelne eepsites.

11.1.4 I2P Mail 1 (Susimail)

Die Anwendung Susimail ist integraler Bestandteil von I2P und ermöglicht den unbeobachteten Austausch von E-Mails. Das Anlegen und Verwalten eines Susimail-Accounts erfolgt auf der eepsite http://hq.postman.i2p.

Es ist möglich, E-Mails in das normale Web zu versenden und auch von dort unter der Adresse *<username>@i2pmail.org* zu empfangen. die Weiterleitung ins normale Internet kann bis zu 24h dauern und ist von den gewählten Einstellungen auf HQ Postmaster abhängig. Um für Spammer unattraktiv zu sein, haben die Entwickler von I2P die Anzahl der ins normale Web versendbaren Mails begrenzt. Es ist möglich, innerhalb von 24h bis zu 20 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.

Routerkonsole nutzen

Ein einfaches Webinterface für Susimail ist in der I2P Routerkonsole erreichbar unter der Adresse http://localhost:7657/susimail/susimail.

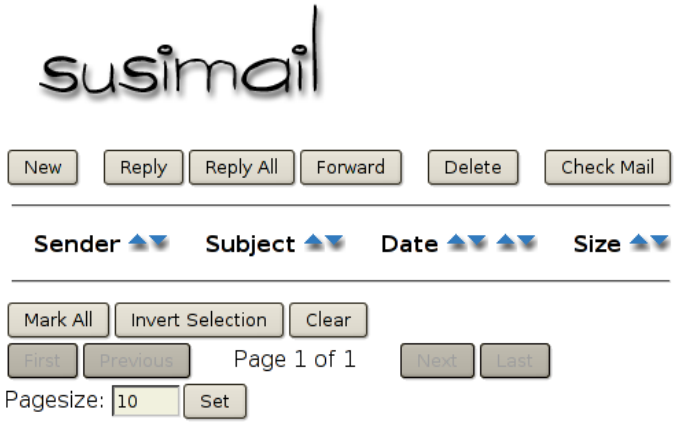


Abbildung 11.7: Webinterface von Susimail

Es bietet eine simple Möglichkeit, Mails abzurufen und zu versenden. Komfortabler ist die Nutzung des bevorzugten E-Mail Clients, vor allem wenn man die Möglichkeiten zur Verschlüsselung der Nachrichten nutzen möchte.

Thunderbird konfigurieren

Der Susimail-Account kann mit jedem E-Mail Client genutzt werden.

```
SMTP-Server: localhost    Port: 7659
POP3-Server: localhost    Port: 7660
Login-Name:  <username>
```

In Thunderbird ist als erstes ein neuer SMTP-Server anzulegen (Konten -> Postausgangs-Server (SMTP) -> Hinzufügen). Der Server erfordert eine Authentifizierung mit den Daten des Susimail Accounts.

Danach kann ein neues POP3-Konto angelegt werden, welches diesen SMTP-Server für die Versendung nutzt. SSL- und TLS-Verschlüsselung sind zu deaktivieren. Der I2P-Router übernimmt die abhörsichere Übertragung.

In den Server-Einstellungen des Kontos sollte die Option *"Alle x Minuten auf neue Nachrichten prüfen"* deaktiviert werden! Die Admins von Susimail bitten darum, den Service nicht unnötig zu belasten.

Susimail mit Tor nutzen

An Stelle des I2P-Routers kann auch Tor für den Abruf und das Versenden von Nachrichten via I2P Mail genutzt werden. Folgende Hidden Services bieten ein SMTP-Gateway (Port: 7659) und POP3-Gateway (Port: 7660):

```
v6ni63jd2tt2keb5.onion
5rw56roal3f2riwj.onion
```

Die Hidden Service Adresse ist als SMTP- und POP3-Server im E-Mail Client für das I2P-Mail-Konto an Stelle von *localhost* einzutragen. Außerdem ist der E-Mail Client so zu konfigurieren, dass er Tor als Proxy nutzt. Sollte der E-Mail Client ständig den Fehler TIMEOUT liefern, hilft es, den Hidden Service erst einmal im Webbrowser aufzurufen.

Hinweise zur Nutzung von Susimail

Der Service wird von *postman* und *mastijaner* in der Freizeit aufgebaut und gepflegt. Sie bitten darum, 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 auf dem Server viele tote Mail-Accounts, wo noch immer Mails eingehen (Spam und Mailinglisten) und viel Speicherplatz verbrauchen.
5. Bitte verwendet den Dienst nicht, um anonyme Beleidigungen oder Drohungen zu schreiben. Das bringt den Betreibern Ärger und gefährdet den reibungslosen Betrieb.

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

11.1.5 I2P Mail 2 (Bote)

I2P Bote bietet serverlose und verschlüsselte E-Mail Kommunikation. Die Daten werden redundant und verschlüsselt in einer DHT gespeichert, über alle Teilnehmer verteilt. Es gibt keinen zentralen Server, der Kommunikationsprofile erstellen oder eine Vorratsdatenspeicherung umsetzen könnte. Starke Kryptografie stellt sicher, dass nur der Empfänger die Nachricht lesen kann.

I2P Bote ist keine Weiterentwicklung von Susimail und es soll es auch nicht ersetzen. Langfristig werden beide Projekte parallel existieren und kooperieren. Das Projekt bietet folgende Features:

- Bedienung im Webinterface der I2P-Routerkonsole.
- Erzeugen von Identitäten, Senden/Empfangen von E-Mails.
- SMTP- und IMAP-Gateway für die Integration in Thunderbird u.a.
- Anonyme Absender und Versenden über Zwischenstationen mit zeitlicher Verzögerung (Remailer-Konzept).
- Dateianhänge bis 500 kB werden unterstützt. Die Begrenzung der Größe der Dateianhänge ist aufgrund der redundanten Speicherung nötig. Die Nachrichten werden mit 20x Redundanz gespeichert und eine 1 MB große Mail würde 20 MB Speicherplatz in der DHT belegen.

Installation von I2P Bote

Um I2P Bote zu nutzen, ist die Installation von 3 Plug-ins für den I2P Router nötig. Auf der Seite I2P Dienste der Routerkonsole (unter http://localhost:7657/configclients.jsp) findet man ganz unten den Abschnitt für die Installation zusätzlicher Plug-Ins (Bild 11.8).

Folgende Plug-Ins sind in dieser Reihenfolge zu installieren:

1. http://sponge.i2p/files/seedless/01_neodatis.xpi2p
2. http://sponge.i2p/files/seedless/02_seedless.xpi2p

Abbildung 11.8: Installation des Plug-in I2P Bote

3. http://i2pbote.i2p/i2pbote.xpi2p

Nach erfolgreicher Installation findet man auf der Startseite in der Liste der *Lokalen Dienste* oder rechts im Menü der Routerkonsole einen neuen I2P Dienst *SecureMail*. Ein Klick öffnet die Web-Oberfläche in einem neuen Browser-Tab.

Eigene Identität erzeugen

Der erste Schritt nach der Installation ist in der Regel die Erstellung einer eigenen Adresse. In der Navigationsleiste rechts wählt man *"Identitäten"* und den Button *"Neue Identität"*.

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

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

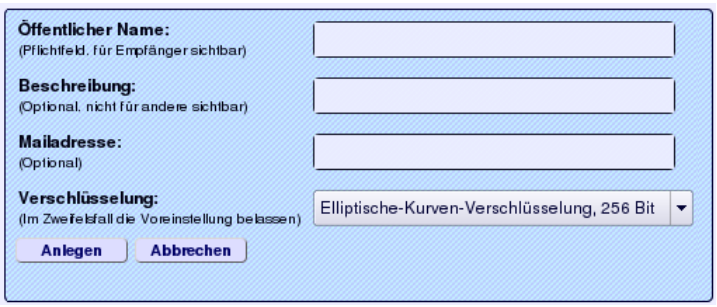


Abbildung 11.9: Neue Identät für I2P-Bote anlegen

Konfiguration

Bevor man loslegt, sollte man einen Blick in die Konfiguration werfen und diese anpassen.

- Abrufen der Nachrichten: Es ist konfigurierbar, ob und in welchem Intervall neue Nachrichten aus der DHT automatisch abgerufen werden sollen. Um die Belastung des Bote-Netzes gering zu halten sollte man Intervalle von 2-3h nutzen. Bei Bedarf kann man das Abrufen neuer Nachrichten auch selbst anstoßen.
- Über Zwischenstationen senden: Wird diese Option deaktiviert ("AUS"), gehen versendete Nachrichten direkt in die DHT. Die Anonymität entspricht der normalen Anonymität bei der Nutzung von I2P.

  Eine höhere Anonymität erreicht man, wenn die Nachricht vor dem Speichern in der DHT über 1...n Teilnehmer des I2P-Bote Netzes geleitet und dort jeweils um eine zufällige Zeitspanne verzögert wird. Die min. und max. Werte für die Verzögerung können konfiguriert werden. Ähnlich wie bei Remailern sinkt damit natürlich die Performance der Kommunikation.
- Durchleitung an Nicht-I2P-Adressen: Es ist möglich, Mails an Nicht-I2P-Bote Teilnehmer zu versenden. Die Nachrichten werden an die Bote-Adresse eines Durchleitungsdienstes versendet, der sich dann um die weitere Zustellung kümmert. Derzeit arbeitet HQ Postman an der Entwicklung dieses Services, der aber noch nicht arbeitsfähig ist.
- Absendezeit: Die Absendezeit sollte man nicht mit versenden, wenn die Nachricht über Zwischenstationen gesendet wird. Anderenfalls ist es ein Feature, dass die Anonymität nur geringfügig erhöhen kann, wenn diese Option deaktiviert wird. Mir hilft es, den Überblick in der Inbox zu behalten, wenn ein Zeitstempel vorhanden ist.

Mails schreiben und empfangen

Das im Bild 11.10 gezeigte Formular für eine neue Mail öffnet sich mit Klick auf den Button *"Neu"*.

Abbildung 11.10: Neue E-Mail in I2P Bote schreiben

Als Absender kann man *Anonym* wählen, oder eine der zuvor angelegten Identitäten. Wer *Anonym* wählt, sollte sich nicht wundern, dass er vom Empfänger als anonymer Unbekannter behandelt wird. Für vertrauliche Konversation muss man seinen Gegenüber verifizieren können.

In die Felder *An*, *Kopie* oder *Blindkopie* sind die kryptischen Bote-Adressen der Empfänger einzutragen, der Rest sollte sich selbst erklären. Eingehende Mails findet man im Ordner *Posteingang*.

Adressbuch

Das Web-Interface bietet ein einfaches Adressbuch. Man kann die Bote-Adressen und Namen von Partnern sammeln und beim Schreiben einer Mail mit zwei Klicks übernehmen.

Außerdem hilft das Adressbuch bei der Verifikation der Absender empfangener Nachrichten. Ein Absender ist eindeutig nur durch seine Bote-Adresse bestimmt. Der Name kann frei gewählt werden und kann auch mehrfach genutzt werden. Es könnte also jemand den Namen HungryHobo nutzen, um sich als Hauptentwickler von I2P-Bote auszugeben.

Ein Vergleich der Bote-Adressen ist nicht intuitiv. Das Adressbuch kann diese Aufgabe übernehmen. Ist der Absender einer Nachricht im Adressbuch enthalten und stimmt die Bote-Adresse überein, dann zeigt die Liste der Inbox ein Häckchen in der Spalte **Bek**.

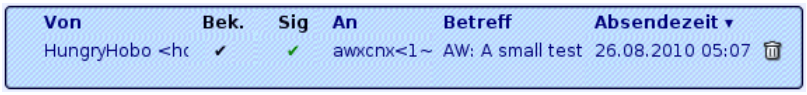


Abbildung 11.11: Inbox mit verifiziertem Absender

11.1.6 I2P IRC

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

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

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

Die wichtigsten Chat-Kommandos

Der Chat wird in der Regeln komplett durch Kommandos gesteuert. Alle Kommandos beginnen mit einem Slash. Eine kurze Liste der wichtigsten Kommandos:

/list Listet alle Diskussions-Channels auf, die auf dem Server verfügbar sind.

/join #channel Den Raum #channel betreten und mitdiskutieren.

/quit Den aktiven Raum verlassen oder vom Server abmelden.

/msg nick <text> Sendet eine Nachricht an den User *nick*.

/ignore nick Einen Troll ignorieren.

/help Beantwortet alle weiteren Fragen.

Im IRC ist man mit einem Nicknamen unterwegs. Die Nicknamen werden registriert und mit einem Passwort geschützt, damit kein Dritter einen bekannten Nicknamen nutzen kann, um sich eine Identität zu erschleichen.

Die Registrierung erfolgt mit folgendem Kommando:

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

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

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

#anonops

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

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

Geben Sie keine persönlichen Informationen im public IRC preis.

- keine Anhaltspunkte im Nicknamen und Realnamen veröffentlichen
- keine persönlichen Informationen im Chat diskutieren
- keine Informationen über die Herkunft diskutieren (Land, Stadt usw.)
- keine Beschreibung von Tattoos, Piercings oder anderer Merkmale
- keine Informationen über Beruf und Hobbys
- keine Sonderzeichen wie äöü verwenden, die nur in Ihrer Sprache verfügbar sind
- veröffentlichen Sie nichts im normalen Netz, während Sie in einem anonymen Chat sind - es kann einfach korreliert werden
- posten Sie keine Bilder von Facebook im Chat, diese Bilder enthalten die persönliche ID
- verbinden Sie sich nicht Tag für Tag zur gleichen Zeit mit dem Chat

11.1.7 I2P BitTorrent

Der I2P-Router bietet auch eine angepasste Implementierung des BitTorent Protokolls für anonymes Peer-2-Peer Filesharing. Im Gegensatz zur 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 dürfen. Torrents findet man z.B. auf den eepsites http://tracker2.postman.i2p, http://crstrack.i2p/tracker oder http://tracker.welterde.i2p. Das Webinterface bietet direkte Links zu diesen eepsites.

Hinweis zur Nutzung: Es gehört beim Filesharing zum guten Ton, Dateien nicht nur zu saugen. Man stellt die heruntergeladenen Dateien auch anderen Teilnehmern zur Verfügung. Bei BitTorrent im normalen Netz gilt es als freundlich, wenn man heruntergeladene Dateien mindestens für 2 Tage zum Upload anbietet oder bis die Datenmenge des

Upload das 2,5fache des Downloads beträgt. Da die Geschwindigkeit im I2P-Netz wesentlich geringer ist, sollte man heruntergeladene Dateien mindestens für 1 Woche zum Upload anbieten.

11.2 DSL-Router und Computer vorbereiten

Um als vollwertiger Teilnehmer an einem anonymen Peer-2-Peer Netz teilzunehmen, muss der eigene Rechner vom Internet aus erreichbar sein. Nur dann können andere Teilnehmer des Netzes den eigenen Knoten kontaktieren. Als typischer Heimnutzer mit DSL-Anschluss sind einige Anpassungen nötig, damit der eigene Rechner aus dem Internet erreichbar ist.

1. Der DSL-Router muss den ankommenden Datenverkehr der anderen Peer-2-Peer Teilnehmer an den eigenen Rechner weiterleiten. Einige Programme können den Router mit UPnP konfigurieren. Aufgrund der Sicherheitsprobleme bei UPnP [2] sollte man dieses Feature auf dem Router deaktivieren und die Weiterleitung per Hand konfigurieren.

   Der Screenshot 11.12 zeigt die Konfiguration für einen Linksys Router. Für I2P wurde im Beispiel der Port 8888 gewählt, für GnuNet muss man die Ports 1080 und 2086 weiterleiten.

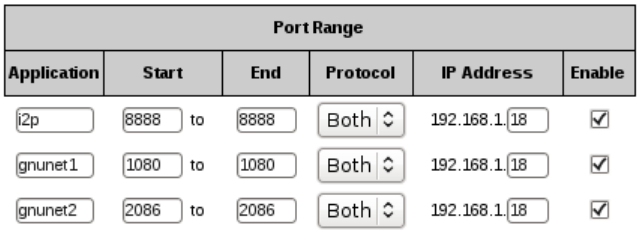


Abbildung 11.12: Portforwarding auf dem Router

2. Die Konfiguration der Weiterleitung auf dem DSL-Router ist einfacher, wenn der eigene Rechner innerhalb des privaten lokalen Netzwerkes eine feste IP-Adresse hat. Dafür ändert man die Konfiguration der Netzwerkschnittstelle von *DHCP* auf *feste IP-Adresse*.

3. Außerdem muss die Firewall auf dem lokalen Rechner den ankommenden Datenverkehr der anderen Peer-2-Peer Teilnehmer auf den Ports durchlasssen, für die eine Weiterleitung im Router konfiguriert wurde.

[2] http://heise.de/-1793625

Kapitel 12

Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) wurden entwickelt, um vertrauenswürdige Endpunkte über unsichere Netzwerke zu verbinden. Sinnvolle Anwendungen für VPNs sind:

- Verbindung von zwei oder mehreren Firmenstandorten über das Internet.
- Einbindung einzelner Außendienst Rechner (Road Warrior) in ein Firmennetz.
- Einbindung externer, industrieller Anlagen an zentrale Leitsysteme (z. B. Windkraftträder im Energiebereich oder dezentrale Pumpwerke in der Wasser/Abwasser Versorgung o.ä.)
- Im privaten Bereich kann mit VPN Technologien verwenden, um in nicht vertrauenswürdigen Wi-Fi Netzwerken (Hotel, Flughafen, U-Bahn o.ä.) die Verbindung zu einem vertrauenswürdigen Zugangsprovider herzustellen. Das verhindert Firesheep-ähnliche Angriffe[1] durch andere, möglicherweise bösartige Nutzer des Wi-Fi Hotspot.

  Die Telekom bietet für ihre Hotspots einen VPN Client an. Alternativ verfügen viele Heimrouter über eine VPN Funktion, die man als VPN-Server nutzen kann, so dass man unterwegs mit der gleichen Sicherheit wie vom heimischen PC surft und gegenüber Webdiensten die Verfolgung der Reisetätigkeit durch Geo-Lokalisierung anhand der IP-Adresse verhindert.

VPN Technologien

Die für ein VPN notwendige Software steht für unterschiedliche Standards als Open Source Software zur Verfügung:

OpenVPN ist ein Klassiker. Die Software arbeitet auf TCP-Ebene (OSI Layer 4) und nutzt SSL/TLS, um den Datenverkehr zwischen zwei Endpunkten zu verschlüsseln. Es werden Client-2-Server und Server-2-Server Verbindungen unterstützt.

OpenConnect wurde ursprünglich von Cisco entwickelt. Es arbeitet mit UDP (OSI Layer 4) und nutzt DTLS, um den Datenverkehr zwischen einem Client und einem Server zu verschlüsseln. Es ist nicht für Server-2-Server Verbindungen geeignet.

IPsec arbeitet einen Level tiefer auf IP-Ebene und bietet daher eine höhere Robustheit gegen Lauscher, da auch die TCP-Header verschlüsselt werden.

IPsec ist ein sehr komplexes Protokoll, das die Lösung eines Problems auf mehreren unterschiedlichen Wegen ermöglicht. Diese Komplexität ist einer der Hauptkritikpunkte von N. Ferguson and B. Schneier in ihrer Evaluierung von IPsec.[2]

[1] http://www.searchnetworking.de/definition/Firesheep-ein-interessantes-Firefox-Plugin
[2] https://www.schneier.com/academic/paperfiles/paper-ipsec.pdf

> *In our opinion, IPsec is too complex to be secure. The design obviously tries to support many different situations with different options.*

WireGuard ist ein relativ junges Projekt, das wie IPsec auf OSI Layer 3 arbeitet. Ziel von WireGuard ist eine VPN Lösung mit geringer Komplexität in der Protokoll Spezifikation und Implementierung sowie einer einfachen Anwendung. Der Quellcode umfasst derzeit nur 4.000 Zeilen Code (OpenVPN: 292.000 Zeilen).

Iodine versteckt den VPN Traffic im DNS Datenverkehr, um VPN-Sperren zu umgehen. Der Datendurchsatz ist viel geringer, als bei anderen VPNs.

PPTP Microsofts Point-to-Point-Tunneling-Protocol (PPTP) ist konzeptuell kaputt und sollte nicht mehr verwendet werden.

Daneben gibt es kommerzielle Anbieter für hochsichere, zertifizierte VPN Lösungen. Beispiele dafür sind die Produktlinien genucrypt (von Genua.de) oder SINA (von Secunet.com), die aus Hardware-Software Kombinationen bestehen und überwiegend (nicht ausschließlich) in kritischen Infrastrukturen wie Energie- und Wasserversorgung sowie bei Behörden eingesetzt werden.

12.1 VPN Dienste als Billig-Anonymisierer

Aus der Werbung eines VPN Providers:

> *Verbergen Sie Ihre Online-Identität und surfen Sie anonym im Netz!*

Nein! VPNs wurden NICHT als Anonymisierungsdienste entwickelt. Der Einsatz als Billig-Anonymisierer ist aus folgenden Gründen nicht sinnvoll:

- VPNs anonymisieren lediglich die IP-Adresse eines Internetnutzers. Für Trackingdienste ist die IP-Adresse aber nur ein geringwertiges Trackingfeature. Durch die Verbreitung mobiler Internetnutzung mit ist der Wert dieses Merkmals weiter gesunken. Modernes Tracking verwendet Fingerprinting und EverCookies, gegen die VPNs nicht schützen. Somit ist durch VPNs keine Anonymität bei Surfen gegeben.

  (Richtige Anonymisierungsdienste wie Tor Onion Router adressieren dieses Problem durch eine einheitliche Browserkonfiguration (TorBrowserBundle), die eine Anonymitätsgruppe schafft, in der einzelne Surfer nicht unterscheidbar sind.)

- Die IP-Anonymisierung von VPNs kann relativ einfach durch Traffic Korrelation oder Traffic Fingerprinting ausgehebelt werden. Die mathematischen Grundlagen dafür lernt jeder Informatikstudent im ersten Jahr im Mathe Grundkurs.

  Hermann/Wendolsky/Federrath haben bereits 2009 in dem Paper *Popular Privacy Enhancing Technologies with the Multinomial Naïve-Bayes Classifier*[3] gezeigt, dass man die Nutzer eines OpenVPN Anonymisierers zu 95% durch Beobachtung des Traffics des VPN-Servers bzw. -Nutzers deanonymisieren kann ohne die Krypto zu knacken. Bei Tor war der gleiche Ansatz unter Laborbedingungen mit 3% Erkennungsrate erfolglos.

  (Inzwischen gibt es auch einige mathematisch ausgefeiltere Angriffe dieser Art auf Tor Onion Router unter Laborbedingungen, die aber nicht so einfach auf die reale Welt übertragbar sind, wie M. Perry in einem Blogartikel schreibt. Tor enthält Schutzmaßnahmen gegen diese Angriffe.)

- Ein VPN Betreiber hat wie ein Internet Zugangsprovider Zugriff auf das gesamte Nutzungsverhalten. Das erfordert ein hohes Maß an Vertrauen in den VPN Betreiber, das bei vielen Betreibern nicht gerechtfertigt ist.

[3] https://epub.uni-regensburg.de/11919

  - Der von Facebook betriebene VPN-Dienst Onavo spioniert seine Nutzer aus und speichert, welche Apps und Internetdienste die Nutzer verwenden. Damit kann Facebook frühzeitig Konkurrenten erkennen und Maßnahmen zur Sicherung der Marktes ergreifen.[4]
  - Der VPN Dienst AnchorFree verwendet für das Angebot Hotspot Shield Fre JavaScript, um IFrames mit personalisierten Werbeanzeigen zu injizieren und außerdem den Standort des Nutzers zu tracken. Eindeutige Identifikationsmerkmale wie MAC-Adressen und IMEI-Nummern von Smartphones werden an Werbenetzwerke weitergegeben, was die Nutzer gegenüber den Trackingdiensten natürlich deanonymisiert.[5]

  Statt einem Gewinn an Privatsphäre wird man als Nutzer solcher VPN Dienste noch mehr ausgespäht.

- Bei vertrauenswürdigen VPN Providern ist zu beachten, dass sie den Gesetzen des jeweiligen Landes folgen müssen. Da diese Dienste wie Zugangsprovider zum Internet arbeiten, kann sich daraus eine deutliche Absenkung der Sicherheit und Privatsphäre ergeben, wenn die Gesetze des Heimatlandes des VPN Anbieters eine Vorratsdatenspeicherung fordern oder unlimitierten Zugriff auf den entschlüsselten Datenverkehr für Geheimdienste.

  Der britische VPN-Dienst HideMyAss (Testsieger beim VPN Magazine[6]) hat z. B 2011 den LuzSec Hacker Cody Kretsin, der dem Anonymitätsversprechen von HideMyAss vertraute, an das FBI verraten. Dabei hat HideMyAss nur im Rahmen der gesetzlichen Vorgaben kooperiert. In einem Blog Artikel verteidigt HideMyAss die Deanonymisierung von Kretsin gegenüber dem FBI.[7]

  Es gibt keinen Grund, einem VPN Anonymisierer mehr zu vertrauen, als einem Internet Zugangsanbieter wie Telekom oder Vodafon oder ....

12.2 Das VPN Exploitation Team der NSA

Aus den Dokumenten, die Edward Snowden bei der NSA rausgetragen hat, ist bekannt, dass die in der NSA das *OTP VPN Exploitation Team* für die Angriffe auf VPNs zuständig ist. Es werden einige Angriffsvektoren beschrieben, die ambitionierte Hacker gegen VPNs einsetzen (nicht nur die NSA setzt diese Techniken ein, auch andere Länder wie Frankreich, China oder Russland haben erhebliche Kapazitäten auf dem Gebiet und Kriminelle Hacker jeglicher Art sind auch interessiert).

Angriffe auf die Verschlüsselung: In den Snowden-Dokumenten wird erwähnt, dass der NSA 2010 einen Durchbruch bei Angriffen auf Verschlüsselung gelang und 60% des weltweiten VPN-Traffics on-the-fly entschlüsselt werden konnte.

2015 wurde die Logjam Attack[8] durch zivile Kryptoforscher publiziert, die die Erfolge der NSA erklären konnte. Dabei handelt es sich um einen pre-computation Angriff auf den Diffie-Hellman Schlüsseltausch.

Dieses Beispiel zeigt, dass staatliche Angreifer mehrere Jahre Informationvorsprung bei der Kryptoanalyse haben. Man sollte deshalb keine Kryptografie einsetzen, die schon ein bisschen schwächelt.

Außerdem werden *Man-in-the-Middle* Angriffe und *TLS-Downgrade* Angriffe eingesetzt. Für beide Angriffe gibt es inzwischen Appliances.

[4] https://netzpolitik.org/2017/facebook-spioniert-nutzer-seines-vpn-dienstes-aus
[5] https://heise.de/-3795523
[6] https://www.vpnmagazin.de/hidemyass-test
[7] http://t3n.de/news/lulzsec-hacker-anonymizer-hidemyass-strafverfolgung-332537
[8] https://weakdh.org

- Bei Man-in-the-Middle Angriffen lenkt der Angreifer den Datenverkehr des Clients auf seinen Server (z. B. mit DNS Manipulationen). Er gibt sich als der gewünschte VPN-Server aus, entschlüsselt den Datenverkehr und tut gegenüber dem VPN-Serven so, als ob er der Client wäre. Während der Kommunikation sitzt der Angreifer janusköpfig zwischen beiden und kann alles mitlesen.
- Bei TLS-Downgrade Angriffen stört der Angreifer den Aufbau der VPN-Verbindung immer wieder und bringt damit beide Seiten dazu, eine immer schwächere Verschlüsselung zu probieren. Wenn dann eine hinreichend schwache Verschlüsselung ausgewählt wurde, die der Angreifer knacken kann, lässt er den Aufbau der Verbindung zu.

  Appliances für TLS-Downgrade Angriffe sind military-grade Hardware hinsichtlich Geheimhaltung und Exportbeschränkungen. Ich kenne nur eine ältere Appliance, die RC4 Cipher on-the-fly brechen konnten. Auch bei der IETF hat man davon gehört und mit RFC 7465 die Verwendung von RC4 verboten.

  An dieser Stelle ein Dank an Jakob Appelbaum, der als erster darauf hinwies:

  > *RC4 is broken in real time by #NSA - stop using it.* (Nov. 2013)[9]

  (In der zivilen Kryptoanalyse ist kein Ansatz bekannt, um RC4 Cipher on-the-fly zu brechen. RC4 gilt als schwacher Cipher und konnte mit der NOMORE Attack[10] in 75h geknackt werden, um HTTPS Cookies zu entschlüsseln, und in 1h bei WPA Passwörtern. RC4 on-the-fly brechen ist bisher NSA-only Level.)

Angriffe auf die kryptografischen Schlüssel sind die logische Alternative, wenn man die Verschlüsselung nicht brechen kann.

Pre-shared Keys (PSK) können alle VPNs zur Authentifizierung nutzen. Das Programm *HappyDance* der NSA hat die Aufgabe, diese Schlüssel zu knacken um den Datenverkehr als passive Lauscher zu entschlüsseln.

Dabei kommen drei Methoden zum Einsatz:

1. Die E-Mail Überwachung wird genutzt, um in den abgefangenen Mails nach Schlüsseln zu suchen, die als pre-shared Keys für die Authentifizierung bei VPNs geeigent sein könnten. Diese Schlüssel werden gesammelt und automatisiert genutzt. (Es gibt immer Admins, die diese Schlüssel per E-Mail verteilen.)
2. Außerdem werden pre-shared Keys von interessanten VPNs mit Brute-Force-Attack angegriffen. Da diese Keys oft mit zu geringer Entropie von der VPN Software erzeugt werden (Shannon E. < 3.5), sind diese Angriffe erfolgreich.
3. In besonders hartnäckigen Fällen wird das Gruppe *Taylored Access Operations* (TAO) der NSA beauftragt, den VPN-Server oder einen beliebigen VPN-Client aus dem VPN-Netzwerk zu knacken und den pre-shared Key zu kopieren.

Pre-shared Keys sollte man nur für Testzwecke nutzen. Das StrongSwan Team warnt aufgrund der Snowden Dokumente vor dem Einsatz. Statt dessen sollte man X509v3 Zertifikate verwenden, auch wenn die Konfiguration damit komplizierter wird.

Kompromittierung der VPN-Server oder -Clients Das *OTP VPN Exploitation Team* der NSA setzt auch diese Methode gegen High-Value-Targets wie z. B. Banken ein, wenn Admins ihre VPNs professionell konfigurieren.

1. Die Gruppe Taylored Access Operations (TAO) der NSA wird damit beauftragt, den VPN-Server oder einen VPN-Client zu knacken.
2. Anschließend installiert das NSP-Team ein Implantat (Rootkit), dass die VPN-Verschlüsselung des Datenverkehrs so stark schwächt, dass sie on-the-fly gebrochen werden kann, ohne das der Admin es jahrelang bemerkt.

[9] https://twitter.com/ioerror/status/398059565947699200
[10] https://www.rc4nomore.com

Gelegentlich greift das TAO-Team die Server nicht direkt an sondern spielt über die Bande und kompromittiert zuerst die Administratoren (*Inside the NSA's Secret Efforts to Hunt and Hack System Administrators*[11]).

[11] https://theintercept.com/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/

Kapitel 13

Daten verschlüsseln

Dass die Verschlüsselung von Daten der Erhaltung der Privatsphäre dient, bemerkt man spätestens, wenn ein USB-Stick verloren geht. Wird ein Laptop gestohlen, möchte man die Fotosammlung sicher nicht im Internet sehen.

Investigative Journalisten, Rechtsanwälte und auch Priester haben das Recht und die Pflicht, ihre Informanten bzw. Klienten zu schützen. Sie sollten sich frühzeitig Gedanken über ein Konzept zur Verschlüsselung machen. Es ist wirklich ärgerlich, wenn die Rote Hilfe einen unverschlüsselten Datenträger mit Mitgliederdaten verliert. Das kann ernste Konsequenzen haben.

Als Whistleblower sind besondere Anforderungen an die Datensicherheit zu stellen. Neben der sicheren Aufbewahrung kommt es auch darauf an, keine Spuren auf den Rechnern zu hinterlassen. Im Fall Bradley Mannings konnten Forensiker viele Daten wiederherstellen.

Die kurzen Beispiele zeigen, dass unterschiedliche Anforderungen an eine Verschlüsselung bestehen können. Bevor man wild anfängt, alles irgendwie zu verschlüsseln, sollte man sich Gedanken über die Bedrohung machen, gegen die man sich schützen will:

1. **Schutz sensibler Daten** wie z. B. Passwortlisten, Revocation Certificates o.ä. erfordert die Speicherung in einem Container oder verschlüsselten Archiv, welches auch im normalen Betrieb geschlossen ist.

2. **Schutz aller persönlichen Daten** bei Verlust oder Diebstahl von Laptop oder USB-Stick erfordert eine Software, die transparent arbeitet ohne den Nutzer zu behindern und bei korrekter Anmeldung möglichst automatisch den Daten-Container öffnet (beispielsweise Veracrypt für Windows/linux oder dm-crypt für Linux).

3. **Backups auf externen Medien** enthalten in der Regel die wichtigen privaten Daten und sollten ebenfalls verschlüsselt sein. Dabei sollte die Wiederherstellung auch bei totalem Datenverlust möglich sein. Es ist nicht sinnvoll, die Daten mit einem PGP-Schlüssel zu chiffrieren, der nach einem Crash nicht mehr verfügbar ist.

4. **Daten in der Cloud** sollten ebenfalls transparent verschlüsselt werden. Außerdem sollte die Verschlüsselung die Synchronisation geänderter Dateien im Hintergrund nicht behindern. Container-basierte Lösungen wie dm-crypt oder Veracrypt sind weniger geeignet, da man bei einer kleinen Änderung nicht den gesamten Container hochladen möchte. Besser geeignet sind Verzeichnis-basierte Ansätze wie *Boxcryptor* oder *Cryptomator* (beide für Windows, MacOS, Linux und Smartphones verfügbar).

5. Wer eine **Manipulation der Systemdaten** befürchtet, kann seinen Rechner komplett verschlüsseln (z. B. mit dm-crypt für Linux).

6. **SDSRDDs** kann man nutzen, wenn Sicherheit absolute Priorität hat, Geld keine Rolle spielt und man sich nicht auf eine Softwarelösung verlassen möchte. SDSRDDs sind

SSD Festplatten mit integrierter Verschlüsselung, Token-Authentifizierung (also nicht mit Keyloggern angreifbar) und eingebautem Mechanismus zur Selbstzertörung, der remote via SMS oder bei unerlaubten Zugriff ausgelöst werden kann.

13.1 Konzepte der vorgestellten Tools

Um die vorgestellten Tools sinnvoll einzusetzen, ist es nötig, die unterschiedlichen Konzepte zu verstehen.

GnuPG arbeitet Datei-orientiert. Einzelne Dateien können verschlüsselt werden. Die unverschlüsselten Originaldateien sind danach sicher(!) zu löschen, damit keine Spuren auf der Festplatte bleiben.

Cryptomator, Boxcryptor arbeiten Verzeichnis-basiert. Es gibt zwei Verzeichnisse:

1. Das Verzeichnis A mit den verschlüsselten Daten wird auf den Datenträger geschrieben bzw. in die Cloud synchronisiert.
2. Ein zweites Verzeichnis B oder ein virtuelles Laufwerk bietet den transparenten Zugriff auf die entschlüsselten Daten.

Veracrypt, dm-crypt arbeiten Container-basiert. Es ist zuerst ein verschlüsselter Container fester Größe zu erstellen, der dann wie ein Datenträger in das Dateisystem eingebunden werden kann. Als Container können komplette USB-Sticks, ganze Partitionen der Festplatte oder (große) Dateien genutzt werden.

Ein Container nimmt immer die gleiche Menge an Platz ein, egal ob leer oder voll. Ist der Container verschlossen, kommt niemand an die dort lagernden Daten heran. Mit einem Schlüssel kann der Container geöffnet werden (gemounted: in das Dateisystem eingefügt) und jeder, der an einem offenen Container vorbeikommt, hat Zugriff auf die dort lagernden Daten. Als Schlüssel dient eine Passphrase und/oder Schlüsseldatei(en).

Der Zugriff auf Dateien innerhalb des geöffneten Containers erfolgt mit den Standardfunktionen für das Öffnen, Schließen und Löschen von Dateien. Auch Verzeichnisse können angelegt bzw. gelöscht werden. Die Verschlüsselung erfolgt transparent ohne weiteres Zutun des Nutzers.

Veracrypt - mit doppeltem Boden

Veracrypt[1] ist ein Nachfolger des legendären Truecrypt. Es beseitigt einige Schwäche, die bei einem Audit von Truecrypt[2] aufgedeckt wurden und wird als Open Source weiterentwickelt. Mit mit zuluCrypt gibt es eine 100% kompatible Linux Software.

Ein besonderes Feature von Veracrypt ist das Konzept des *versteckten Volumes*, eine Art doppelter Boden für den verschlüsselten Container. Der Zugriff auf diesen Bereich ist mit einem zweiten Schlüssel geschützt, einer weiteren Passphrase und/oder Schlüsseldatei(en). Öffnet man den Container mit dem ersten Schlüssel, erhält man Zugriff auf den äußeren Bereich. Verwendet man den zweiten Schlüssel zum Öffnen des Containers, erhält man Zugriff auf den versteckten Inhalt im doppelten Boden.

Während ein einfacher Container leicht als verschlüsselter Bereich erkennbar ist, kann der doppelte Boden innerhalb eines Containers ohne Kenntnis des zweiten Schlüssels nicht nachgewiesen werden. Ist man zur Herausgabe der Schlüssel gezwungen, kann man versuchen, nur den Schlüssel für den äußeren Container auszuhändigen und die Existenz

[1] https://www.veracrypt.fr/en/Home.html
[2] https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf

des doppelten Bodens zu leugnen.

Ob es plausibel ist, die Existenz des doppelten Bodens zu leugnen, hängt von vielen Faktoren ab. Zeigt z. B. die Historie der geöffneten Dokumente einer Textverarbeitung, dass vor kurzem auf einen verschlüsselten Bereich zugegriffen wurde, und man präsentiert einen äußeren Container, dessen letzte Änderung Monate zurück liegt, trifft man wahrscheinlich auf einen verärgerten Richter. Auch der Such-Index verschiedener Programme für die Indexierung der Dokumente auf dem lokalen Rechner (WINDOWS Suche, Google Desktop Search...) liefern möglicherweise Hinweise auf den versteckten Container.

13.2 Gedanken zur Passphrase

Die im folgenden vorgestellten Tools zur Datenverschlüsselung arbeiten in der Regel mit symetrischer Verschlüsselung (Ausnahme GnuPG: hybride Verschlüsselung).

1. Bei der Initialisierung wird eine kleine Menge von zufälligen Zufallszahlen generiert, die als Schlüssel für die symmetrische Verschlüsselung mit AES256-XTS o.ä. dient.
2. Dieser Schlüssel aus zufäligen Zufallszahlen wird mit einer Passphrase verschlüsselt und im Header der verschlüsselten Daten gespeichert.
3. Beim Zugriff auf die Daten wird zuerst der Schlüssel aus Zufallszahlen mit dem Passphrase entschlüsselt und danach für den Zugriff auf die Daten genutzt.

Es ist nach derzeitigem Stand der zivilen Kryptoanalyse unmöglich, die symmetrische Verschlüsselung wie AES-XTS oder Twofisch oder... mit mathematischen Methoden zu knacken, wenn hinreichend zufällige Zufallszahlen als Schlüssel verwendet werden.

Alle bekannten Angriffe auf moderne Datenverschlüsselungen konzentrieren sich darauf, die Passphrase zu erraten, um damit Zugriff auf den Schlüssel für die symmetrische Verschlüsselung zu bekommen und somit die geschützten Daten lesen zu können.

Die Stärke und Länge der Passphrase ist somit der entscheidende Faktor für die Sicherheit der Datenverschlüsselung und gleichzeitig auch oft das schwächste Glied in der Kette. Eine Passphrase, welche die gleiche Stärke gegen Brute-Force Angriffe wie AES128 hätte, könnte beispielsweise aus 12 zufällig generierten Wörtern bestehen (Diceware):

```
"stuff plastic young air easy husband exact install web stick hurt embody"
```

Das ist schon etwas kompliziert zu merken und in der täglichen Benutzung ganz schön umständlich. In der Regel werden die meisten Anwender einfachere Passphrasen wählen un damit ist die Passphrase der schwächsten Punkt der Verschlüsselung.

Eine gute Passphrase sollte zufällig sein, schwer zu erraten und nicht in einem Wörterbuch zu finden sein. Das die Namen von Familienangehörigen oder Haustieren ungeeignet sind, wurde in Unterhaltungsliteratur und -filmen hinreichend thematisiert. Außer Buchstaben sollte ein Passphrase auch Zahlen und Sonderzeichen enthalten.

Herausgabe von Passwörtern an Strafverfolgungsbehörden

Zur Herausgabe von Passwörtern im Fall einer Beschlagnahme des Rechners oder eines verschlüsselten Datenträgers gibt es immer wieder Missverständnisse. In Deutschland gelten folgende gesetzliche Reglungen:

- Richten sich die Ermittlungen gegen den Besitzer des Rechners oder Datenträgers, muss man grundsätzlich keine Passwörter herausgeben.
- Richten sich die Ermittlungen gegen Dritte, kann man die Herausgabe von Keys verweigern, wenn man sich auf das Recht zur Zeugnisverweigerung berufen oder glaubhaft(!) versichern kann, dass man sich damit selbst belasten würde. Im Zweifel sollte man einen Anwalt konsultieren.

In Großbritannien ist es bereits anders. Gemäß dem dort seit Oktober 2007 geltendem RIPA-Act können Nutzer von Verschlüsselung unter Strafandrohung zur Herausgabe der Schlüssel gezwungen werden. Es drohen bis zu 2 Jahre Gefängnis oder Geldstrafen. Dass die Anwendung des Gesetzes nicht auf böse Terroristen beschränkt ist, kann man bei Heise.de nachlesen. Es wurde als erstes gegen eine Gruppe von Tierschützern angewendet.[3]

Bei Einreise in die USA sind die Grenzbehörden berechtigt, elektronische Geräte (Laptops und Smartphones) zu durchsuchen. Eine Herausgabe von Passwörtern kann ohne Durchsuchungsbeschluss nicht erzwungen werden, aber die Behörden können das Gerät zur weiteren Untersuchung einziehen, wenn man das Passwort nicht herausgeben will. Die EFF.org rät, mit einer leeren, unverschlüsselten Festplatte einzureisen und ein datenloses Handy zu nutzen.[4]

Den Polizeibehörden ist bekannt, dass es starke Verschlüsselung für Festplatten gibt, die im ausgeschalteten Zustand nicht geknackt werden kann. Deshalb sind die Festnahme Spezialisten des SEK u.ä. darin geschult, bei einer Festnahme (Polizei-Sprech: *Zugriff*) die Computer im eingeschalteten Zustand zu übernehmen und ein Backup der unverschlüsselten Daten anzufertigen.

- Ross Ulbricht (der Betreiber von Silk Road 2.0) wurde festgenommen, während er seinen Tor Hidden Service administrierte. Das FBI konnte den eingeschalten Laptop übernehmen und als Beweis die aktiven Login-Sessions auf den Servern des Drogenhandelsplatzes sicherstellen. Das war sicher kein Zufall sondern beabsichtigt.
- Der deutsche Betreiber eines illegalen Waffenhandels im Deep Web konnte bei der Festnahme mit dem Fuß das Stromkabel aus seinem batterielosen Laptop reißen und die Verschlüsselung damit aktivieren. Das SEK hatte aber zweifellos den Auftrag, bei der Festnahme den Laptop im eingeschalteten Zustand sicherzustellen.[5]

[3] http://www.heise.de/newsticker/meldung/99313
[4] https://www.eff.org/wp/digital-privacy-us-border-2017
[5] http://motherboard.vice.com/de/read/bis-das-sek-kommt

13.3 Dokumente verschlüsselt speichern

Es gibt mehrere Anwendungen, die Dokumente verschlüsselt speichern können. Das Öffnen der Dokumente ist dann nur möglich, wenn das notwendige Passwort angegeben wird. Die verschlüsselte Speicherung ist bei vertraulichen Daten sinnvoll wie Steuererklärungen, Mitgliederlisten für politisch aktive Vereine. . . usw.

Man kann verschlüsselte Dokumente auch als Quick&Dirty Alternative zu verschlüsselten E-Mails verwenden, indem man den Inhalt in ein verschlüsseltes Dokument schreibt und dieses Dokument als Anhang mit der E-Mail schickt. Das Passwort zum Öffnen des Dokumentes muss man dem Empfänger über einen sicheren Kanal mitteilen.

LibreOffice Dokumente verschlüsselt speichern

LibreOffice bietet die Möglichkeit, Dokumente mit AES256 verschlüsselt zu speichern, indem man beim Speichern die Option *Mit Kennwort speichern* aktiviert. Außerdem können die Dokumente mit OpenPGP verschlüsselt gespeichert werden (Abb. 13.1).

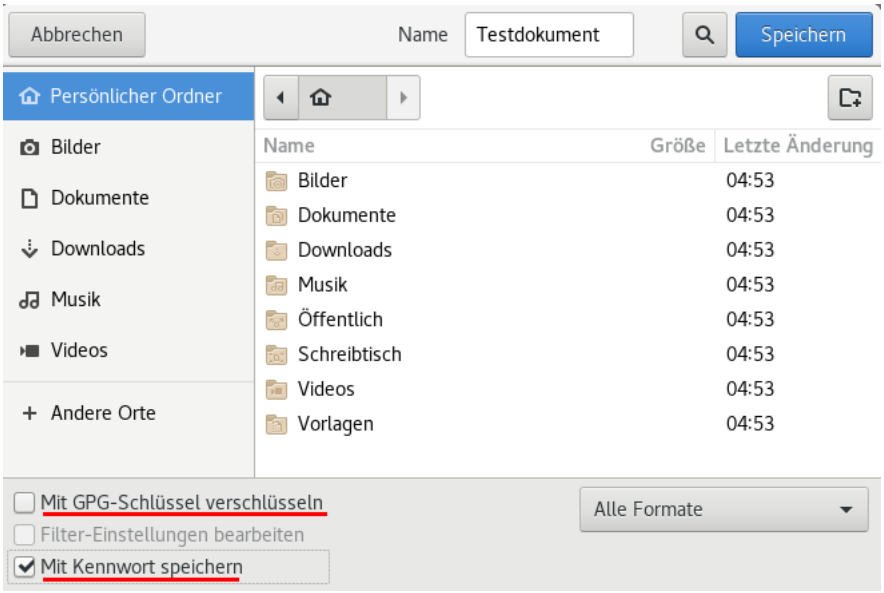


Abbildung 13.1: Verschlüsselte Speicherung in LibreOffice aktivieren

Im folgenden Dialog kann man den/die OpenPGP Schlüssel auswählen oder ein Kennwort für das Öffnen der verschlüsselten Datei festlegen. Um keine Spuren auf der Festplatte zu hinterlassen, sollte man den Schutz aktivieren, bevor das Dokument erstmalig gespeichert wird und bevor sensitive Daten in das Dokument geschrieben werden.

PDF Dokumente

Der PDF-Standard definiert ein Berechtigungsmodell, das auch die verschlüsselte Speicherung von Dokumenten ermöglicht. Dieser Standard ist aber *Broken by Design*. Ein Angreifer kann das PDF Dokument modifizieren, so dass ihm beim Öffnen des Dokumentes der vertrauliche Inhalt via Internet zugesendet wird.[6]

> *We analyze the security of encrypted PDF and show how an attacker can exfiltrate the content without having the corresponding keys.*

Die kryptografischen Signaturen im PDF Standard sind ebenfalls kaputt by Design.

[6] https://www.pdf-insecurity.org/

13.4 Quick and Dirty mit GnuPG

Eine Möglichkeit ist die Verschlüsselung einzelner Dateien oder Verzeichnisse mit GnuPG. Die grafischen Tools *GPA* (GNU Privacy Assistent) oder *Kleopatra* bieten dafür im Menü den Punkt *Datei - Datei verschlüsseln/signieren* und *Datei - Datei entschlüsseln/prüfen*.

Noch einfach geht es, wenn man im bevorzugten Dateimanager mit der rechten Maustaste auf eine Datei klickt und in dem Kontextmenü den Punkt *Datei verschlüsseln* wählt. Es startet ein Assistent, der durch die Auswahl der Schlüssel usw. führt.

Abbildung 13.2: Kleopatra GnuPG GUI: Assinstent zur Verschlüsselung von Dateien

Mit der Auswahl eines Schlüssels legt man fest, wer die Datei wieder entschlüsseln kann. Für Backups wird in der Regel der eigene Schlüssel verwendet. Es ist auch möglich, mehrere Schlüssel für verschiedene Empfänger zu nutzen. Die Verwaltung der OpenPGP Schlüssel ist im Kapitel *E-Mails verschlüsseln* beschrieben. Anschließend ist das unverschlüsselte Orginal NICHT(!) in den Papierkorb sondern in den Reißwolf zu werfen.

Sollen mehrere Dateien in einem Container verschlüsselt werden, erstellt man ein Verzeichnis und kopiert die Dateien dort hinein. Anschließend verpackt man dieses Verzeichnis mit *WinZip, 7zip* o.ä. in einem Archiv und verschlüsselt dieses Archiv.

Zum Entschlüsseln reicht in der Regel ein Klick (oder Doppelklick) auf die verschlüsselte Datei. Nach Abfrage der Passphrase für den Schlüssel liegt das entschlüsselte Orginal wieder auf der Platte.

GnuPG für WINDOWS

Diese simple Verschlüsselung klappt allerdings unter WINDOWS nicht auf Anhieb. Es ist zuerst das Programmpaket **gpg4win**[7] zu installieren.

[7] https://www.gpg4win.org

13.5 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.

Für das Backup der persönlichen Daten habe ich eine kleine Ideensammlung zusammengestellt, die keinen Anspruch auf Vollständigkeit erhebt. Grundsätzlich sollten diese Daten verschlüsselt werden. Als Schlüssel für den Zugriff sollte eine gut merkbare Passphrase genutzt werden. Keyfiles oder OpenPGP-Schlüssel könnten bei einem Crash verloren gehen.

1. Die persönlichen Daten oder einzelne Verzeichnisse mit häufig geänderten Dateien könnte man regelmäßig mit einer Kopie auf einem verschlüsselten Datenträger synchronisieren (USB-Stick, externe Festplatte). Da nur Änderungen übertragen werden müssen, geht es relativ schnell.

2. Einzelne, in sich geschlossene Projekte könnten platzsparend als komprimiertes verschlüsseltes Archiv auf einem externen Datenträger abgelegt werden.

3. Größere abgeschlossene Projekte könnten auf einem optischen Datenträger dauerhaft archiviert werden.

13.5.1 Schnell mal auf den USB-Stick

Inzwischen gibt es preiswerte USB-Sticks mit beachtlicher Kapazität. Aufgrund der einfachen Verwendung sind sie für Backups im privaten Bereich gut geeignet. Für große Datenmengen kann man auch eine externe USB-Festplatte nutzen. Wer eine Beschlagnahme der Backupmedien befürchtet, findet vielleicht eine Anregung bei true-random[8].

Das Backupmedium sollte man mit Veracrypt oder DM-Crypt komplett verschlüsseln. Die vollständige Verschlüsselung verhindert eine Manipulation des Datenträgers. Der Verfassungsschutz demonstrierte auf der CeBIT 2007, dass sich mit manipulierten Sticks Trojaner einschleusen lassen. Die vollständige Verschlüsselung des Backup Mediums macht es überflüssig, sich um eine zusätzliche Verschlüsselung der Daten beim Backup zu kümmern. Man kann die Daten nach dem Öffnen des Backup Containers einfach synchronisieren.

Die von verschiedenen Herstellern angebotenen Verschlüsselungen sind oft unsicher. USB-Datentresore mit Fingerabdruckscanner lassen sich einfach öffnen[9]. Einige USB-Sticks mit Verschlüsselung verwenden zwar starke Algorithmen (in der Regel AES256), legen aber einen zweiten Schlüssel zur Sicherheit auf dem Stick ab, der mit geeigneten Tools ausgelesen werden kann und Zugriff auf die Daten ermöglicht. Selbst eine Zertifizierung des NIST ist keine Garantie für saubere Implementierung.[10]

Unison-GTK

Für die Synchronisation der Daten steht z. B. Unison-GTK [11] für verschiedene Betriebssysteme (auch WINDOWS) zur Verfügung und bietet ein GUI für die Synchronisation. Die Installation ist einfach: Download, Entpacken und Binary starten. Linuxer können das Paket *unison-gtk* mit der Paketverwaltung installieren.

[8] http://true-random.com/homepage/projects/usbsticks/small.html
[9] http://heise.de/-270060
[10] http://heise.de/-894962
[11] http://www.cis.upenn.edu/ bcpierce/unison/

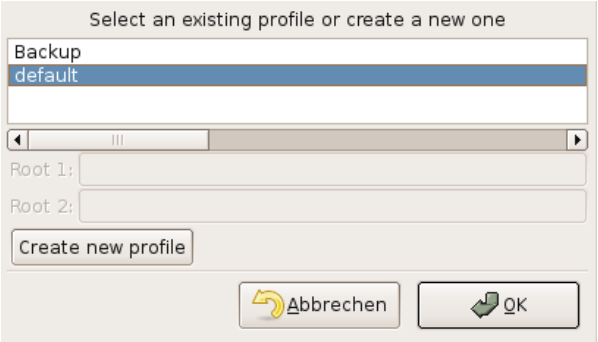


Abbildung 13.3: Profil nach dem Start von Unison-GTK auswählen

Nach dem ersten Start wählt man Quell- und Zielverzeichnis für das Default-Profil. Es ist möglich, mehrere Profile anzulegen. Bei jedem weiteren Start erscheint zuerst ein Dialog zur Auswahl des Profiles (Bild 13.3).

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.

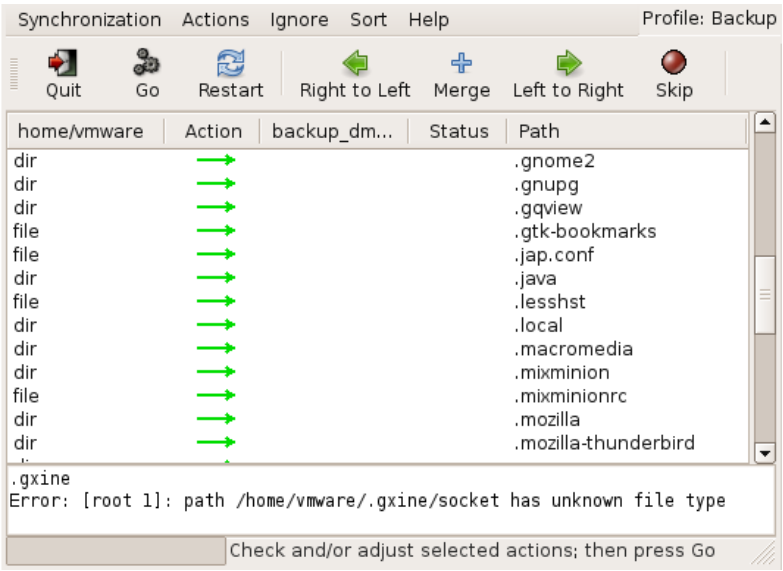


Abbildung 13.4: Hauptfenster von Unison-GTK

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

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

13.5.2 Online Backups

Neben dem Backup auf einem externen Datenträger kann man auch Online-Speicher nutzen. Bei TeamDrive.com, DataStorageUnit.com, ADrive.com, rsync.net u.v.a.m. gibt es

Angebote ab 3,- Euro monatlich. Wer einen eigenen (V)Server gemietet hat, kann seine Backups auch dort ablegen. Um die Verschlüsselung der Daten vor dem Upload muss man sich immer selbst kümmern.

Ein Online-Backup ist praktisch, wenn man mit Laptop in ein Land wie die USA reist. Bei der Einreise werden möglicherweise die Daten der Laptops gescannt und auch kopiert. Die EFF.org empfiehlt, vor der Reise die Festplatte zu "reinigen" [12]. Man könnte ein Online-Backup erstellen und auf dem eigenen Rechner die Daten sicher(!) löschen, also *shred* bzw. *wipe* nutzen. Bei Bedarf holt man sich die Daten wieder auf den Laptop. Vor der Abreise wird das Online-Backup aktualisiert und lokal wieder alles gelöscht.

Mit dem Gesetzentwurf zum Zugriff auf Bestandsdaten der Telekommunikation (BR-Drs. 664/12) vom 24.10.2012 räumt die Bundesregierung den Geheimdiensten und Strafverfolgern die Möglichkeit ein, ohne richterliche Prüfung die Zugangsdaten zum Online-Speicher vom Provider zu verlangen. Um die gespeicherten Daten, die meist aus dem Bereich *privater Lebensführung* stammen, angemessen vor dem Verfassungsschutz zu schützen, ist man auf Selbsthilfe und Verschlüsselung angewiesen.

An ein Online-Backup werden deshalb folgende Anforderungen gestellt:

- Das Backup muss auf dem eigenen Rechner ver- und entschlüsselt werden, um die Vertraulichkeit zu gewährleisten.
- Es sollten nur geänderte Daten übertragen werden, um Zeitbedarf und Traffic auf ein erträgliches Maß zu reduzieren.

duplicity ist ein kleines Backuptool für Linux, dass die Daten lokal ver- und entschlüsselt, bevor sie in einen beliebigen Cloud-Speicher hochgeladen werden. Für die unverschlüsselten Cloud-Speicher kann man Verzeichnisse transparent mit *Boxcryptor*[13] oder *Cryptomator*[14] verschlüsseln. Beide gibt es für Windows, MacOS, Linux und diverse Smartphones.

E. Snowden hat in Interviews mehrfach vor Dropbox, Facebook und Google gewarnt und den amerikanischen Cloud-Provider Spideroak empfohlen, weil dieser Cloud-Provider die Daten irgendwie verschlüsselt. E. Snowden weiß aber nicht genau, wie Spideroak die Daten verschlüsselt. Hmmm - ein US-amerikanischer Provider, der die Daten irgendwie verschlüsselt. Ist das als Empfehlung ausreichend? Nein - für uns reicht es nicht.

[12] https://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t
[13] https://www.boxcryptor.com
[14] https://cryptomator.org

Kapitel 14

Daten löschen

Neben der sicheren Aufbewahrung von Daten steht man gelegentlich auch vor dem Problem, Dateien gründlich vom Datenträger zu putzen. Es gibt verschiedene Varianten, Datein vom Datenträger zu entfernen. Über die Arbeit der einzelnen Varianten sollte Klarheit bestehen, anderenfalls erlebt man evtl. eine böse Überraschung.

14.1 Dateien in den Papierkorb werfen

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

Auch beim Löschen der Dateien in dem speziellen Müll-Verzeichnis werden keine Inhalte beseitigt. Lediglich die von den Dateien belegten Bereiche auf dem Datenträger werden als "frei" gekennzeichnet. Falls sie nicht zufällig überschrieben werden, kann ein mittelmäßig begabter Angreifer sie wiederherstellen. Forensische Toolkits wie *Sleuthkit* unterstützen dabei. Sie bieten Werkzeuge, die den gesamten, als frei gekennzeichneten Bereich, eines Datenträgers nach Mustern durchsuchen können und Dateien aus den Fragmenten wieder zusammensetzen.

14.2 Dateien sicher löschen (Festplatten)

Um sensible Daten sicher vom Datenträger zu putzen, ist es nötig, sie vor dem Löschen zu überschreiben. Es gibt diverse Tools, die einzelne Dateien oder ganze Verzeichnisse shreddern können.

- Für WINDOWS gibt es AxCrypt (http://www.axantum.com/AxCrypt). Das kleine Tool zur Verschlüsselung von Dateien integriert sich in den Explorer und stellt in der Premium Version zusätzliche Menüpunkte für das sichere Löschen von Dateien bzw. Verzeichnissen bereit.
- Unter Linux kann KGPG einen Reißwolf auf dem Desktop installieren. Dateien können per Drag-and-Drop aus dem Dateimanager auf das Symbol gezogen werden, um sie zu shreddern.
- Für Liebhaber der Kommandozeile gibt es *shred* und *wipe* für Linux. Einzelne Dateien kann man mit *shred* löschen:

  ```
  > shred -u dateiname
  ```

  Für Verzeichnisse kann man *wipe* nutzen. Das folgende Kommando überschreibt rekursiv (Option -r) alle Dateien in allen Unterverzeichnissen 4x (Option -q) und löscht anschließend das gesamte Verzeichnis.

```
> wipe -rqf verzeichnis
```

Standardmäßig (ohne die Option -q) überschreibt *wipe* die Daten 34x. Das dauert bei großen Dateien sehr lange und bringt keine zusätzliche Sicherheit.

Btrfs soll das kommende neue Dateisystem für Linux werden und wird bereits bei einigen Server-Distributionen eingesetzt. Bei diesem Dateisystem funktionieren shred und wipe NICHT. Btrfs arbeitet nach dem Prinzip *Copy on Write*. Beim Überschreiben einer Datei werden die Daten zuerst als Kopie in einen neuen Bereich auf der Festplatte geschrieben, danach werden die Metadaten auf den neuen Bereich gesetzt. Ein gezieltes Überschreiben einzelner Dateien auf der Festplatte ist bei Btrfs nicht mehr möglich.

Auch bei diesen Varianten bleiben möglicherweise Spuren im Dateisystem zurück. Aktuelle Betriebssysteme verwenden ein Journaling Filesystem. Daten werden nicht nur in die Datei geschrieben, sondern auch in das Journal. Es gibt kein Tool für sicheres Löschen von Dateien, welches direkten Zugriff auf das Journal hat. Die Dateien selbst werden aber sicher gelöscht.

14.3 Dateireste nachträglich beseitigen

Mit Bleachbit [1] kann man die Festplatte nachträglich von Dateiresten säubern. Das Programm gibt es für Windows und Linux. Linuxer können es auch aus den Repositories installieren.

Nach der Installation ist Bleachbit als Adminstrator bzw. root zu starten und nur die Option *Free disk space* zu aktivieren (Bild 14.1). Außerdem ist in den Einstellungen ein schreibbares Verzeichnis auf jedem Datenträger zu wählen, der gesäubert werden soll. Anschließend startet man die Säuberung mit einem Klick auf den Button *Clean*.

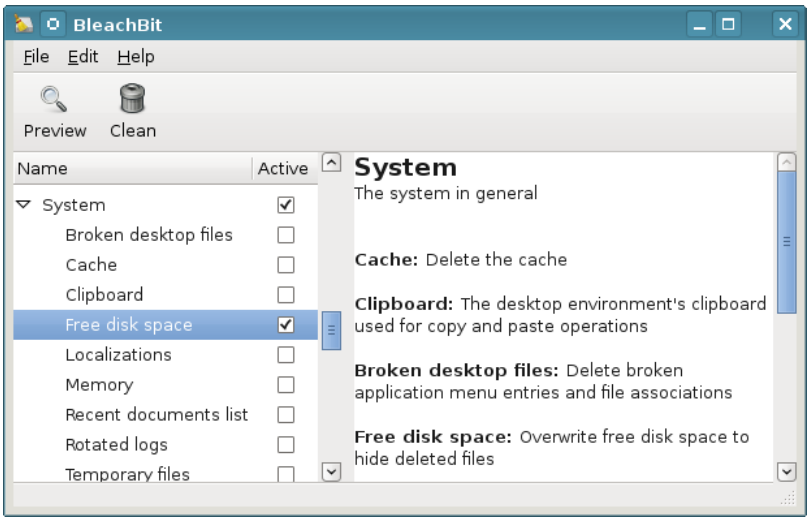


Abbildung 14.1: Bleachbit

Die Säuberung einer größeren Festplatte dauert einige Zeit. Dabei werden nur die als *frei* gekennzeichneten Bereiche überschrieben, das Dateisystem bleibt intakt.

[1] http://bleachbit.sourceforge.net/download

14.4 Dateien sicher löschen (SSDs)

Die für Festplatten emfpohlenen Tools funktionieren nicht mit Flash basierten Solid State Disks (SSDs). Um die Speicherzellen zu schonen, sorgt die interne Steuerelektronik dafür, dass für jeden Schreibvorgang andere Zellen genutzt werden. Ein systematisches Überschreiben einzelner Dateien ist nicht möglich. Mehr Informationen liefert die Publikation *Erasing Data from Flash Drives*.[2]

Für SSDs ist die TRIM Funktion zu aktivieren. Dabei werden den Speicherzellen eines Blocks einige Zeit nach dem Löschen der Datei auf den Ursprungszustand zurück gesetzt. Weitere Maßnahmen zum sicheren Löschen sind nicht nötig.

Windows aktiviert TRIM standardmäßig, wenn bei der Installation eine SSD Festplatte gefunden wurde. Mit fogendem Befehl kann man prüfen, ob TRIM aktiv ist:

```
> fsutil behavior query disabledeletenotify
```

Wenn ein Wert = 0 ausgegeben wird, ist Trim aktiviert. Wird ein Wert = 1 ausgegeben (weil man eine SSD nachträglich eingebaut hat oder den AHCI Mode im BIOS erst nachträglich aktiviert), aktivieren sie die Trim Funktion mit dem Kommando:

```
> fsutil behavior set disabledeletenotify 0
```

Mit *fsutil* wird das Trimmen lediglich aktiviert. Ob es wirklich funktioniert, kann man mit dem kleinen Tool *trimcheck*[3] prüfen. Das Tool ist in einem Verzeichnis auf dem Datenträger abzulegen, den man testen möchte, und als Administrator zu starten.

Linuxer haben für das Trimmen der Datenträger drei Möglichkeiten:

1. Standardmäßig verwenden in dem meisten Linux Distributionen *Batched TRIM*. Einmal pro Woche werden alle eingebauten SSDs gesäubert.
   Mit folgendem Kommando kann man prüfen, ob die Säuberung aktiv ist:

   ```
   > sudo systemctl status fstrim.timer
       fstrim.timer - discard unsed blocks once a week
         Loaded: loaded
         Active: active (waiting)
         ...
   ```

   Aktivierung/Deaktivierung der wöchtentliche Säuberung erfolgt mit:

   ```
   > sudo systemctl enable/disable fstrim.timer
   ```

2. Alternativ kann man *Online TRIM* verwenden, um ungenutzte Blöcke unmittelbar nach dem Löschen der Dateien zu säubern. Für unverschlüsselte Datenträger wird es in */etc/fstab* aktiviert, indem man die Mountoption *discard* hinzufügt:

   ```
   UUID=[NUMSLETTER] / ext4 discard,noatime,errors=remount-ro 0 1
   ```

   Bei LUKS verschlüsselten Datenträgern ist *Online TRIM* in */etc/crypttab* zu aktivieren, indem man die Mountoption *discard* hinzufügt:

   ```
   sda2-crypt /dev/sda2 none luks,discard
   ```

   Nach dem Ändern der Mountoptionen in */etc/fstab* oder */etc/crypttab* ist es eine gute Idee, die initramfs Images neu zu bauen:

   ```
   > sudo update-initramfs -u -k all
   ```

[2] https://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf
[3] https://github.com/CyberShadow/trimcheck

3. Außerdem kann man das Trimmen eines SSD Datenträgers per Hand starten:

   ```
   > sudo fstrim <Mountpoint>
   ```

   Linux Distributionen ohne systemd enthalten in der Regel ein Cron-Script, das wöchentlich den fstrim Befehl für alle internen Datenträger aufruft.

14.5 Gesamten Datenträger säubern (Festplatten)

Bevor ein Laptop oder Computer entsorgt oder weitergegeben wird, sollte man die Festplatte gründlich putzen. Am einfachsten erledigt man diesen Job mit Darik's Boot and Nuke (DBAN) [4] Live-CD. Nach dem Download ist das ISO-Image auf eine CD zu brennen und der Computer mit dieser CD zu booten. Es werden automatisch alle gefundenen Festplatten gelöscht - fertig.

Eine beliebige Linux Live-CD tut es auch (wenn man bereits eine Live-CD nutzt). Nach dem Booten des Live Systems öffnet man ein Terminal (Konsole) und überschreibt die gesamte Festplatte. Bei einem Aufruf wird der Datenträger 4x überschrieben, es dauert einige Zeit.

Für die erste IDE-Festplatte:

```
> wipe -kq /dev/hda
```

Für SATA- und SCSI-Festplatte:

```
> wipe -kq /dev/sda
```

Wenn die Live-DVD das Tool *wipe* nicht enthält, kann man alternativ *dd* (disk doubler) nutzen. Um die erste IDE-Festplatte einmal mit NULL und dann noch einmal mit Zufallszahlen zu überschreiben, kann man folgende Kommandos nutzen:

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

(Einmal mit NULLEN überschreiben reicht, alles andere ist paranoid.)

14.6 Gesamten Datenträger säubern (SSDs)

Das komplette Löschen einer SSD-Platte oder eines USB-Sticks funktioniert am besten, wenn der Datenträger den ATA-Befehl SECURE-ERASE unterstützt. Diese Funktion muss allerdings durch den Datenträger bereitgestellt werden. Unter Linux kann man das Tool *hdparm* nutzen, um diese Funktion aufzurufen.

Als erstes ist zu prüfen, ob SECURE-ERASE unterstützt wird:

```
> sudo hdparm -I /dev/sdX
```

Das Ergebnis muss einen Abschnitt *Security* enthalten und muss auf *not frozen* stehen. Falls die Ausgabe *frozen* liefert, wird SECURE-ERASE im Bios des Rechners blockiert.

```
Security:
    Master password revision code = 64060
        supported
    not enabled
    not locked
    not frozen
        expired: security count
        supported: enhanced erase
```

[4] http://www.dban.org/

Dann kann man ein Passwort setzen und den Datenträger vollständig löschen:

```
> sudo hdparm --user-master u --security-set-pass GEHEIM /dev/sdX
> sudo hdparm --user-master u --security-erase GEHEIM /dev/sdX
```

Falls der Datenträger SECURE-ERASE nicht unterstützt, bleibt nur das einfache Überschreiben des Datenträgers. Dabei werden aber nicht alle Speicherzellen garantiert gelöscht. Unter Linux auf der Kommandozeile wieder mit:

```
> dd if=/dev/zero of=/dev/sdc
```

14.7 Datenträger zerstören

Den Datenträger physisch zu zerstören, ist die ultimative Form der Datenvernichtung. Man kann es selbst versuchen mit Bohrmaschine und Flex in der Kellerwerkstatt oder man übergibt die Daten an professionellen Serviceanbieter, der das fachmännisch erledigt.

Die Berliner Firma Nitrokey.com bietet mit NiroShred[5] diesen Service für Privatkunden und kleinere Unternehmen in Kooperation mit der Rhenus Data Office GmbH an. Die Datenträger (SSDs, Festplatten, USB-Sticks, Handys, CDs oder DVDs) werden per Post an die Nitrokey GmbH gesendet, gesammelt der Rhenus Data Office GmbH übergeben und dort gemäß DSGVO, BDSG und DIN 66399 geshreddert. Das Material wird am Ende recycled. Somit eignet sich der Service auch zur sauberen Entsorgung von alten Smartphones (Kosten: 12,- Euro + Porto), um das grüne Gewissen ein bisschen zu beruhigen.

Hinweis: Der Postversand innerhalb Deutschlands ist vom BSI für vertrauliche Daten bis zur Geheimhaltungsstufe VS-NfD (Nur für Dienstgebrauch) zugelassen.

[5] https://shop.nitrokey.com/de_DE/shop/product/nitroshred-datentragervernichtung-on-demand-106

Kapitel 15

Daten anonymisieren

Fotos, Office Dokumente, PDFs und andere Dateitypen enthalten in den Metadaten viele Informationen, die auf den ersten Blick nicht sichtbar sind, jedoch vieles verraten können.

Fotos von Digitalkameras enthalten in den EXIF-Tags oft eine eindeutige ID der Kamera, Zeitstempel der Aufnahmen, bei neueren Modellen auch GPS-Daten. Die IPTC-Tags können Schlagwörter und Bildbeschreibungen der Fotoverwaltung enthalten. XMP Daten enthalten den Autor und der Comment üblicherweise die verwendete Software.

Office Dokumente enthalten Informationen zum Autor, letzte Änderungen, Kommentare von anderen Bearbeitern, verwendete Softwareversion u.v.a.m.

Es ist manchmal interessant, wenn man die letzten Änderungen rückgängig machen kann und sieht, welche Formulierungen oder Zahlen zuletzt geändert oder angepasst wurden. Office Dokumente sollte man NIE veröffentlichen!

PDF Dokumente enthalten ebenfalls viele Metadaten. Besonders geschwätzig sind PDFs, die mit Microsoft Office generiert wurden. Sie enthalten nicht nur beschreibende Metadaten für das Dokument sondern evtl. auch URLs, von denen Bilder eingebunden wurden, Kommentare, Lesezeichen usw.

Ein Beispiel: professionelle Personalmanager schauen sich bei online zugesendeten Bewerbungen routiniert die Metadaten der Dokumente an. Wenn der Autor des Dokumentes nicht der Bewerber selbst war sondern bspw. *bewerbungsmappe.de*, hat man Hinweise, wo die Vorlage herkommt und kann diese Informationen in die Bewertung einfließen lassen.

Vor dem Upload von Fotos und anderen Dateien ins Internet ist es ratsam, diese überflüssigen Informationen zu entfernen. Es gibt mehrere Firmen, die sich auf die Auswertung dieser Metadaten spezialisiert haben. Ein Beispiel ist die Firma Heypic, die die Fotos von Twitter durchsucht und anhand der GPS-Koordinaten auf einer Karte darstellt. Auch Strafverfolger nutzen diese Informationen. Das FBI konnte einen Hacker mit den GPS-Koordinaten im Foto seiner Freundin finden[1].

Der *StolenCameraFinder*[2] sucht anhand der KameraID in den EXIF-Daten alle Fotos, die mit dieser Digital-Kamera gemacht wurden (Smartphone Kameras werden nicht unterstützt). Da die Kamera ID mit hoher Wahrscheinlichkeit eindeutig einer Person zugeordnet werden kann, sind viele Anwendungen für diese Suche denkbar. Die verbesserte Version *CameraForensics*[3] ist nur für Strafverfolgung verfügbar.

[1] http://www.tech-review.de/include.php?path=content/news.php&contentid=14968
[2] http://www.stolencamerafinder.com
[3] https://www.cameraforensics.com

15.1 Fotos und Bilddateien anonymisieren

- **Irfan View** [4] (Windows) kann in Fotos mit *Öffnen* und *Speichern* die Metatags entfernen. Im Batchmode kann man die Funktion *Konvertieren* nutzen, um mehrere Bilder mit einem Durchgang zu bearbeiten. Man konvertiert die Fotos von JPEG nach JPEG und gibt dabei in den Optionen an, dass keine EXIF, XMP und IPTC Daten erhalten bleiben sollen.

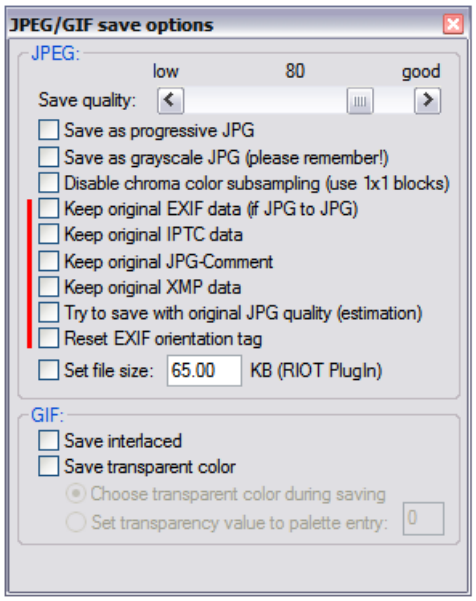


Abbildung 15.1: Informationen in Fotos löschen mit Irfan View

- **exiv2** (für Linux) ist ein nettes kleines Tool zum Bearbeiten von EXIF, XMP und IPTC Informationen in Bilddateien. Es ist in den meisten Linux Distributionen enthalten und kann mit dem bevorzugten Paketmanager installiert werden:

  ```
  > sudo apt install exiv2
  ```

  Nach der Installation kann man z. B. Fotos auf der Kommandozeile säubern:

  ```
  > exiv2 rm foto.jpg
  ```

  Das Kommando kann man als ServiceMenü für Bilddateien in verschiedene Dateimanager integrieren. Für Konqueror und Dolfin (KDE) steht eine passende Datei auf der Webseite[5] zum Download bereit.

15.2 PDF-Dokumente säubern

Man sollte ein PDF Dokument zuerst in eine neues PDF Dokument drucken, um die Metainformationen von eingebetteten Bildern und Medien zu entfernen. Dafür braucht man einen PDF-Drucker. Unter Linux stellt CUPS standardmäßig einen PDF-Drucker bereit. Unter Windows wird dieser Drucker wird z. B. vom *PDF Creator* von PDF24.org bereitgestellt. Nach der Installation des Paketes steht ein PDF-Drucker zur Verfügung.

[4] http://www.heise.de/download/irfanview.html
[5] https://www.privacy-handbuch.de/handbuch_43b.htm

Für **Windows** gibt es das Tool *BeCyPDFMetaEdit* [6] oder den *Hexonic PDF Metadaten Editor*[7], um die Metadaten aus PDF Dokumenten zu entfernen. Nach dem Download und evtl. der Installation kann man das Tool starten und die zu säubernden PDF-Dokumente laden. Auf den Reitern *Metadaten* und *Metadaten (XMP)* klickt man auf den Button *Alle Felder löschen* und speichert das gesäuberte Dokument.

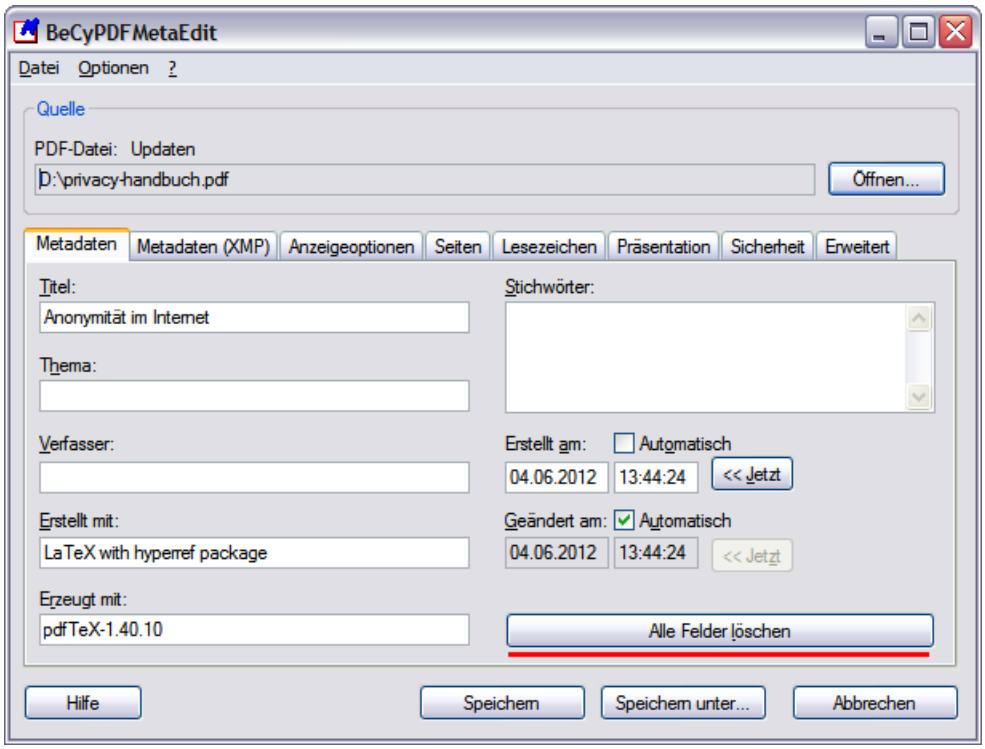


Abbildung 15.2: Metadaten in PDF-Dokumenten löschen

[6] http://www.becyhome.de/download_ger.htm
[7] http://www.hexonic.de/index.php/hexonic-pdf-metadata-editor

Kapitel 16

Daten verstecken

Geheimdienste orakeln seit Jahren immer wieder, dass *Terroristen* über versteckte Botschaften in Bildern kommunizieren. Telepolis berichtete 2001 und 2008 kritisch-ironisch über Meldungen von Scotland Yard, wonach islamische Terroristen ihre Kommunikation in pornografischen Bildern verstecken würden. Stichhaltige Belege für die Nutzung von **Steganografie** konnten bisher nicht geliefert werden. Andere Journalisten hinterfragten die Meldungen weniger kritisch:

"Bislang ist zwar noch nicht bewiesen, ob die Terrorverdächtigen die Bilder - bei einem Verdächtigen wurden 40.000 Stück gefunden - nur zum persönlichen Vergnügen heruntergeladen haben oder ob tatsächlich ein Kommunikationsnetzwerk aufgebaut wurde." (Welt Online[1], wieder einmal viel heiße Luft.)

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

Ein Beispiel

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

```
Morgen!
```

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

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

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

Ein Beobachter könnte auf den Gedanken kommen: *"Was - wieso Radio? Der zahlt doch keine GEZ!"* Er wird aufmerksam und mit ein wenig Probieren kann 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.

[1] http://www.welt.de/politik/article2591337/

16.1 Allgemeine Hinweise

Das Beispiel verdeutlicht, welche Voraussetzungen für die Nutzung von Steganografie zum Austausch von versteckten Botschaften gegeben sein müssen:

- Sender und Empfänger müssen sich darüber verständigt haben, wie die Nutzdaten versteckt werden.
- Das Passwort für die Verschlüsselung muss ausgetauscht werden.
- Die Modalitäten für den Austausch der Trägermedien müssen geklärt werden. Wo kann der Empfänger die Fotos mit den versteckten Botschaften finden?

Wenn diese Vorausetzungen geklärt sind, kann es losgehen

1. Der Absender schreibt seine Botschaft mit einem einfachen Texteditor.
2. Die Textdatei wird in einem (anonymisierten) Foto oder in einer Audiodatei mit Steganografie Tools wie z. B. *DIIT* oder *steghide* versteckt und gleichzeitig mit dem Passwort verschlüsselt.
3. Das Foto könnte man dem Empfänger per E-Mail senden. Das ist aber nicht unbedingt die beste Idee, da dabei die Metadaten der Kommunikation ausgewertet werden können (A hat B eine Mail geschrieben, Stichwort: Kommunikationsanalyse). Um auch die Metadaten der Kommunikation zu verstecken, könnte der Absender das Foto in seinem (anonymen) Blog veröffentlichen, man könnte es bei Flickr oder Twitpic hochladen oder an eine öffentliche Newsgruppe im Usenet senden. Wichtig ist, dass es öffentlich publiziert wird und der Empfänger nicht erkennbar ist. Außerdem kann der Absender verschiedene Maßnahmen ergreifen, um selbst anonym zu bleiben.
4. Der Empfänger muss wissen, wo er aktuelle Nachrichten finden kann. Fotos oder Audiodateien, in denen der Empfänger eine Botschaft vermutet, sind herunterzuladen.
5. Danach kann der Empfänger versuchen, die geheime Botschaft aus dem Trägermedium zu extrahieren. Dabei ist das gleiche Tool wie beim Verstecken zu verwenden. Wenn er alles richtig macht und das korrekte Passwort verwendet, wird die Textdatei extrahiert und kann mit einem einfachen Texteditor gelesen werden.

Unsichtbare Markierungen, Wasserzeichen

Man kann Steganografie Tools auch nutzen, um unsichtbare Wasserzeichen an Bildern oder Audiodateien anzubringen.

Wenn Fotos oder Videos nur einem kleinen Kreis von Personen zugänglich gemacht werden sollen, dann können individuelle Wasserzeichen steganografisch in den Dateien versteckt werden. Sollten diese Fotos oder Videos in der Öffentlichkeit auftauchen, kann das Leck anhand des unsichtbaren steganografischen Wasserzeichens ermittelt werden.

16.2 steghide

steghide ist ein Klassiker unter den Tools für Steganografie und wird auf der Kommandozeile gesteuert. Es kann beliebige Daten verschlüsselt in JPEG, BMP, WAV oder AU Dateien verstecken. Die verwendeten Algorithmen sind sehr robust gegen statistische Analysen. Die Downloadseite bietet neben den Sourcen auch Binärpakete für WINDOWS. Nutzer von Debian und Ubuntu installieren es wie üblich mit *aptitude*.

Um die Datei *geheim.txt* zu verschlüsseln und in dem Foto *bild.jpg* zu verstecken, ruft man es mit folgenden Parametern auf (mit dem Paramter -sf kann optional eine dritte Datei als Output verwendet werden, um das Original nicht zu modifizieren):

```
> steghide embed -cf bild.jpg -ef geheim.txt
Enter passphrase:
Re-Enter passphrase:
embedding "geheim.txt" in "bild.jpg"... done
```

Der Empfänger extrahiert die geheimnisvollen Daten mit folgendem Kommando (mit dem Parameter -xf könnte ein anderer Dateiname für die extrahierten Daten angegeben werden):

```
> steghide extract -sf bild.jpg
Enter passphrase:
wrote extracted data to "geheim.txt".
```

Außerdem kann man Informationen über die Coverdatei bzw. die Stegodatei abfragen. Insbesondere die Information über die Kapazität der Coverdatei ist interessant, um abschätzen zu können, ob die geheime Datei reinpasst:

```
> steghide info bild.jpg
    Format: jpeg
    Kapazität: 12,5 KB
```

16.3 stegdetect

Auch die Gegenseite ist nicht wehrlos. Manipulationen von steghide, F5, outguess, jphide usw. können z. B. mit *stegdetect* [2] erkannt werden. Ein GUI steht mit *xsteg* zur Verfügung, die Verschlüsselung der Nutzdaten kann mit *stegbreak* angegriffen werden. Beide Zusatzprogramme sind im Paket enthalten.

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

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

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

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

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

Antwort: Ja - und das geht so:

1. Der professionelle Forensiker erstellt zuerst eine 1:1-Kopie der zu untersuchenden Festplatte und speichert das Image z. B. in *terroristen_hda.img*

2. Mit einem kurzen Dreizeiler scannt er alle 40.000 Bilder in dem Image:

[2] http://www.outguess.org/download.php

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

(Für Computer-Laien und WINDOWS-Nutzer sieht das vielleicht nach Voodoo aus, für einen Forensiker sind das jedoch Standardtools, deren Nutzung er aus dem Ärmel schüttelt.)

3. Nach einiger Zeit wirft man einen Blick in die Datei *ergebnis.txt* und weiß, ob es etwas interessantes auf der Festplatte des Terroristen gibt.

Kapitel 17

Live-DVDs

Es gibt einige Projekte, die fertig konfigurierte Live-DVDs bereitstellen. Bei der Nutzung einer Live-DVD erhält man ein sinnvoll vorkonfiguriertes und garantiert sauberes System ohne Trojaner. Da man keine Updates einspielen kann, sollte man regelmäßig eine aktuelle Version des ISO-Images von der Webseite herunterladen.

Linux Fast alle Linux-Distributionen und einige BSD-Derivate stellen Live-DVDs bereit. *The LiveCD List*[1] bietet eine Übersicht. Man kann diese Live-DVDs zum Kennenlernen nutzen oder für viele kleine Aufgaben, die ein sauberes System erfordern.

TAILS *The Amnesic Incognito Live System* ist die offizielle Live-DVD von Torproject.org. Der gesamte Datenverkehr ins Internet wird in der Standardkonfiguration durch Tor geschickt. TAILS bietet die Anonymisierungsdienste Tor und I2P.

17.1 USB-Sticks als Bootmedium vorbereiten

Für TAILS wird alle 6-8 Wochen eine aktualisierte Version zum Download freigegeben. Deshalb verwende ich USB-Sticks als Boot Medium statt DVDs. Regelmäßige Aktualisierung ist (nicht nur) für sicherheitsrelevante Software ein Muss. Auch andere Live-DVDs lassen sich auf USB-Sticks leichter verwenden.

Windows: Mit dem *Easy Universal USB Installer* von Pendrivelinux.com kann man einfach einen bootfähigen USB-Stick aus einem Linux ISO-Image erstellen. Mit dem *YUMI Multiboot USB Creator* kann man mehrere Systeme auf den USB-Stick packen.

Nach dem Download ist die EXE-Datei zu starten (keine Installation nötig). Man wählt die Option *Try unlisted Linux ISO image*, das herunter geladene ISO-Image und außerdem den USB-Stick, der verwendet werden soll.

17.2 BIOS-Einstellungen für Win8+ Rechner

TAILS und Debian Live-DVDs unterstützen kein Secure Boot. Um diese Live-DVDs mit modernen Windows 8+ kompatiblen Rechnern zu nutzen, sind Anpassungen an den BIOS-Einstellungen nötig. Sonst erhält man beim Booten des Live-Systems den Fehler:

```
Image Authorization Fail
System can not boot this device due to Security Violation.
```

Wie man die BIOS-Einstellungen öffnet, ist von Rechner zu Rechner unterschiedlich. Üblicherweise muss man in den ersten 1-2 Sekunden beim Booten des Rechners die Taste F1, F2 oder ENTF drücken. Mein Laptop hat eine extra Taste dafür. Das Handbuch zur

[1] https://livecdlist.com/

Abbildung 17.1: Easy Universal USB Installer

Hardware liefert konkrete Antworten.

In der Sektion *Boot* in den BIOS-Einstellungen muss man die Option *Secure Boot* deaktivieren. Bei einigen Computern versteckt sich diese Option hinter *OS Selection* und man muss *WIN 7/others OS* wählen.
Außerdem sollte man *PXE-Boot* deaktivieren (siehe: DHCP Privacy).

Zur Vereinfachung in der täglichen Nutzung kann man die Bootreihenfolge im BIOS ändern. Standardmäßig bootet der Computer das OS vom DVD-Laufwerk oder der ersten Festplatte. Man kann den USB-Stick als erstes Boot Medium setzen. Dann bootet das installierte OS nur, wenn der USB-Stick nicht angesteckt ist.

Alternativ kann man das beim Starten des Rechners das *BIOS Boot Select Menü* aufrufen (bei PCs üblicherweise mit den Tasten F8, F10 oder F12, bei Macs die ALT-Taste gedrückt halten), wenn man den USB-Stick nutzen will. Das Handbuch zur Hardware liefert wieder konkrete Antworten.

Kapitel 18

Smartphones

> *Wenn mir früher jemand gesagt hätte, ich würde freiwillig eine Wanze mit mir herum tragen und sie auch noch selbst aufladen, hätte ich laut gelacht. Heute habe ich ein Smartphone.*

Braucht man das Ding wirklich oder ist es nur ein nettes Lifestyle Gadget? Für den Berliner Philosophen und Medientheoretiker Byung-Chul Han sind Smartphones das wesentliche Element zur Kontrolle der Bevölkerung im Zeitalter der Psychomacht:

> *Jede Herrschaftstechnik bringt eigene Devotionalien hervor, die zur Unterwerfung eingesetzt werden. Sie materialisieren und stabilisieren die Herrschaft ... Das Smartphone ist eine digitale Devotionalie, ja die Devotionalie des Digitalen überhaupt. Es funktioniert wie der Rosenkranz. Beide dienen der Selbstprüfung und Selbstkontrolle. Like ist das digitale Amen. Das Smartphone ist nicht nur ein effizienter Überwachungsapparat, sondern auch ein mobiler Beichtstuhl. Facebook ist die Kirche, die globale Synagoge.*

(Für manche Leute ist es Facebook, für andere Instagram oder Twitter oder. . . - aber immer ist man online und auf der Jagd nach Likes.)

Mit der zunehmenden Verbreitung von Smartphones entstehen neue Gefahren für die Privatsphäre, die deutlich über die Gefahren durch datensammelnde Webseiten beim Surfen oder E-Mail scannen bei Mail Providern wie Google hinaus gehen. Da wir die handliche Wanze immer mit uns umhertragen und unterwegs nutzen, ist es möglich, komplexe Bewegungsprofile zu erstellen und uns bei Bedarf zu lokalisieren. Greg Skibiski beschrieb 2009 im Interview mit Technology Review seine Vision von einer Zukunft mit breiter Auswertung der via Smartphone gesammelten Daten wie folgt:

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

10 Jahre später sind die Vision von Greg Skibiski Wirklichkeit. Bewegungsdaten von Smartphones werden im Corona-Jahr 2020 routiniert verwendet, um die Bevölkerung zu durchleuchten und mehr oder weniger interessante Analysen zu veröffentlichen:

- Das Statistische Bundesamt analysiert die Veränderungen der Fahrgastzahlen der Deutschen Bahn nicht anhand der Verkäufe von Fahrkarten und Platzkarten (was vielleicht naheliegend wäre) sondern anhand der Bewegungsdaten von Mobiltelefonen. Ergebnis: die Fahrgastzahlen sind 2020 um 50% niedriger als im Vorjahr.
- Dez. 2020 veröffentlichte das Statistische Bundesamt eine weitere Studie auf Basis anonymisierter Bewegungsdaten von Mobiltelefonen und kommt zu dem Schluss, dass die Mobilität in großen Stadten wie Berlin und Hamburg durch Corona um 19% niedriger ist als im Vorjahr, in Bremen um 16% und deutschlandweit um 8,5%.
- Forscher der Universität Stanford kamen durch Auswertung der Standortdaten von Mobiltelefonen von 100 Mio. Menschen in 10 großen US-Städten zu der Erkenntnis,

das sich die Ansteckungsgefahr mit Corona in Restaurants um 80% verringern würde, wenn die Restaurants 80% weniger Plätze anbieten würden.

Gleichzeitig würde sich der Umsatz der Restaurants um 42% reduzieren, was evtl. nicht mehr kostendeckend wäre aber besser als eine vollständige Schließung.

Man sollte sich darüber im Klaren sein, dass es gegen die Lokalisierung und Beobachtung von Bewegungsprofilen keinen technischen Schutz gibt.

18.1 Kommerzielle Datensammlungen

Bei den möglichen Gewinnen durch die Auswertung und Verarbeitung von Daten, die mit Smartphones und Apps gesammelt werden, wundert es nicht, dass viele Teilnehmer aggressiv bei den Datensammlungen beteiligt sind.

18.1.1 Datensammlungen der Smartphone Hersteller

iPhones: In Apples Datenschutzbestimmungen räumt der Konzern sich das Recht ein, den Standort des Nutzers laufend an Apple zu senden. Apple wird diese Daten Dritten zur Verfügung stellen. Damit begann die heute allgegenwärtige Datensammlung im Gerät und für diese Innovation wurde Apple mit dem BigBrother 2011 geehrt.

Seit iOS Version 8 übertragen Apples Mobilgeräte automatisch die Liste der Telefonanrufe an Apple-Server (Telefonnummer, Datum/Uhrzeit, Dauer). Diese Datenspeicherung kann man nur verhindern, wenn man die iCloud komplett abschaltet.

Mit iOS Version 10 hat Apple diese Datenspeicherung ausgeweitet und überträgt die Metadaten der Kommunikation von allen Apps in die Apple Cloud, die mit CallKit-Unterstützung eingehende Anrufe auf dem Lockscreen anzeigen. Das betrifft neben Telefonie und SMS auch iMessage, WhatsApp, Skype und andere verschlüsselten VoIP Telefonate sowie Kommunikation via Messenger. Apple nennt es Call History.

Mit iOS Version 13 wird die Call History verschlüsselt in der Cloud gespeichert.

Die Kommunikationsdaten werden für 4 Monate im iCloud-Konto des Benutzers gespeichert und können dort ggf. von Behörden abgegriffen und für die Kommunikationsanalyse genutzt werden. Die Firma Elcomsoft bietet Geheimdiensten Tools, um diese Daten zu erschließen. Nur wenn die 2-Faktor-Authentifizierung für den Zugriff auf die iCloud aktiviert wurde, stellt die mit iOS 13 eingeführte Verschlüsselung die Geheimdienste vor ernsthafte Probleme.

Google Android: die tief im System verankerte Google Play Service App sendet alle 20min folgende Daten an Google:

- Telefonnummer und SIM-Kartennummer
- Gerätenummer (IMEI) und Seriennummer des Gerätes
- WLAN-MAC-Adresse und IP-Adresse
- Andoid-ID (E-Mail Adresse des Google Kontos)
- Standort (wenn die *Standortverfolgung* aktiv ist)

Mit Android 10 hat Google für Apps den Zugriff auf eindeutige Hardwarekennungen wie IMEI, SIM, Seriennummer, MAC Adressen usw. allgemein verboten und nur für eine restriktiv gepflegten Liste von Ausnahmen zugelassen. Apps sollen die Werbe-ID für das Tracking nutzen, die der Nutzer neu auswürfeln oder löschen kann. Den Zugriff auf eindeutigen Hardwarekennungen beansprucht Google exklusiv für sich.

Auch Googles Smartphones übertragen seit April 2016 die gesamte Call History (Telefonnummer, Datum/Uhrzeit, Dauer). Zur Call History gehören auch die Metadaten verschlüsselter Anrufe mit Messenger Apps wie Signal, Telegram, Elements oder Videokonferenzen via Zoom App. In Googles Datenschutz Policy steht:

> *Wenn Sie unsere Dienste nutzen, um Anrufe zu tätigen und zu erhalten oder um Nachrichten zu senden und zu empfangen, erheben wir möglicherweise Telefonie-Informationen wie Ihre Telefonnummer, die Anrufernummer, die Nummer des Angerufenen, Weiterleitungsnummern, das Datum und die Uhrzeit von Anrufen und Nachrichten, die Dauer, Routing-Informationen und die Art der Anrufe.*

Die Call History wird wie alle anderen Daten für die Optimierung der Werbung verwendet und auch an Werbepartner weitergegeben. Anhand der Daten werden Vermutungen über sexuelle Vorlieben, politische Orientierung und andere Themen erstellt. Die Privacy Policy von Google beschreibt es als gaaaanz harmlos:

> *Diese Daten verwenden wir beispielsweise, um Ihnen ein YouTube-Video zu empfehlen, das Ihnen gefallen könnte.*

Da Google seit 2009 Partner im PRISM Spionageprogramm der NSA ist, kann man wohl davon ausgehen, dass…

Neben Google können auch Apps die Call History absaugen, wenn sie die Berechtigung *Reading SMS and Call Logs* haben. Die Facebook App[1] nutzte natürlich diese Möglichkeit und sammelte die Call History von Smartphones ein, auf denen die App installiert war. Seit 2019 hat Google diese Berechtigung für Apps etwas eingeschränkt. Apps benötigen eine Erlaubnis von Google für den Zugriff auf die Call History.[2]

Es ist manchmal verwunderlich, wenn Leute seit 20 Jahren gegen die gesetzliche Verpflichtung zur Vorratsdatenspeicherung (bzw. Mindestspeicherpflicht) kämpfen und bei ihren Lieblings-Lifestyle-Gadgets keine Probleme damit haben, wenn Apple oder Google die Kommunikationsdaten freiwillig auf Vorrat sammeln und Behörden zur Verfügung stellen.

Huawei Android: Aufgrund der US-Sanktionen gegen Huawei werden die aktuellen Smartphones des chinesischen Konzerns ohne Google Dienste und Zugriff auf den Google Playstore ausgeliefert. Google-freie Huawei Phones übertragen keine Call History in die Cloud. (Ein Backup der Call History kann auf einen Datenträger erfolgen und dann auf ein neues Smartphone übertragen werden (wenn gewünscht).)

Es werden nur die Standortortdaten an Server von Huawei übertragen, wenn man Apps aktiv nutzt, die auf den Standort zugreifen und dabei Informationen über WLANs in der Umgebung zur Verbesserung der Genauigkeit verwenden.

/e/ Android: Die googlefreien Smartphones der /e/ Foundation mit dem installiertem Custom ROM /e/ verwenden standardmäßig keine Cloud Dienste und übertragen keine Daten an die /e/ Foundation. Um Cloud Funktionen zu nutzen, kann man einen Account bei der /e/ Cloud erstellen oder eine eigene Nextcloud Instanz nutzen.

Erfahrene Nutzer können das Costum ROM von /e/ auch auf einem vorhandenen Google Smartphone installieren und damit Google rauswerfen. Es werden aktuell 93 Android Smartphones unterstützt (Stand Okt. 2020).

18.1.2 Datensammlungen mit Smartphone Apps

Standortdaten: Tausende Apps sammeln überflüssigerweise Standort- und Bewegungsdaten der Nutzer. Der ehem. Bundesdatenschutzbeauftragte erwähnt beispielsweise eine App, die das Smartphone zur Taschenlampe macht und dabei den Standort an den Entwickler der App sendet (vielleicht lustig bis harmlos?)

Weniger lustig wird es, wenn die *Muslim Prayer App* mit mehr als 98 Mio. Nutzern weltweit, die nur an das Gebet erinnert und die Richtung nach Mekka anzeigt, oder die populäre *Muslim Dating App* Standortdaten sammeln und an die Firma Locate X senden. Die Daten werden vom US-Militär gekauft und zur Planung von gezielten

[1] https://www.theverge.com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android
[2] https://android-developers.googleblog.com/2019/01/reminder-smscall-log-policy-changes.html

Tötungen mit Drohnen genutzt. Außerdem kauft das U.S. Special Operations Command (USSOCOM) diese Daten zur Planung und Unterstützung von verdeckten Special Forces Einsätzen. Secret Service und US Customs and Border Protection (CBP) sind weitere Kunden, die die Datensammlung von Locate X abonniert haben.[3] [4]

Außerdem zahlt US Customs and Border Protection (CBP) jährlich fast eine halbe Mio. Dollar an die Firma Vettel für den Zugriff auf die Standort- und Bewegungsdaten. Auch die US-Immigrationspolizei (ICE) gehört zu den Kunden von Venntel. Die Firma kauft Daten von harmlosen Wetter Apps und Spielen und bereitet sie auf.[5]

Der norwegische Journalist M. Gundersen hat in einer Recherche die Datensammlung der Firma Venntel genauer analysiert. Im Februar 2020 hat er auf einem neuen Smartphone 160 Apps installiert und dieses Smartphone ständig bei sich getragen. Keine der 160 Apps nannte die Firma Venntel in ihren Datenschutzklauseln.[6]

Im August forderte er von Venntel Einsicht in die Daten, welche die Firma über ihn gesammelt hatte. Zur Identifizierung übergab er die Advertising-ID des Smartphone. Als Antwort erhielt er 75.406 Datenpunkte mit Location und Zeitstempel, die in den 6 Monaten gesammelt wurden. Anhand der Daten konnte sein Wohnort, seine Arbeitstelle und auch seine Wanderungen in der Freizeit nachvollzogen werden sowie jede Bank, auf der er sich während der Wanderung ausgeruht hatte. Abb. 18.1 zeigt den Ausschnitt von 36min aus einer Wanderung mit einer Rast.

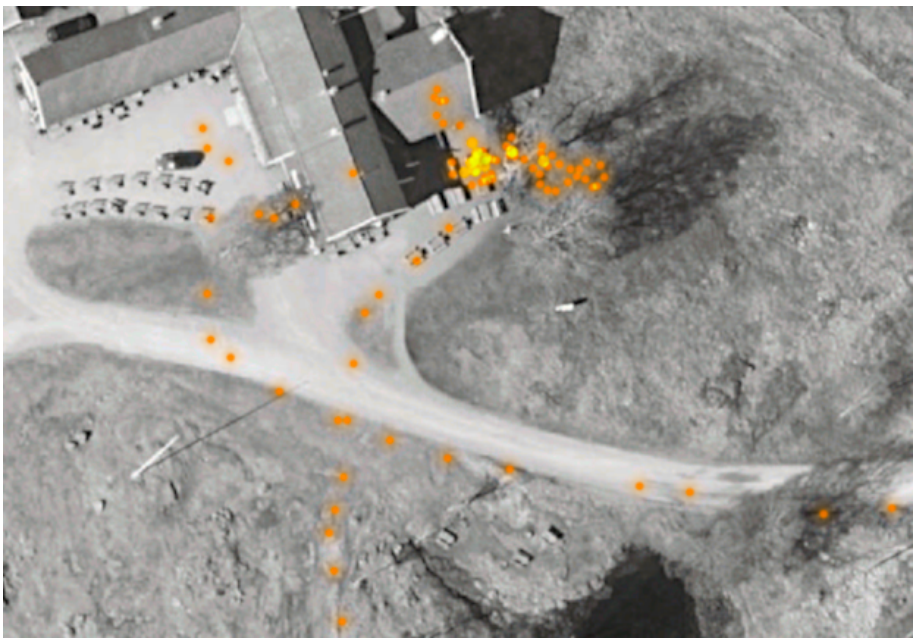


Abbildung 18.1: Illustration: Harald K. Jansson/Norge i bilder

Venntel informiert M. Gundersen auch darüber, dass seine Daten an die zahlenden Kunden der Firma weiterverkauft wurden, nannte aber keine Namen von Kunden.

In weiteren Recherchen konnte M. Gundersen ermitteln, das Venntel die Daten u.a. von der französischen Firma Predicio und von der US-Firma Complementics kauft. Ein großer Teil der ortsbezogenen Daten stammt außerdem von dem slowakischen Unternehmen Sygic, das ein Portfolio von 70 Apps anbietet.

[3] https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x
[4] https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street
[5] https://www.vice.com/en/article/k7qyv3/customs-border-protection-venntel-location-data-dhs
[6] https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants

Neben Locate X und Venntel ist die Firma Anomaly Six ein weiterer Baustein bei der Sammlung von Standort- und Bewegungsdaten für US-Behörden und Geheimdienste. Das SDK der Firma Anomaly Six wurde in 500 Apps eingebaut und die Entwickler dafür bezahlt. Diese Apps senden damit laufend die Standortdaten von einigen hundert Mio. Nutzern an das US-amerikanische Unternehmen. Anomaly Six analysiert die Bewegungsmuster von Personen und Gruppen und verwendet nach eigenen Angaben noch weitere Datenquellen. Die Ergebnisse der Analyse werden an US-Firmen weiter verkauft und die Daten von Nicht-US-Bürgern auch an US-Behörden.[7]

Für den Daten- und Überwachungsforscher Wolfie Christl hat diese Form der Überwachung eine völlig neue Qualität:

> *Ich habe das Gefühl, dass viele nicht verstehen, dass dies völlig beispiellos ist und anders als das ist, was Edward Snowden im Jahr 2013 aufdeckte.*
>
> *Statt kompliziertem Schnüffeln im Traffic ist die US-Regierung jetzt ein weiterer Marktteilnehmer in einer bestehenden kommerziellen Trackingwirtschaft.*

Fun Fact: Die NSA forderte im August 2020 die Mitarbeiter in der Spionage Community auf, auf den privaten Smartphones die Nutzung von Apps mit Standortverfolgung stark einzuschränken, weil auch andere Staaten diese Möglichkeiten nutzen.

Browserverlauf: Die Spiele der Hersteller iApps7 Inc, Ogre Games und redmicapps gehen in ihrer Sammelwut so weit, dass sie von Symantec als Malware eingestuft werden. Die Spiele-Apps fordern folgende Rechte um Werbung einzublenden:

- ungefährer (netzwerkbasierter) Standort
- genauer (GPS-)Standort
- uneingeschränkter Internetzugriff
- Browserverlauf und Lesezeichen lesen
- Browserverlauf und Lesezeichen erstellen
- Telefonstatus lesen und identifizieren
- Automatisch nach dem Booten starten

Auch Spiele von Disney verlangen sehr weitreichende Freigaben, so dass sie nur als Spionage-Tools bezeichnet werden können.

Adressbücher: Viele Apps beschränken sich nicht auf die Sammlung von Standortdaten und Anzeige von Werbung. Die folgenden Apps lesen die Kontaktdaten aus dem Adressbuch und senden sie ohne Freigabe durch den Nutzer an den Betreiber:

- die Social Networks *Facebook*, *Twitter* und *Path*
- die Location Dienste *Foursquare*, *Hipster* und *Foodspotting*
- die Fotosharing App *Instagram*
- die VoIP Software *Viper* sowie verschiedene Messaging Dienste
- ...

Politisch brisant können diese Datensammlungen werden, wenn z. B. Twitter alle Daten von Wikileaks Unterstützern an die US-Behörden herausgeben muss. Damit geraten auch die Freunde von Wikileaks Unterstützern als potentiell suspekte Individuen ins Visier von US-Behörden, was u.U. unerwünschte Konsequenzen haben kann.

Über die Firma Viper findet man kaum Angaben. Sitzt die Firma in Zypern, Israel, USA oder Weissrussland? Die auf der Webseite angegebene Kontakt-Adresse ist ein Briefkasten auf Zypern, Telefonnummern haben amerikanische Vorwahlen und die Domain versteckt sich hinter Domains by Proxy. Trotzdem haben bisher 50 Millionen Nutzer die Liste ihrer persönlichen Kontakte der Firma zur Verfügung gestellt.

[7] https://www.wsj.com/articles/u-s-government-contractor-embedded-software-in-apps-to-track-phones-11596808801

Analytics: Viele Smartphone Apps enthalten datensammelnde Bibliotheken von Dritten. Führend sind dabei Google (in 50% aller Apps) und Facebook (in 30% aller Apps). Die in den Apps enthaltenen Bibliotheken sammeln fleißig Daten über jede Interaktion des Nutzers mit der App oder Standortdaten oder... und schicken sie an die großen Datensammler. Als Gegenleistung bekommen die Entwickler Analysedaten über das Nutzerverhalten ihrer App, Crashreports und Einnahmen durch Werbung.

Die Datenkonzerne werten die Daten natürlich parallel auch für ihre Interessen aus. So sammelt Facebook beispielsweise über diesen Weg große Mengen an Daten über Nichtmitglieder, die in sogenannten Schattenprofilen geführt werden.

Die Webseite **Exodus Privacy**[8] hat 52.000+ Android Apps analysiert und sammelt weiterhin Analysen von Apps. Die Übersicht der Tracker zeigt, dass am häufigsten Google Tracking Bibliotheken verwendet werden und das Facebook an zweiter Stelle steht. Bibliotheken für Werbung und Analytics werden besonders gern verwendet, da sie jede Aktion des Nutzers protokollieren und an Google, Facabook o.a. senden.

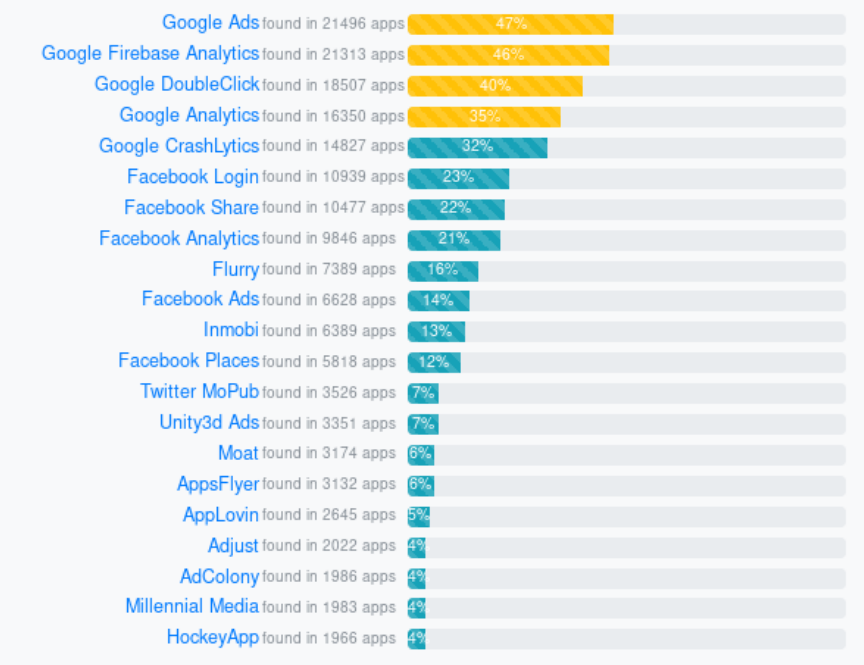


Abbildung 18.2: Die häufigsten Tracking Bibliotheken in Android Apps

Neben den negativen Beispielen mit mehr als 30 Tracking Bibliotheken in einzelnen Apps findet man auf Exodus Privacy auch positive Beispiele ohne Tracker[9]. Wenn man eine App für eine bestimmte Aufgabe sucht, findet man dort Alternativen ohne Tracker (wobei ich Crash Reporting Bibliotheken als unkritisch einstufen würde).

Hinweis: man muss nicht immer für jeden Anwendungsfall eine App nutzen. Viele Dienste bieten eine Smartphone-taugliche Webseite im responsive Design, die mit einem privacy-freundlichen Browser (z. B. Firefox Klar) genutzt werden kann.

Passwörter: Einige E-Mail Apps übertragen bei Einrichtung eines E-Mail Accounts die E-Mail Adresse und das Passwort für den Account an den Hersteller der App. Hey - das nennt man Phishing und nicht Service!

Die Server der App Hersteller verwenden die Login Credentials, um sich bei dem externen E-Mail Account einzuloggen und nach neuen E-Mails zu suchen. Sie laden die Mails auf den eigenen Server, beschnüffeln sie manchmal ein bisschen und benachrichtigen den Nutzer dann per Google Push Service über neue E-Mails.

[8] https://reports.exodus-privacy.eu.org/en/
[9] https://reports.exodus-privacy.eu.org/en/reports/?filter=no_trackers

- Prominentes Beispiel ist die *MS Outlook App für iOS und Adroid*. Das EU Parliaments IT department (DG ITECS) hat deshalb die Nutzung der MS Outlook App verboten[10]. In dem Privacy Statement findet man den Hinweis, dass die Login Credentials für E-Mail Accounts (Username, Passwort) von Microsoft gesammelt werden und dass sich Microsoft die E-Mails von den Providern holt und verarbeitet:

  > *Email Credentials: We collect and process your email address and credentials to provide you the service.*
  >
  > *Email Data: We collect an process your email messages and associated content to provide you the service. [...]*

- M. Kuketz nennt in seinem Blog mit den E-Mail Apps *BlueMail, TypeMail Mail.Ru, myMail* u.a.m. weitere Beispiele. Mit der Einrichtung des E-Mail Accounts in der BlueMail App gibt man der Firma das Recht, in dem Mail Account zu schnüffeln:

  > *When you link your email accounts (provided by third parties) to Blue Mail, you give Blue Mail permission to securely access your information contained in or associated with those accounts.*

  Außerdem beschnüffelt der BlueMail Server die E-Mails und wertet z. B. die Geolocation Tags in versendeten Fotos aus. Wer das nicht möchte, soll eine Kamera verwenden, die keine Geolocation Informationen in den Fotos speichert. Auch diese Schnüffelei wird juristisch korrekt im Privacy Statement benannt.

Vertrauenswürdige Alternativen für E-Mail Apps sind **K9Mail**[11] oder **FairEmail**[12]. Nach dem Wechsel auf eine vertrauenswürdige App sind die Passwörter für die betroffenen E-Mail Accounts zu wechseln!

18.2 Überwachung

Auch Strafverfolgungsbehörden und Geheimdienste nutzen die neuen Möglichkeiten zur *Durchleuchtung der Gesellschaft*:

- Die NSA sammelt täglich rund 5 Milliarden Standortdaten von Mobiltelefonen weltweit im Rahmen des Programms STORMBREW. Nahezu jeder Handynutzer ist betroffen. Das Analyse-Programm *Co-Traveler* sucht anhand der Standortdaten nach Verbindungen zu Zielpersonen. Wer sich zufällig mehrmals am gleichen Ort wie eine Zielperson aufgehalten hat oder zufällig im gleichen Zug saß, kann auch als Unschuldiger ins Netzwerk der Spionage geraten. Außerdem wird nach Verhaltensmustern gesucht, die auf ein erhöhtes Sicherheitsbewusstsein hindeuten.

- NSA/GCHQ sammeln täglich fast 200 Millionen SMS mit dem Programm DISHFIRE. Anhand der Datensammlung werden Kontaktbeziehungen (Identifizierung neuer Zielpersonen), Reisedaten, Finanztransfers (Konto- und Kreditkartennummern) u.a.m. analysiert.

- Das FBI nutzt das Tracking von Smartphones seit mehreren Jahren, wie Danger Room berichtete. Muslimische Communities werden systematisch analysiert, ohne dass die Personen im Verdacht stehen, eine Straftat begangen zu haben. [13].

- Im Iran werden mit Hilfe der Funkzellenauswertung die Teilnehmer von Demonstrationen in Echtzeit ermittelt. Die Technik dafür wird von westlichen Unternehmen

[10] https://www.scmagazineuk.com/eu-parliament-blocks-microsoft-outlook-apps-over-privacy-fears/article/537584/
[11] https://k9mail.app
[12] https://email.faircode.eu
[13] https://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims/

entwickelt, beispielsweise von Siemens/Nokia und Ericsson. Nachdem die Unterstützung von Siemens/Nokia für die Überwachung bekannt wurde und ein Boykottaufruf zu mehr als 50% Umsatzeinbruch im Iran führte, wurde die Überwachungstechnik bei Siemens/Nokia in eine Tochtergesellschaft ausgelagert: Trovicor. Zu den Kunden von Trovicor zählen auch Bahrain, Katar u.ä. Diktaturen.

- In der Ukraine wurden die Geofenching Daten von Handys bereits im Jan. 2014 zur Einschüchterung von Demonstranten genutzt. Teilnehmer einer Demonstration gegen den damals amtierenden Präsidenten bekamen eine SMS mit dem Inhalt:[14]

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

Auch in Deutschland wird die Lokalisierung von Smartphones mittels Funkzellenauswertung zur Gewinnung von Informationen über politische Aktivisten genutzt:

- Die flächendeckende Auswertung von Handydaten im Rahmen der Demonstration GEGEN den (ehemals) größten Nazi-Aufmarsch in Europa in Dresden im Februar 2011 hat erstes Aufsehen erregt. Obwohl die Aktion von Gerichten als illegal erklärt wurde, werden die gesammelten Daten nicht gelöscht und weiterhin für die Generierung von Verdachtsmomenten genutzt.[15]

- Seit 2005 wird diese Methode der Überwachung auch gegen politische Aktivisten eingesetzt. So wurden beispielsweise die Aktivisten der Anti-G8 Proteste per groß angelegter Funkzellenauswertung durchleuchtet.[16] Die Überwachung Handys der Aktivisten begann bereits zwei Jahre vor dem G8-Gipfel in Heiligendamm.

- Die breite Funkzellenauswertung in Berlin zur Aufklärung von Sachbeschädigungen wird als gängige Ermittlungsmethode beschrieben. Auf Anfrage musste die Polizei zugeben, dass diese Methode bisher NULL Erfolge gebracht hat.

- Die Nutzung der Stillen SMS zur Lokalisierung von Personen boomt gerade beim Verfassungschutz:

  - 1. Halbjahr 2013: 28.500 Stille SMS versendet
  - 1. Halbjahr 2014: 53.000 Stille SMS versendet
  - 2. Halbjahr 2014: 142.000 Stille SMS versendet

  Gleichzeitig stagniert die Nutzung der Stillen SMS bei Strafverfolgern (Polizei, BKA usw.) oder geht zurück. Man kann jetzt darüber spekulieren, was die Gründe für diese Aktivitäten des Verfassungsschutz sind.

- Die Bundeswehr entwickelt zusammen mit Airbus Group das Spionagesystem ISIS. Es soll an Bord einer Drohne die Überwachung von Mobilkommunikation aus der Luft ermöglichen. Wenn die Drohne über dem Gebiet Kassel, Gotha, Fulda oder Suhl kreist, könnte man mit ISIS das gesamte Gebiet der BRD überwachen.

[14] https://www.heise.de/-2095284
[15] https://www.heise.de/tp/artikel/34/34973/1.html
[16] https://www.heise.de/tp/artikel/35/35043/1.html

Die Nutzung des Systems gegen Protestler wird ausdrücklich beworben:

> *Bei Protestcamps, Besetzungen u. ä. werden üblicherweise in größeren Umfang lizenzfreie Handfunkgeräte, Wi-Fi-Knoten, Schnurlostelefone und in geringerem Umfang auch Satellitentelefone eingesetzt. Üblicherweise werden diese Funksysteme von Gruppen oder Menschen mit hohem Organisationsgrad verwendet, die sich nicht auf das Funktionieren der überlasteten oder örtlich nicht verfügbaren Mobilfunknetze verlassen wollen. Der Inhalt dieser Funkverbindungen ist demzufolge aus Sicht eines Abhörers oft hochwertig, weil er Zugang zu strategischen Informationen verspricht. Für die Lokalisierung, Identifizierung und Aufzeichnung aller dieser Funksysteme ist ISIS hervorragend geeignet.*

Die Aufgaben von ISIS kann man kurz zusammenfassen: Information, Spionage, Überwachung, Identifizierung. Das System soll aus den verarbeiteten Daten die Sprecher identifizieren können und mehrere tausend Mobilfunkgeräte gleichzeitig lokalisieren und verfolgen.

18.3 Aktivierung als Abhörwanze

Dass Strafverfolger und Geheimdienste ein Handy/Smartphone remote als Abhörwanze aktivieren können, ist seit 2006 bekannt. Das FBI nutzte damals die Handys der Mafiabosse Ardito und Peluso remote zur akustischen Raumüberwachung, um Beweise zu sammeln[17]. Bereits 2007 hat das BSI deshalb empfohlen, bei Gesprächen mit sensiblen Inhalten keine Handys mitzuführen.

> *Aus Sicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die effektivste Schutzmaßnahme ein Vermeiden des Mitführens von Handys bei Gesprächen mit sensitivem Inhalt, die Detektion jedweder Mobilfunkaktivität im Raum durch den vom BSI entwickelten Mobilfunkdetektor MDS sowie das Deaktivieren sämtlicher drahtloser Schnittstellen von Mobilfunkgeräten.*

Der Missbrauch eines Smartphones als Abhörwanze ist nicht auf potente Geheimdienste beschränkt. Angreifer können auch Apps mit verdeckten Funktionen verwenden. Dafür gab es in der Vergangenheit bereits mehrere Beispiele:

- Die offizielle App der spanischen Fußballliga *La Liga* aktivierte während der Ausstrahlung der Fußballspiele im TV das Mikrophone der Smartphones zur Raumüberüberwachung, um in Kombination mit den GPS Standortdaten nach der unlizensierten öffentliche Übertragung von Ligaspielen zu fahnden. Die App hat ca. 10 Mio. Nutzer in Spanien.[18]

- Die Hamas hat anläßlich der WM ebenfalls eine App für Fußball Fans in der israelischen Armee entwickelt und außerdem mehrere Dating Apps für israelische Soldaten (Heart Breaker), die der Spionage dienten inklusive akustischer Raumüberwachung und Zugriff auf die Kamera.[19]

  Ein Sicherheitsoffizier der IDF kommentierte:

  > *Whatever you can do with your phone, a malicious app can do too.*

- ...und dann gibt es noch Alexa, Siri & Co. wo auch mitgehört werden kann. Nach Protesten von Nutzern haben Google, Amazon und Apple laut offiziellen Statements im Sommer 2019 die langjährige Praxis beendet, das Mitarbeiter die von Alexa, Siri & Co. übertragenen Daten zur Spracherkennung abhören, um die Qualität der Spracherkennung zu verbessern. Aber technisch besteht diese Möglichkeit weiterhin. Bisher versprechen die Konzerne nur, dass keine menschlichen Mitarbeiter mehr im Rahmen der Qualitätskontrolle zuhören werden.

[17] http://news.cnet.com/2100-1029-6140191.html
[18] https://heise.de/-4075636
[19] https://www.rt.com/news/431663-hamas-dating-app-idf-israel

Die Beispiele zeigen, dass man sich selbst nur schwer gegen eine mögliche Überwachung mit Smartphone Wanzen schützen kann. Selbst wenn man sein eigenes Smartphone zuhause lässt, dann hat möglicherweise ein Freund oder Kamerad sein Smartphone dabei und die Wanze belauscht nicht nur ihn sondern auch mich.

18.4 WLAN ausschalten, wenn nicht genutzt

Alle Smartphones (und Laptops!) haben ein WLAN Modul. Es ist bequem, wenn man nach Hause kommt oder wenn das Smartphone am Arbeitsplatz automatisch das WLAN nutzt statt der teuren Datenverbindungen des Mobilfunk Providers.

Wenn man mit aktiviertem WLAN Modul und automatischem Login für die bevorzugte WLANs unterwegs ist, dann sendet das Smartphone oder der Laptop regelmäßig aktive Probes, um die Umgebung nach den bevorzugten WLANs zu scannen. Dabei wird neben der weltweit eindeutigen MAC Adresse auch eine Liste der SSIDs der bevorzugten WLANs gesendet, mit denen sich das Smartphone automatisch verbinden würde (Prefered Network List, PNL). Diese Liste liefert Informationen über Orte, an denen sicher der Besitzer des Smartphones bevorzugt aufhält. (Home, Office...)

Mit geringem technischen Aufwand kann man diese Daten der aktiven WLAN Probes zum Tracking und für Angriffe nutzen:

1. Auf der re:publica 2013 wurde ein kostenfreies WLAN bereitgestellt. Dieses WLAN verfolgte alle WLAN-fähigen Geräte (Laptops und Smartphones) der Besucher, unabhängig davon, ob die Geräte das WLAN nutzten oder nicht. Das Projekt *re:log - Besucherstromanalyse per re:publica W-LAN* visualisiert die Daten.[20]

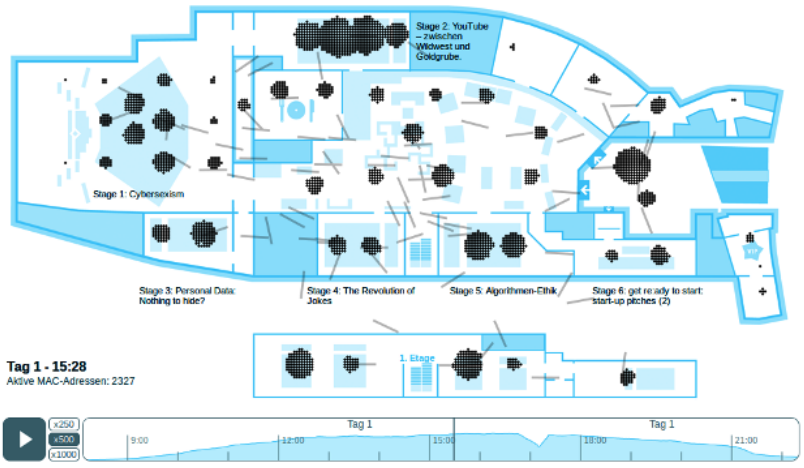


Abbildung 18.3: WLAN Tracking auf der re:publica 2013

2. Forscher der Università di Roma sind mit der Studie *Signals from the Crowd: Uncovering Social Relationships through Smartphone Probes*[21] einen Schritt weiter gegangen. Sie haben gezeigt, dass man die aktiven WLAN Probes für eine soziale Analyse der Crowd nutzen kann. Crowd steht dabei für eine Ansammlung von Personen (Teilnehmer von Veranstaltungen oder Demonstrationen, Bordell Besucher .... usw.).

3. Die Security Firma Sensepost ging noch einen Schritt weiter. Auf der Blackhat Asia 2014 wurde die *Drohne Snoopy*[22] vorgestellt. Diese Drohne wertet die Probes der

[20] http://apps.opendatacity.de/relog/
[21] http://conferences.sigcomm.org/imc/2013/papers/imc148-barberaSP106.pdf
[22] http://www.sensepost.com/blog/7557.html

WLAN Module aus und simuliert dann die SSID eines bevorzugten WLANs des Smartphones. Das Smartphone meldet sich automatisch bei der Drohne an. Der Internet Traffic läuft über die Drohne und kann dort analysiert und modifiziert werden. Es wurde auf der Konferenz demonstriert, wie *Snoopy* Login Credentials von PayPal, Yahoo usw. abgreifen konnte, Name und Wohnort der Nutzer ermitteln konnte und die Smartphones über einen längeren Zeitraum tracken konnte. Auf Github.com steht der Source Code für Snoopy, Server und Webinterface für eigene Experimente zum Download bereit.

4. Android Smartphones kann ein Angreifer durch einen Fehler in der Funktion Wi-Fi Direct kompromittieren. Dabei stellt ein Angreifer einen virtuellen Accesspoint mit einer bösartigen SSID auf. Damit kann er verwundbare System in Funkreichweite lahm zu legen, Speicherinhalte auszulesen und potenziell sogar Schadcode zur Ausführung zu bringen. Das Problem betrifft auch Linux auf dem PC oder Laptop. Solange der Fehler nicht behoben wurde, können Linuxer in der Datei */etc/wpa_supplicant/wpa_supplicant.conf* folgende Option als Schutz gegen diesen Angriff aktivieren:

   ```
   p2p_disabled=1
   ```

Es gibt bereits erste praktische Ansätze der Werbeindustrie, um die WLAN Probes der Smartphones zum Schnüffeln zu nutzen:

- Die Werbefirma Renew stellte zu den Olympischen Spielen 2012 in London 200 Abfallbehälter auf, die mit einem integrierten WLAN Access Point die Fußgänger anhand der MAC Adressen der Smartphones verfolgten. Innerhalb einer Woche wurde über 4 Mio. Geräte auf dem Weg durch die Londoner City verfolgt.[23]

  We will cookie the street. (K. Memari, chief executive of Renew)

- **Ins Netz gegangen** (Pressemitteilung der BVG, PDF)[24]: Die Berliner Verkehrsbetriebe werden in Zusammenarbeit mit HOTSPLOTS auf den U-Bahnhöfen kostenfreien Wi-Fi zur Verfügung stellen. Bis Ende 2016 sollen 76 U-Bahnhöfe mit den Access Points ausgestattet werden. Die Bahnhöfe wurden so gewählt, das rechnerisch 2/3 der täglich 1,5 Mio U-Bahn-Kunden erfasst werden können. Außerdem wird mit kostenfreiem WLAN auf den Buslinien 200 und 204 experimentiert.

  Die Nutzung ist ganz einfach. Wenn man beim Warten auf die U-Bahn noch schnell mal…wählt man das *BVG Wi-Fi* und ruft eine Webseite auf. Nachdem man die Nutzungsbedingungen bestätigt und die erste Werbeseite gesehen hat, kann man kostenfrei Surfen usw. Es wird kein Name und E-Mail Adresse abgefragt.

  Zukünftig meldet sich das Smartphone bei jedem Ein. und Aussteigen und bei jeder Durchfahrt durch den Bahnhof automatisch bei dem BVG Access Point an. In den Nutzungsbedingungen ganz unten (runterscrollen) findet man die Daten, die bei jedem (automatischen) Connect gespeichert werden:

  – die eindeutige MAC-Adresse des Gerätes
  – die zugewiesene IP-Adresse
  – Zeitstempel des Login und Logout

  Die Daten werden gem. TKG und gemäß Vorratsdatenspeicherung (neudeutsch: Mindestspeicherfristen) gespeichert. Außerdem werden sie von HOTSPLOTS ausgewertet und der BVG für statistische Auswertungen zur Verfügung gestellt. Diese Daten ermöglichen eine Verfolgung von Bewegungen in der realen Welt, wie es anhand der Besucherstöme auf der republica 2013 demonstriert wurde.

[23] https://www.rt.com/news/trash-bin-surveillance-wifi-402/
[24] http://unternehmen.bvg.de/de/index.php?section=downloads&cmd=180&download=2070

- Auf dem Flughafen Amstersam-Schiphol findet man fogendes Schild, das auf Wifi- und Bluetooth-Tracking hinweist (Abb: 18.4). Auf der Webseite des Flughafens findet man die Erklärung, dass das Wifi-Tracking genutzt wird, um die Anzahl und Bewegung der Reisenden in den unterschiedlichen Bereichen des Flughafens zu beobachten und damit die Anzeigen für die geschätzten Wartezeiten zu aktualisieren.

Abbildung 18.4: Wifi-Tracking am Flughafen Amsterdam-Schiphol

- Die Technik zur Verfolgung der Besucher- bzw. Kundenströme mittels Wifi-Tracking wird auch von mehrere Handelsketten wie z. B. Karstadt Sports und Escada eingesetzt, um Bewegungen der Kunden im Einkaufsbereich zu verfolgen.[25]

  Neben WLAN Tracking wird auch Bluetooth in Einkaufsfilialen eingesetzt, weil Bluetooth Beacons eine genauere Standortbestimmung der Kunden in der Filiale ermöglichen. Leider gibt es in Deutschland kein Gesetz, das ähnlich wie bei der Videoüberwachung einen deutlichen Hinweis auf das Wifi-Tracking fordert.

  U. Spaan vom Handelsforschungsinstitut EHI schätzt, das 20% der Einzelhändler in Deutschland derzeit (Feb. 2018) mit Trackingmethoden in Läden experimentieren.

- Die Firma AdNear experimentiert mit Drohen, welche die Wi-Fi und Baseband Signale der Smartphones auswerten. Anhand der MAC Adresse der WLAN Module werden die Bewegungen der Nutzer verfolgt.[26]

  > *Today we started initial tests with drones to collect data. And the results have been fantastic! Besides, this turns out to be the most efficient mode.*

Schlussfolgerung: WLAN abschalten, wenn man es nicht braucht.

18.5 Tracking blockieren

Auf dem Desktop PC installiert man einen AdBlocker im Browser. Auf einem Smartphone ist das Blockieren von Tracking kompliziert, da fast jede App Trackingdienste einbindet. Einige Apps verwenden bis zu 40 Trackingdienste, die die Nutzung beobachten.[27]

Die Verbindungen zu Tracking- und Werbeservern könnte man auf DNS Ebene blockieren. Aus technischer Sicht handelt es sich dabei um die klassische Zensur. Der Nutzer zensiert den Zugriff auf Trackingserver, indem er die DNS Namensauflösung blockiert.

Seit Herbst 2020 funktioniert diese Form der Filterung immer schlechter und wird löchrig. Die Trackingdienste nutzen Anti-Zensur Techniken, um die Filterung zu umgehen:

- Apple unterstützt die Trackingdienste dabei mit der Implementierung von DNS-over-TLS oder DNS-over-HTTPS in iOS Version 14+. Apps haben die Möglichkeit,

[25] https://www.heise.de/-3973727
[26] https://adnear.com/february2015/experimenting-with-drones-for-data-collection.php
[27] https://reports.exodus-privacy.eu.org

mit wenig Code einen eigenen, unzensierten DNS Server via DoT oder DoH zu verwenden statt des Servers, der in den Systemeinstellungen konfiguriert wurde, und damit die Zensur durch den Nutzer zu umgehen. Ein Video erklärt die Schritte.[28]

- Android Nutzer beschweren sich seit Sept./Okt. 2020 in diversen Foren immer häufiger, dass ihnen in Spielen usw. nach kurzer Verzögerung beim Start Werbung angezeigt wird, obwohl Tracking- und Werbeserver auf DNS-Ebene blockiert wurden.

  Auch hier kommt ein eigener DNS Server in der App zum Einsatz, der via DNS-over-TLS oder DNS-over-HTTPS die Blockade umgeht und das VPN durchtunnelt.

Wenn Anti-Zensur Techniken entwickelt werden, dann müssen wir uns nicht wundern, wenn auch die Trackingbranche diese Techniken verwendet, um Blockaden zu umgehen.

Für weniger hochentwickelte Apps funktioniert die Zensur auf DNS Ebene weiterhin. Für aktuelle Varianten von Andoid und iOS ist die Variante (2) empfehlenswert.

(1) Man könnte die Apps **Blokada** (Andoid, iPhone) oder **DNSCloak** (iPhone) installieren und als Trackingblocker nutzen. Beide Apps registrieren sich als VPN Dienst, so dass andere Apps den Traffic über zu diesen Filter-Apps schicken. Die Apps übernehmen die Auflösung der DNS Namen und blockieren Verbindungen zu vielen Tracking- und Werbeservern. Blokada verwendet lokale Blacklisten für das blockieren der DNS Namen. DNSCloak überlässt die Filterung dem DNS-Server, den man auswählt.

Nachteilig bei diesen Lösungen ist, dass man kein anderes VPN mehr nutzen kann.

(2) Aktuelle Android und iOS Versionen unterstützen die Konfiguration eines DNS-over-TLS oder DNS-over-HTTPS Servers in den Systemeinstellungen. Wenn man einen DNS Server mit Blocklisten für Tracking und Werbung auswählt, werden Tracking- und Werbungserver auf DNS Ebene zensiert und man kann gleichzeitig ein VPN nutzen.

Android unterstützt seit Version 9 (Pie) DNS-over-TLS. Die Option heißt *Privates DNS* und verbirgt sich in den erweiterten Einstellungen für *Netzwerk & Internet*.

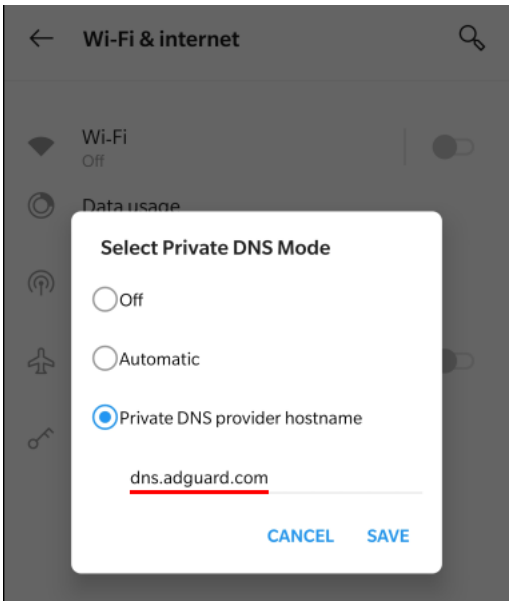


Abbildung 18.5: DNS-over-TLS Server in Android konfigurieren (Privates DNS)

[28] https://developer.apple.com/videos/play/wwdc2020/10047/

Es ist der Hostname eine DNS-over-TLS Servers einzutragen, der Trackingdienste und Werbung blockiert. Die initiale Ermittlung der IP-Adresse des DoT-Servers erfolgt mit dem DNS Server, der via DHCP zugeteilt wurde. Nach dem Captive Portal Check wird auf DNS-over-TLS umgeschaltet.

iPhones unterstützen verschlüsseltes DNS seit iOS Version 14. Die Konfiguration ist ein bisschen umständlicher als bei Android aber machbar:

1. Man muss sich ein Konfigurationsprofil für den DNS Server herunterladen. Es gibt mehrere Webseiten, die Profile für einige DNS Server bereitstellen. Es ist aber empfehlenswert, ein signiertes Profil direkt vom Anbieter herunter zu laden, z. B. vom bekannten russischen DNS Anbieter AdGuard.[29]
2. Dann ist das Konfigurationsprofil zu installieren: (*Einstellungen -> Profil geladen*) und die Warnung zu bestätigen, dass DNS Einstellungen modifiziert werden.
3. Standardmäßig ist das zuletzt installierte Profil automatisch aktiv. Wenn man mehrere Profile für DNS Server installiert hat, kann man in den Einstellungen unter *Allgemein -> VPN & Netzwerk -> DNS* das aktive Profil auswählen.

18.6 Krypto-Apps

Eine Warnung: Jede kryptografische Anwendung braucht einen vertrauenswürdigen Anker. Üblicherweise geht man davon aus, dass der eigene PC oder Laptop ein derartiger vertrauenswürdiger Anker ist, über den man volle Kontrolle hat. Bei Smartphones kann man nicht davon ausgehen, dass der Nutzer volle Kontrolle über die Software hat.

1. Mit dem Kill Switch[30] hat Google die Möglichkeit, auf Android Handys beliebige Apps zu deinstallieren, zu installieren oder auszutauschen. Das iPhone[31] und Windows Phone[32] haben ebenfalls einen Kill Switch. Jede Crypto-Anwendung aus den Markets muss also als potentiell kompromittiert gelten. Sie kann genau dann versagen, wenn man den Schutz am nötigsten braucht.

2. Jede Crypto-Anwendung benötigt gute Zufallszahlen. Der Zufallszahlengenerator der Android Java VM war so besch.... schlecht, dass man als Angreifer nicht die Kompetenz und Rechenleistung der Crypto-City von Fort Meade braucht. Ganz gewöhnliche Hacker konnten die Schwächen der Android Implementierung im Sommer 2013 nutzen, um Geldbörsen von Bitcoin Nutzern leer zu räumen[33].

3. Smartphones sind leicht kompromittierbar:

   - Remote Code Execution ist normalerweise ein schwerer Sicherheitsfehler. Bei Android Smartphones ist es ein Feature. Apps können Code aus dem Internet nachladen, der weder von Sicherheitsscanner auf dem Smartphone noch von den Sicherheitsprüfungen in App Stores kontrolliert werden kann. Viele kostenlose Apps für Spiele nutzen diese Möglichkeit für Werbezwecke. Da die Verschlüsselung der Internetverbindungen zu den Servern nicht immer dem aktuellen Stand entspricht oder garnicht vorhanden ist, kann ein Angreifer gezielt bestimmte Smartphones mit Trojanern verseuchen, indem er den Download on-the-fly modifiziert.
   - Der Sicherheitsexperte C. Mulliner hat das *Dynamic Dalvik Instrumentation Framework for Android* entwickelt, mit dem man jegliche Kryptografie komplett aushebeln kann. In seinem Blogartikel weist C. Mulliner darauf hin, dass er zum Deployment des Frameworks nichts schreiben muss, weil für dieses Problem genügend Lösungen publiziert wurden.

[29] https://adguard.com/en/blog/encrypted-dns-ios-14.html
[30] https://mashable.com/2011/03/06/android-kill-switch
[31] https://www.telegraph.co.uk/technology/3358134/Apples-Jobs-confirms-iPhone-kill-switch.html
[32] https://www.heise.de/-1131297
[33] https://www.heise.de/-1933714

- Auch das *Xposed Framework* kann mit einem ähnlichen Trick Kryptografie komplett aushebeln oder die Privacy-Einstellungen verschärfen (je nach Intention).

OpenPGP-Verschlüsselung

Man kann OpenPGP auch auf dem Smartphone nutzen, aber:

> *Never store your private PGP key on your mobile phone... Mobile phones are inherently insecure.* (Mike Cardwell)

Der Yubikey NEO hat eine OpenPGP Smartcard, die via NFC genutzt werden kann. Der private Schlüssel wird dabei auf dem Yubikey gespeichert und verlässt diese Umgebung nie. Die PIN zur Freigabe des Schlüssel wird zusammen mit den zu entschlüsselnden oder zu signierenden Daten via NFC an den Yubikey gesendet und das Ergebnis der Kryptooperation wird zurück an das Smartphone gegeben.

1. Auf dem Andoid Smartphone benötigt man folgende Software, die man aus dem Google Play Store oder F-Droid Store installieren kann:
   - **OpenKeychain** kümmert sich um Ver-/Entschlüsselung und die Verwaltung der Schlüssel. Seit Version 3.2 vom 06. Mai 2015 wird der Yubikey NEO via NFC als OpenPGP Smartcard unterstützt.
   - Das E-Mail Programm **K9mail** kann direkt mit OpenKeychain zusammenarbeiten und integriert Buttons zum Verschlüsseln bzw. Entschlüsseln von E-Mails.
   - Der Jabber/XMPP Client **Conversations** kann in Kombination mit OpenKeychain die Chats mit OpenPGP verschlüsseln, der private Key liegt dabei aber auf dem Smartphone. OTR- und OMEMO-Verschlüsselung sind auch möglich.
2. Den Yubikey NEO bereitet man am einfachsten mit Enigmail auf einem PC vor (siehe: OpenPGP Smartcards). Die OpenPGP Smartcard Funktion ist freizuschalten, die PIN und Admin-PIN ist zu ändern und die Schlüssel sind zu generieren.
3. Das neu erstellte Schlüsselpaar kann man aus Enigmail in eine Datei exportieren (geheimen + öffentlichen Schlüssel!). Der geheime Schlüssel in dieser Datei enthält praktisch nur einen Verweis, welche Smartcard genutzt werden muss.
4. Diese Schlüsseldatei ist auf das Smartphone zu übertragen und in OpenKeychain zu importieren.
5. Außerdem muss man noch die öffentlichen Schlüssel der Kommunikationspartner in OpenKeychain auf dem Smartphone importieren. Diese Schlüssel kann man ebenfalls aus Enigmail exportieren, wenn sie dort vorhanden sind. Alle benötigten Schlüssel können markiert werden (STRG-Taste drücken, wenn der Schlüssel mit der Maus markiert wird) und in eine Datei zusammen gespeichert werden. Diese Datei wird ebenfalls auf das Smartphone übertragen und in OpenKeychain importiert.

18.7 Stille SMS ind IMSI-Catcher erkennen

Die App **SnoopSnitch** von SRLabs steht seit Januar 2015 für Android im F-droid Store und im PlayStore bereit. Die App erkennt ISMI-Catcher und erkennt außerdem, ob jemand die Gespräche belauscht und mit einem SS7-Exploit die Verschlüsselung gehackt hat. Für die Installation ist ein Rooten des Smartphone nötig. Die App funktioniert nur, wenn das Smartphone einen Qualcomm Chipsatz hat.

Das **GSMK CryptoPhone** hat einen ganz gut funktionierenden IMSI-Catcher-Detector onBoard. Mit diesem Detector wurden in Washington DC in der Umgebung des White House und US Capitol sowie in der Nähe von Botschaften 18 IMSI-Catcher aufgespürt [34].

[34] https://rt.com/usa/189116-washington-dc-spying-phone

> *I would bet money that there are governments that are spying in DC.* (C. Soghoian)

Washington DC ist kein Einzelfall. Auch in Oslo wurden IMSI-Catcher im Regierungsviertel gefunden. Leider mussten die Journalister einer Zeitung mit einem GSMK CryptoPhone die norwegische Spionageabwehr erst darauf aufmerksam machen.[35]

> *Die gefundenen Geräte seien nicht auf dem freien Markt erhältlich, sie seien sehr ausgereift und teuer. Nur Organisationen mit großen Ressourcen, etwa ausländische Geheimdienste, seien zu einer solchen Überwachung in der Lage.*

In Sicherheitskreisen vermutet man, das die IMSI-Catcher in den Regierungsvierteln in erster Linie der Beobachtung dienen, wer in den verschiedenen Einrichtungen ein- und ausgeht. Das Abhören von SMS und Telefonaten ist vermutlich eher nebensächlich. Das Smartphone ist eine Trackingwanze, die wir freiwillig mit uns umhertragen!

18.8 Juice Jacking Angriffe

Juice Jacking nennt man Angriffe, die von USB Ladestationen ausgehen. Kriminelle können öffentliche Ladestationen mit USB-Anschluss oder vergessene Ladekabel nutzen, um Malware auf einem Smartphone zu installieren oder Daten sowie Passwörter zu stehlen.

In Deutschland sind diese Angriffe kaum bekannt, weil es nur wenige öffentliche Ladestationen gibt. International ist man schon weiter, sowohl bei der Bereitstellung öffentlicher Ladestationen an Flughäfen, in Hotels und öffentlichen Plätzen, als auch…

Die Behörden von Los Angeles (USA) haben im Nov. 2019 eine dringende Warnung vor öffentlichen Ladestationen für Smartphones mit USB-Anschluss veröffentlicht.[36]

> *Travellers should avoid using public USB power charging stations in airports, hotels and other locations because the may contain dangerous malware.*

Moderne Smartphone haben einen Softwareschutz gegen diese Angriffe (in Android deaktivierbar). Das Smartphone sollte den Nutzer erst fragen, ob der Gegenüber vertrauenswürdig ist, wenn eine Datenverbindung initiert wird. Allerdings scheinen die Behörden von LA wenig Vertrauen in diesen Schutz zu haben.

Man kann natürlich seinen AC-Charger nutzen oder (wenn der Stecker mal nicht passt) eine Powerbank, die man via USB auflädt um damit dann das Smartphone zu laden.

Außerdem gibt es das *USB Condom* oder *USB Data Blocker*. Das sind kleine Adapter für USB-Stecker, in denen nur die Kontakte für die Energieversorgung verbunden sind aber nicht die Kontakte für Datenleitungen. Im deutschen Fachhandel gibt es diese Dinger noch nicht, aber man kann sie bei Amazon o.ä. Händlern mit internationaler Lieferung bestellen.

18.9 Das Hidden OS im Smartphone

In jedem Smartphone steckt neben dem End-User-Betriebssystem (Android, iOS, Windows Phone) und dem Linux Kernel ein weiteres, verstecktes Betriebssystem. Dieses Hidden OS läuft auf dem Baseband Prozessor und bearbeitet die Kommunikation mit den Mobilfunkstationen in Echtzeit. Es handelt sich dabei um ein Real-Time Betriebssystem. Der Markt wird von Qualcomm mit AMSS dominiert, die Software ist Closed Source.

Im Betrieb hat das Hidden OS die volle Kontrolle über die gesamte Hardware incl. Mikrofon und Kamera. Linux Kernel und End-User Betriebssysteme laufen als Slaves

[35] https://www.zeit.de/digital/datenschutz/2014-12/norwegen-spionage-oslo
[36] http://da.lacounty.gov/community/fraud-alerts/juice-jacking-criminals-use-public-usb-chargers-steal-data

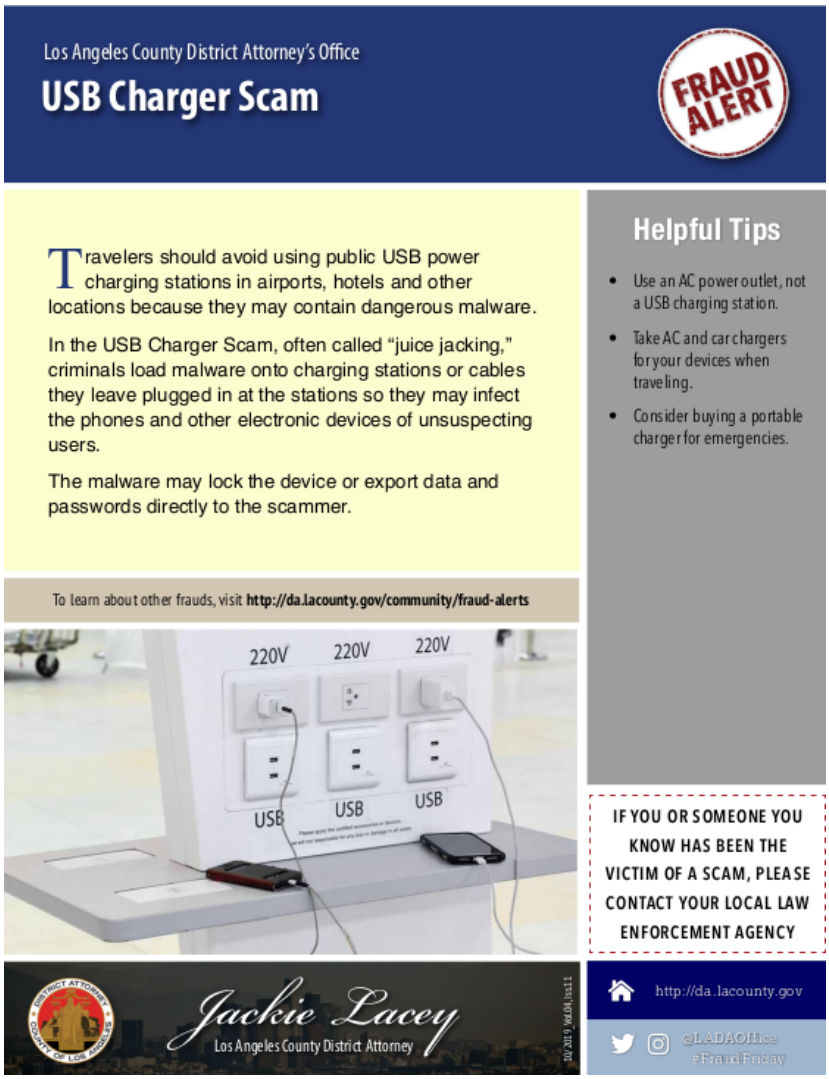


Abbildung 18.6: Warnung vor USB Charger Scam

unter Kontrolle des Hidden OS.

Die implementierten Sicherheitsstandards des Hidden OS stammen aus dem vergangenen Jahrhundert. Die Daten der Mobilfunkstationen werden z. B. ungeprüft als gültig übernommen. Security Analysen sind schwierig, da jede Analyse zuerst ein Reverse Engeniering der Closed Source Software erfordert. Trotzdem stellen Sicherheitsexperten seit Jahren immer wieder gravierende Mängel vor:

- Weinmann stellte auf der DeepSec 2010 mit *All Your Baseband Are Belong To Us* einen Angriff vor, der mit einem nur 73 Byte großem Remote Code Execution Exploit eine Backdoor öffnete und das Smartphone in eine Abhörwanze verwandelte..[37]

- Mit den *Hexagon challenges* wurde auf der PacSec 2013 ein verbesserter Angriff auf das Hidden OS von Rals Phillip Weinmann vorgestellt.[38]

- Forscher der TU Berlin demonstrierten auf dem *22nd USENIX Security Symposium* eine Angriff auf das Hidden OS, der nur geringe Ressourcen erforderte. Mit einigen

[37] http://www.securitytube.net/video/5372
[38] http://pacsec.jp/speakers.html

manipulierten Smartphones wurden andere Smartphones in der Umgebung kompromittiert und der Empfang von Anrufen und SMS blockiert.[39]

- Das GSMK-Team demonstrierte 2013 einen Over-the-Air Angriff auf Smartphones, bei dem zuerst das Hidden OS des Baseband Prozessors durch ein *Over-the-Air Update* kompromittiert und dann das Smartphone OS (iOS und Android) angegriffen wurde. Es wurden alle verfügbaren erfolgreich Smartphones kompromittiert.[40]

  > *Compromised phones can then be used to record conversations or gain access to sensitive data. It would also be possible to monitor content being accessed through pwned smartphones.*

  Der Angriff ist relativ aufwendig und wird daher wahrscheinlich sehr selten eingesetzt, da es einfachere Möglichkeiten durch Verteilung kompromttierter Apps via Play Store oder ähnliches gibt.

[39] http://phys.org/news/2013-08-firmware-tweak-block-subscriber-berlin.html
[40] https://www.theregister.co.uk/2013/03/07/baseband_processor_mobile_hack_threat/Malware-flingers%20can%20pwn%20your%20mobile%20with%20over-the-air%20updates