Irgendwann nach dem 28.08.2014 habe ich in einem Forum das Tutorial „Probleme unsichtbar zu sein & wie werde ich es doch“ gefunden und es für so informativ gehalten, dass ich mir ein PDF daraus gemacht habe. Nachdem die staatlichen Überwachungsmassnahmen immer schlimmer werden stell ich an dieser Stelle nicht nur den Inhalt des PDF hier rein, sondern ergänze das Ganze am Ende mit weiteren (der heutigen Situation angepassten) hilfreichen Informationen.

> *Amateure üben, bis sie es richtigmachen. Profis üben, bis sie es nicht mehr falsch machen können. Du kannst es nur einmal vermasseln.*

Der folgende Text soll die Probleme behandeln, die auftauchen, wenn man seine Identität vor den Behörden verbergen muss. Es soll eine Aufzählung sein, die für die Ausarbeitung deines Sicherheitskonzeptes zur Rate gezogen werden kann.

Ob der Ansatz zu übertrieben ist, soll hier nicht das Thema sein. Vielmehr soll ein Denkprozess angeregt werden, in dem Du, der Leser, dazu gebracht wirst, Dein Verhalten und die daraus resultierenden Konsequenzen besser einschätzen zu können.

Die Überlegungen und Empfehlungen stützen sich auf gesammelten Geschehnissen aus der näheren Vergangenheit, Angaben aus Büchern und anderen Quellen. Es werden, soweit es möglich ist, Links zu den Artikeln oder Berichten angegeben. Auf Behauptungen aus Foren oder anderen unseriösen Quellen, wird bewusst verzichtet.

Ob der Grad der Paranoiker realistisch ist, hängt eher von deinen Aktivitäten ab, als von deinem subjektiven Gefühl ab. Dazu findest du ein Thread von spider "OPSEC Gedankenmodell Sicherheitsstrategie" , der dir helfen kann, deine Situation besser einzuschätzen. Hier jedoch gehen wir vom Worst Case aus. Unser Motto soll ganz nach Joseph Hellers Meinung lauten: "Nur, weil Du paranoid bist, heißt es nicht, dass sie nicht hinter Dir her sind."

1. Die Menschen lügen.
   - 1.1 100% sicher.
   - 1.2. Es ist alles halb so schlimm. Und in der Masse gehe ich doch unter.
     - 1.2.1 Die Vics erleiden kein Schaden. Sie sind dagegen versichert.
     - 1.2.2 Sie sind selber schuld, wenn sie ihre Systeme nicht absichern.
     - 1.2.3 Freedom Fighter oder Terrorist
   - 1.3 Ich bin sicher, da ich zusätzlich VPN benutze.
   - 1.4 Vorratsdatenspeicherung ist gefallen. Mir kann also nichts passieren.
   - 1.5 Mit PGP bin ich sicher.
2. Du, das größte Sicherheitsrisiko
   - 2.1 Verschwiegenheit
   - 2.2 Datenverschwiegenheit
   - 2.3 Identitäten erstellen
3. Welches Betriebssystem
   - 3.1 Microsoft Windows
   - 3.2 Linux
4. (fast) Anonym durch VPN, Tor, JonDo & Co
   - 4.1 Tor
   - 4.2 JonDo
   - 4.3 VPN-Provider
   - 4.4 VPN/Tor Kaskadierung
   - 4.5 Internetverbindung
     - 4.5.1 Offene Café WLAN

4.5.2 Wardriving
4.5.3 Freifunk
4.6 Mobile Verbindung über anonyme SIM Sicherheitsrisiko IPv6
4.6.1 Deaktivierung der IPv6
5. Browser absichern
5.1 Automatische Absicherung
5.2 Manuelle Absicherung
6. Kommunikation
6.1 Sicherer E-Mail-Verkehr
6.1.1 Anonyme E-Mail Accounts aus dem Clearnet
6.1.2 PGP
6.1.3 Meta-Daten anonymisieren
6.1.4 Alternative zur E-Mail Accounts
6.2 Handykontrolle
6.3 Messenger
6.3.1 Bitmessanger.
6.3.2 Torchat
6.3.3 IRC
7. Sichere Hardware
7.1 Notebooks
7.2 Handykontrolle
7.3 Mobiles Internet
8. Sichere Passwörter
8.1 Zettelalgorithmus
8.2 Cloud Passwort-Manager
8.3 Password Manager App

Weiter Themen, die noch bearbeitet werden:

- Datenverschlüsselung und sicheres Löschen.
- Nähere Betrachtung der Tracking-Verfahren. (Flash Cookies, JavaScript und andere Verfahren).
- Sicheres und anonymes Bezahlen

Aber bevor wir anfangen den technischen Teil näher zu betrachten, schauen wir uns den unsichersten Teil an: Dich!

> *Kennst du dich und kennst du deinen Gegner, brauchst du den Ausgang von tausend Schlachten nicht fürchten Sun Tzu 544-496 v.Ch*

1. Die Menschen lügen. Jeden Tag. Sie lügen ihre Freunde, ihre Kollegen und ihre Liebsten an. Aber am meisten belügen sie sich selbst. Und genau das tust Du auch. Genau in diesem Moment. Ob die Lüge darin besteht, dass Du nach dem Studieren dieser Zeilen sicher bist, oder dass es die absolute Sicherheit überhaupt gibt. Vielleicht dass Dich entsprechende Technik schon schützen wird oder dass alles nicht so schlimm ist. Ob diese oder andere Lügen, sie haben alle eins gemeinsam: sie spielen Dir eine falsche Realität vor. Deswegen räumen wir erst mit dem Gerüst der Selbstlügen auf.

1.1 100% sicher.
Die Sicherheit ist ein Prozess, dass immer wieder aufs Neue überprüft und optimiert werden muss. Es findet nie ein Ende. Sie ist nie 100%. Es gibt nur mehr oder weniger sichere Konzepte und Verfahren. Und sie alle haben eine gravierende Schwachstelle: Dich! Dazu wird in Punkt 2. Du, das größte Sicherheitsrisiko näher eingegangen.

1.2. Es ist alles halb so schlimm. Und in der Masse gehe ich doch unter.

Die Annahme, dass die jeweiligen Aktivitäten nicht so schlimm sind und die "Gesetzeshüter" zu viel zu tun haben, als dass sie genau dich packen würden, ist sehr gefährlich. Du musst dir immer im Klaren sein, was du tust und welche Konsequenzen dein Tun, für die Betroffenen und dich, falls du erwischt sein solltest, hat. In den folgenden Unterpunkten werden grob Gruppen gebildet. In welcher Du passt, musst du selber entscheiden.

1.2.1 Die Vics erleiden kein Schaden. Sie sind dagegen versichert.

Nehmen wir an, du willst ein "bisschen" Geld "verdienen". Gehen wir weiter davon aus, dass du den hier im Forum beschriebenen Methoden folgen möchtest. Du solltest dir immer vor Augen führen, dass Du in erster Linie Menschen betrügst. Es sind nicht gesichtslose Firmen, Banken oder Versicherungen, die den größten Schaden davontragen. Nein, es sind die Inhaber der Konten, die du mit der Überweisung belastest. Auch wenn sie ihr Geld wiederbekommen. Vorausgesetzt natürlich sie entdecken die unrechtmäßige Überweisung und melden diese auch innerhalb der drei monatigen Frist. Bis sie es wiederbekommen, haben sie Stress! Sie gehen davon aus, dass ihr Konto sicher ist. Es ist in erster Linie ein Eindringen in ihre Privatsphäre. Durch das Abheben wird ein Loch in ihr Budget gerissen, was unter Umständen dazu führen kann, dass sie ihre Rechnungen nicht begleichen können. Wenn es z.B. die Miete ist, kann es schon mal sehr weite Konsequenzen haben. Mögliche Mahnkosten, die dadurch entstehen, werden nicht erstattet! Das Ansehen oder die Kreditwürdigkeit kann dadurch geschädigt werden.

Die weit verbreitete Meinung, dass die Kosten die Banken oder ihre Versicherungen tragen, ist falsch. Denn nicht die Bank verliert hier Geld. Die Bank gewinnt IMMER! Sie sind gegen solchen Betrug versichert. Aber auch nicht die Versicherung verliert hier Geld, denn welche auch immer bei deinem Betrug das Geld erstattet, sie ist ein Unternehmen, das zu dem Zweck errichtet worden ist, Geld zu verdienen. Also wer zahlt im Endeffekt für den Schaden? Der Kunde! Genauer genommen ALLE Kunden; auch Du! Mit deinen Gebühren.

Ein anderer Aspekt, denn du stets beachten solltest ist, dass der Betrug, den du begehst, nicht mit einem Ladendiebstal zu vergleichen ist!

Ein Betrug nach §263 StGB kann mit bis zu 5 Jahren und bei schweren Fällen mit bis zu 10 Jahren Freiheitsentzug bestraft werden!

Mehr unter StGB §263 und Was ist ein Betrug?

Dass es schnell ins Auge gehen kann, zeigt der kürzlich bekannt gemachte Fall: "... konnten US-Behörden ihn lokalisieren. 41 Minuten später nahmen deutsche Beamte ihn fest." Quelle: Drahtzieher im groß angelegtem Bankbetrug festgenommen. Hier wurde anschaulich gezeigt, wie erfolgreich die Exekutive zusammengearbeitet hat und diese "Experten" verhaften konnte. Glaube also nicht, dass es Dir nicht passieren kann!

1.2.2 Sie sind selber schuld, wenn sie ihre Systeme nicht absichern.

Nehmen wir an, du willst ein bisschen Hacken und Systeme auf Sicherheitslücken "testen". Vielleicht hast du die Möglichkeit bekommen eine Seite, ein Forum, ein Shop oder was auch immer zu übernehmen. Für den Betroffenen entsteht dadurch immer ein Schaden. Bei kommerziellen Angeboten sogar ein Finanzieller. Zu argumentieren, dass sie ja selber schuld sind, ist ziemlich blauäugig. Man könnte genauso behaupten, dass diejenigen, die ihre Autos auf der Straße parken müssen, selber schuld sind, wenn sie Kratzer im Lack verpasst bekommen.

Eine Webpräsenz zu zerstören könnte man mit dem Anzünden eines Fahrzeugs vergleichen. Sollten Kundendaten kopiert werden, könnte man auch das damit vergleichen, dass mit dem gestohlenen Fahrzeug eine Straftat verübt worden ist.

Vielleicht wird dir nach diesen Vergleichen klar, dass die Betroffenen es nicht mit einem Schulterzucken abtun werden. Mit jedem weiteren Hack, wird der Druck auf die Legislative höher. Schon jetzt werden die Stimmen laut härtere Strafen für Datenhehlerei zu verhängen.

1.2.3 Freedom Fighter oder Terrorist

Nehmen wir an, Du kämpfst gegen die Ungerechtigkeiten, die in deinem Land vom Staat verübt werden. Deswegen bist du auf der "richtigen" Seite und glaubst "im Recht" zu sein. Genau hier fängt schon die Selbstlüge an! Für einige wirst du vielleicht ein Held sein und neben Che oder Gandhi gereiht. Für die meisten bist du jedoch ein Terrorist! Ein subversives Subjekt, das aus der Gesellschaft entfernt werden muss.

In den letzten zehn Jahren wurden viele wegen "terroristischen Tätigkeiten" verurteilt oder gar verschleppt. Man erinnert sich nur an den gefangenen, in Deutschland geborenen Türken, der nach Guantanamo verschleppt und dem nie vorher ein Prozess gemacht worden ist. Ob zu Recht oder Unrecht, beschuldigt für die Al-Qaida tätig zu sein, kann dir den Mittag versauen. Es spielt dabei keine Rolle, ob es stimmt.

Wenn du glaubst in einem Rechtsstaat, wie BRD behautet eins zu sein, sicher zu sein, gehörst du zu den 40%, die noch kein Kontakt damit hatten. Dein "Freund und Helfer" in Blau ist nur ein Werkzeug, das im besten Fall kalt und distanziert nach Vorschrift handelt und sich stets an das geltende Recht hält. Leider ist das selten der Fall. Oft sind die exekutiven "Hüter des Rechts", vor allem die Jungen, übermütig und meinen die Handschellen extra stramm anlegen zu müssen. Solltest du verhaftet worden sein, werden dir alle deine Sachen, zur Verwahrung, entnommen. Sollte sich auch darunter ein Portmonee mit Banknoten befinden, solltest du nicht überrascht sein, wenn die bei der Rückgabe fehlen sollten.

Auch die Judikative geht den Weg des geringsten Widerstandes. Es wird sich keiner für dich einsetzen, nur um dem Recht Genüge zu tun. Es werden zeitsparende und teilweise rechtswidrige Urteile gefällt. Die Gründe sind vielseitig. Ob es mit der persönlichen Befindung oder Einstellung des Richters zusammenhängt. Oder durch die derzeitige Rechtsgrundlage, die auch sehr fragwürdig sein kann. Recht haben und Recht bekommen, sind und bleiben verschiedene Sachen, wie es gerade vor kurzem wieder mal geschehen ist: Polizisten halten eine Frau illegal fest: Die Staatsanwaltschaft meint, den Beamten war unklar, dass das verboten ist.

In einem Land, wo man dich in ein Präventivgewahrsam für 24 Stunden, ohne vorherige richterliche Verfügung stecken kann, kannst du nicht drauf hoffen, fair behandelt zu werden. Auch in einem Staat, in dem Beweise, nach einer rechtswidrigen Hausdurchsuchung, verwendet werden können, ist es mit dem Recht nicht weit. Erklärung zur Gefahr im Verzug. Ein weiter interessanter Artikel über rechtswidrige Beweise.

Und das alles in ein einem vermeintlichen Rechtsstaat. Nicht auszudenken was in einer, sagen wir mal, nicht so zivilisiertem Land alles zu Norm gehört.

Anonym zu bleiben ist unter diesen Umständen absolut unumgänglich.

Ob du dich in einer der Gruppen einordnest oder ein anderes Bild von dir hast, spielt kaum eine Rolle. Natürlich ist es wichtig, dass du dich selber in einem "guten Licht" siehst; schon alleine von der psychologischen Seite her. Wichtiger, ja überlebenswichtig ist es jedoch die Frage, wie dich dein Gegner sieht. Wirklich sieht und nicht wie du es gerne hättest!

Ein Fehler kann dich viel kosten. Ob es Geld, Freiheit oder dein Leben ist, hängt von der Tat, die man dir anlasten wird.

Auch wenn du nur ein kleiner Fisch bist und dich in den dunklen Weiten des Internets versteckst. Ist man auf dich aufmerksam geworden, wird man dich ins Licht zerren, um dich wie einen Fisch auszunehmen. Dabei wird dir der kleinste Fehler zum Verhängnis.

Ich hoffe, dass du die oberen Zeilen nicht zu sehr als eine Standpauke empfunden hast. Wichtig ist vor allem, dass du dich nicht, durch deine falschen Annahmen, in Sicherheit wiegst und mit offenen Augen durch die Welt gehst.

1.3 Ich bin sicher, da ich zusätzlich VPN benutze.

Nein. Das ist nicht per se so. Was oft nicht verstanden wird, ist, dass die VPN-Provider lediglich deine Privatsphäre gegenüber Dritten schützen. Und das nur soweit, bis sie durch einen Richterbeschluss zur Offenlegung der Daten gezwungen werden.

Ob die VPN-Provider wirklich nichts speichern, kannst du nicht wissen. Es kann sein, dass sie es aus "Versehen" tun. Oder dazu gezwungen wurden, z.B. durch den oben erwähnten Richterbeschluss. Oder weil sie einen Deal, mit Behörden und Agenturen eingegangen sind. Du kannst nicht mal sicher sein, dass nicht die Agenturen selbst diesen Dienst anbieten! Deswegen ist die Nutzung von Tor zur VPN, um deine Anonymität zu schützen, unumgänglich. Mehr dazu im Punkt 4 (fast) Anonym durch VPN, Tor, JonDo & Co.

1.4 Vorratsdatenspeicherung ist gefallen. Mir kann also nichts passieren.

Falsch. Telekom hat erstritten, dass sie 7 Tage die IP Adressen speichern dürfen. Auch die der Flatrate-Nutzer! Da Telekom es macht, werden es auch andere machen.

Auch wenn die Bestands- und Verkehrs-Daten eigentlich nur zur Störungsbeseitigung gespeichert werden und nicht für die Straffverfolgung genutzt werden dürfen, glaubt nicht, dass dich das schützt. Siehe dazu Rechtswidrig erlangte Beweise dürfen verwendet werden

1.5 Mit PGP bin ich sicher.

Eben nicht. Mit dem PGP-Verfahren wird lediglich der Nachrichteninhalt verschlüsselt. Der Versender und der Empfänger sind im Klartext zu sehen.

Mit diesen Meta-Daten kann ein Profil erstellt werden. Sollte dein Kommunikationspartner unter Beobachtung stehen, wirst du automatisch in die Liste der Verdächtigen aufgenommen. Wie das umgangen werden kann, erfährst du unter Punkt 6.1. Sicherer E-Mail-Verkehr.

2. Du, das größte Sicherheitsrisiko

In den oberen Betrachtungen wurden mehrere Aktivitäten und deren Problematik beschrieben. Dass es weit mehr als die Genannten gibt, versteht sich von selbst. Was sie alle, auch die nicht Genannten, verbindet, ist, dass sie weitgehend illegal sind. Es gibt also Institutionen, ob staatlicher oder privater Natur, die gegen dich vorgehen werden. Um sich dagegen zu schützen, muss du in erste Linie verschwiegen sein.

2.1 Verschwiegenheit

Das heißt:

- Nirgends deinen richtigen Namen nennen.
- Niemanden deine Adresse nennen.
- Keiner darf über deine privaten Interessen Kenntnis haben.
- Fotos von dir sind absolut verboten. Auch Fragmente davon.
- Kontakt im Real Live (RL) ist zu vermeiden.
- Niemals deine private Handy Nummer weitergeben.
- Niemals mit deinem privaten Handy einen Anonyme SIM verwenden.
- Deine Freunde im RL dürfen nichts von deinen Aktivitäten wissen,
- schon gar nicht deine Freundin/Frau/Freund/Mann!

Wieso keiner deiner "Geschäftspartner" deinen richtigen Namen und/oder deine Wohnadresse kennen darf, ist im Grunde klar: Du bist erpressbar bzw. kannst von Rechtsbeamten leichter identifiziert werden. Deine Identität kann durch Fehler, die du begehst, rekonstruiert werden. Beispiele sind Nicknames im Forum, E-Mail usw. den Rückschluss auf deinen Namen oder Wohnort erlauben.

Links zu deinem Facebook- oder Twitter-Account, auch wenn du sie nicht als deine Accounts angegeben hast, können in Verbindung mit anderen Angaben deiner Person zugeschrieben werden. Gibst du deine Interessen preis, z.B., dass du letzte Woche auf einem Konzert gewesen bist, kann man dich, in Verbindung mit dem Facebook oder Twitter, auf dem du darüber gepostet hast, Identifizieren. Analog gilt das für deinen Job, Hobby, Lebensstatus usw.

Hat man mögliche Verbindung im RL ermittelt, können Fotos von dir noch einfacher zugeordnet werden. Auch wenn es sich nur um Fragmente handelt. Bei Besonderheiten wie z.B. Tattoos oder einen absonderlichen Finger ist es besonders einfach.

Hast du aus Versehen deine private Handy Nummer weitergegeben, gleicht das einen GAU. Auch wenn sie nicht auf deinen Namen angemeldet ist, kann man anhand der Nummern, die du anrufst, auf deine Identität schließen.
Hast du dir eine Prepaid Simkarte gekauft und sie unter falschen Namen angemeldet, sie jedoch mit deinem privaten Handy benutzt, kann man anhand der IMEI Nummer trotzdem auf deine Identität kommen. Auch wenn sie nicht 100% einzigartig ist, wird man sie auf die Liste der zu abhörenden Telefone setzen. Man kann auch das Handy mit der entsprechenden IMEI Nummer triangulieren. Da es in BRD den Behörden nicht erlaubt ist Nutzer ständig zu triangulieren, werden Stille-, Test- bzw. 0-SMS versendet. Somit gehen die Behörden die Regelung um und erhalten so deine Bewegungsmuster. Mehr dazu unter Punkt 6.2 Handykontrolle

Die besten Freunde können ganz schnell zum schlimmsten Feind werden. Deswegen kann es dich viel kosten, solltest du so indiskret sein und mit deinen Aktivitäten vor deinen (noch) Freunden prallen. Oft muss es nicht mal das sein. Manchmal prallen deine Freunde mit dir und verraten dich ungewollt.

Was für deine Freunde zutrifft, trifft umso mehr für deinen Lebenspartner! Trennt man sich, kann die/der Ex meist sehr nachtragend sein und jede deiner Schwächen gegen dich verwenden. Sollte man mehr über dich wissen, als gesund für dich wäre, kannst du mit dem Besuch der örtlichen Polizei rechnen. Auch ungewollt kann es zu der besagten Verhaftung kommen, wie es z.B. den Anonymos Hacker Higinio O Ochoa (wQrmer) traf. Er wurde geschnappt, weil er ein Foto seiner Freundin auf Twitter gepostet hat. Leider hat er die Exif- Daten im besagten Bild nicht gelöscht.

Wie du die Exif-Daten aus deinen Bilder löscht, wurde bereits von Frank Castle erklärt. Somit verriet ihn seine Freundin, ohne ihren Mund aufzumachen. Aber auch ohne diesen makabren Witz sollte jedem klar sein, dass man sich verplappern kann und was für einen selbst gilt, gilt auch für deine Mitwisser.

2.2 Datenverschwiegenheit

Aber nicht nur du muss verschwiegen sein. Auch dein Werkzeug muss verschwiegen sein.
Das heißt:

- Fotos nie mit Exif- und Meta-Daten veröffentlichen.
- Handgeschriebene Zettel solltest du nicht veröffentlichen.
- Nie von deinem Drucker ausgedruckte Blätter abgeben.
- Nie deinen regulären PC/Notebook für einen Job benutzen.
- Nie zu viel schreiben.
- Nie mit deinem Auto zum Job fahren.

Oft werden Fotos in Forum gepostet. Dass man die Exif-Daten entfernen muss, wurde oben genannt. Dass einen die eigene Handschrift verrät, scheint vielen nicht bekannt zu sein. Wendet man ein Schriftvergleich an, kann man dich identifizieren.

Auch dein Drucker kann dich verraten. Dass viele Laser-Drucker sogenannte Tracking-Dots, Wasserzeichen oder Machine Identification Code (MIC) auf dem Ausdruck hinterlassen, ist bekannt. Anhand dieser, kann man die Hersteller und Seriennummer des Gerätes, sowie Datum und Uhrzeit des Druckvorgangs erhalten.

Hier noch eine weitere Quelle.

Eine weitere Möglichkeit ist die Drucker anhand ihrer Unregelmäßigkeiten zu ermitteln. "Wie mechanische Schreibmaschinen auch", hinterlassen die Drucker "kleine, individuelle Abweichungen" die dem jeweiligen Drucker zugeordnet werden können.

Das solltet ihr beachten, wenn ihr darüber nachdenkt, eure fingierten Überweisungsausdrucke an die Bank zu senden.

Nie mit der "inkognito" Hardware rumsurfen! Es ist dein Werkzeug, das du ausschließlich für diesen einen Job benutzt! Zum Rumspielen benutzt du ein anderes Gerät!

Wieso wirst du jetzt vielleicht fragen. Die Antwort ist genauso einfach wie einleuchtend: umso mehr Spuren du hinterlässt, und du hinterlässt eine Menge Spuren, desto einfacher wirst du identifiziert. Je mehr Seiten du besuchst, je mehr Inhalte dein Rechner passieren, desto mehr Anhaltspunkte werden gesammelt, wer du bist.

Des Weiteren steigt das Risiko, dass du was Dummes tust und dich, wie schon erwähnt, z.B. in deinem privaten Facebook Account anmeldest. Die hinterlassenen Cookies geben Rückschlüsse auf deine Identität. So kann Facebook, auch wenn du nicht angemeldet bist, Daten über dich sammeln.

Die Tracking-Möglichkeiten bleiben jedoch nicht nur auf den Cookies hängen. Manche "Cookies" können nicht einmal gelöscht werden! Werbefirmen setzen bereits häufig nichtlöschbaren Cookie-Nachfolger ein.

Anhand deines Schreibverhaltens, deiner Satzbildung oder deiner Rechtschreibfehler, kann man dich identifizieren. Es ist so einzigartig, wie deine Handschrift. Die Verwendung eines bestimmten, außergewöhnlichen Wortes, kann einen Hinweis zur deiner Identifizierung liefern.

Dein Auto hat mindestens zwei Kennzeichen. Wenn du umweltbewusst bist, auch ein Drittes, Grünes, an deiner Windschutzscheibe Klebendes. Passierst du eine Maut-Station auf der Autobahn, wird es von Toll-Collect, dem Betreiber dieser Stationen, aufgenommen. Diese sollen zur Verbrechensbekämpfung genutzt werden können. Zurzeit ist das noch nicht rechtsgültig, aber wer schon den Artikel über rechtswidrige Beweise gelesen hat, wird wohl anders über mögliche Beweise denken.

Wie weit die Kameras auf den Ampeln, die zur Verkehrsüberwachung dienen sollen, verwendbaren Bilder von dir oder deinem Kennzeichen liefern können, ist mir nicht bekannt. Bei dem derzeitigen Stand der Technik ist der Gedanke nicht gerade abwegig.

Dein Kennzeichen abzuschrauben und die grüne Plakette abzukratzen, ist nicht das richtige Vorgehen. Das provoziert geradezu eine Polizeikontrolle. Wie du es dennoch unmerklich, unkenntlich machen kannst, wird in dem Buch "Das verbotene Buch" von Anonymus beschrieben.

Einzel für sich genommen, sind die meisten Informationen nichtsagend. In der Summe jedoch bilden sie ein Gesamtbild, dass die Profiler zu einer Identität zusammensetzen. Bei einer Anklage werden sie gegen dich verwendet.

2.3 Identitäten erstellen

Die Identitäten sollen wie Sleeves an und ausgezogen werden. Erstelle jede Einzelne separat für sich. Lass sie nicht miteinander in Kontakt treten. Auch niemals die Identitäten vertauschen. Identität bedeutet E-Mail, Forum Nicknames, Bitmessenger, TorChat, IRC, Bitcoin Wallet, im Grunde alles, was du für deinen Job benötigst.

Wenn du z.B. Hacker bist und ein paar Personendaten samt Kreditdaten erbeutet hast, verkaufe sie nicht mit derselben Identität. Sollte man auf dich als Hehler aufmerksam werden, würdet du umso interessanter sein. Wenn man dich noch mit Hacken in Verbindung setzen kann, bist du dran. Das gilt natürlich auch für alle anderen Aktivitäten.

Rufe niemals alle E-Mails deiner Identitäten gleichzeitig ab. Das heißt sie nicht alle Accounts in einen E-Mail-Client einfügen. Anhand derselben IP, kann man sie miteinander in Verbindung setzen. Mahr dazu unter Punkt 6.1 sicherer E-Mail-Verkehr.

Verwende möglichst für jede Identität separate Hardware. Das gilt für die Handys wie auch für die Notebooks. Mahr dazu unter Punkt 7. Sichere Hardware.

Nochmal: umso aktiver du bist, desto attraktiver bist du für deine Häscher. Deswegen verteile die verschiedenen Jobs auf unterschiedliche, voneinander unabhängige Identitäten.

3. Welches Betriebssystem

Es gibt unterschiedliche Meinungen, welches OS verwendet werden sollte. Die einen meinen, dass Windows schon OK ist. Man soll schließlich das verwenden, womit man sich auskennt. Die anderen meinen wiederum, dass es verantwortungslos ist. Da kann man sich gleich bei den Bullen melden.
Fakt ist, dass man das so pauschal nicht sagen kann. Je nachdem, was du vorhast, und wie gut du dich auskennst, kann das eine oder das andere für dich die bessere Wahl sein. Schließlich kann Linux, auch wenn im Grunde sicherer als Windows, durch falschen Gebrauch deine Identität verraten. Bei einem kurzzeitigen Einsatz, ist gegen ein gut abgesichertes Windows System nichts einwenden. Bei langfristigen Einsätzen ist eindeutig Linux zu bevorzugen. Aber auch hier ist nicht alles sicher. Ubuntu und seine Derivate sind als unsicher anzusehen.

3.1 Microsoft Windows

Dass Microsoft mit den Geheimdiensten zusammenarbeitet, ist seit dem Snowden-Debakel allseits bekannt. Auch dass die Passwörter für die Anmeldung überhaupt kein Hindernis darstellen, sollte jedem bekannt sein. Was hier eine Abhilfe schaffen könnte, ist die Verschlüsselung der Festplatte. Dazu gibt es mehrere Programme auf dem Markt. Proprietäre Programmen sollte man generell misstrauen, da man nicht prüfen kann, ob sie wirklich das tun, was sie vorgeben. Das bekannteste kostenlose opensource Verschlüsselungsprogramm VeraCrypt, kann dazu genutzt werden diese Aufgabe zu übernehmen. Es ist seit ein paar Monaten umstritten und man behauptet, dass es unsicher sei. Bis jetzt wurden jedoch diese Behauptungen nicht gänzlich bewiesen. Dass die Preboot-Variante gehackt worden ist, ist seit fünf Jahren bekannt. Die Verschlüsselung der Container gilt bis heute jedoch als sicher. Natürlich in Abhängigkeit der Passphrase.

Eine Alternative zum Preboot würde eine Virtuelle Maschine (VM) in einem verschlüsselten Container darstellen. Das erfordert jedoch, dass dein PC ausreichend Ressourcen zur Verfügung hat. Ein Betrieb in VM bringt zusätzlich den Vorteil, dass die meiste Schadsoftware nicht aktiv wird. Dies ist ein Selbstschutz, da die Virenscanner Schädlinge in eine VM gepackt und so identifiziert werden. Solltest du dir jedoch in der Hauptinstallation einen Keylogger einfangen, kann das Passwort des Containers abgefangen werden. Damit ist die Sicherheit dahin.

Eine weitere Sicherheitslücke besteht beim laufenden Rechner. Sollte der PC laufen und entsperrt sein, kann man die Passwörter unter Windows aus dem RAM auslesen.

Windows ist das meistverbreitete OS und deswegen auch das meist verseuchte. Viren, Trojaner und andere Malware sind Standard unter Windows. Ein aktueller Virenscanner ist daher Pflicht. In der c‘t 5/2013 wurden 16 Virenwächter mit 248 Trojanern getestet. Man sollte sich jedoch nicht in Sicherheit wiegen. Virenscanner hinken den Viren hinterher. Ein Virenscanner kann dich nicht vor 0-Day Exploits schützen.

3.2 Linux

Linux ist nicht gleich Linux. Während du mit Ubuntu von Live-CD starten kannst, muss du bei Arch alles selber kompilieren. Bei Debian wiederum kannst du nicht davon ausgehen, dass die neuste Hardware unterstützt wird.

Linux bringt vom Hause aus viele Sicherheitseinstellungen, die nicht ohne weiteres überwunden werden können. Hier kann man z.B. schon während der Installation die komplette Festplatte verschlüsseln. Somit kann man sich diese Krücke, die bei Windows angewendet werden muss, sparen. Zudem laufen sogar die neusten Linux Distributionen auf älterer Hardware. Das steigert deine Sicherheit enorm, da du Notebooks

schon für kleines Geld kaufen und somit deine Private- von der Arbeits-Hardware trennen kannst. Problem stellt nur dein Wissen über den Umgang mit dem OS.

Bist du nicht in der Lage mit dem OS sicher umzugehen, wirst du deine Anonymität nicht wahren können. Du musst noch einige Einstellungen vornehmen, damit du z.B. ausschließlich über Tor mit dem Internet verbunden bist. Bricht die Verbindung ab, darf über deine IP kein Traffic erzeugt werden. Auch der DNS-Leak muss du stopfen, wenn du mit VPN im Internet bist. Dazu kommst du um die IP-Tables nicht herum. Dass es wichtig ist immer anonym zu sein, hat Hector Xavier Monsegur alias »Sabu« der Anoymos Hacker-Gruppe LulzSec, schmerzlich in Erfahrung gebracht. Er wurde nur deswegen geschnappt, weil er sich ein einziges Mal in seinem IRC Chanel ohne Tor eingeloggt hat. Hätte er nicht mit der FBI kooperiert, säße er jetzt, wie der Rest der Gruppe, für eine lange Zeit ein.

Außerdem ist die pauschale Aussage, dass das Linux sicher ist, einfach falsch! Benutzerfreundliche Linux-Distributionen wie Ubuntu, werden als unsicher eingestuft. Richard Stallman, Gründer und Präsident der Free Software Foundation, bezeichnet Ubuntu (Version 12.10) sogar als Spyware, da sie die Daten der Nutzer ausliest und an Amazon sendet. Auch wenn es anonymisiert geschehen soll, deine Daten werden abgegriffen und analysiert.

Ubuntu-Derivate sind ebenfalls nicht empfehlenswert.

Fakt ist, ob Windows oder Linux, du musst dich mit deinem Werkzeug gut auskennen, um damit auch sicher arbeiten zu können. Das gilt für die Bohrmaschine wie auch für das Betriebssystem.

Wenn du mit dem Gedanken spielst, von Windows auf Linux umzusteigen, muss du viel Zeit investieren und viel lesen, um in das OS einzusteigen. In dem Artikel "Das richtige Linux für Sie" in der c't 19/2014, sind die gängigsten Linux Betriebssysteme anschaulich vorgestellt.

4. (fast) Anonym durch VPN, Tor, JonDo & Co

Who do I trust? Me!
Scarface

4.1 Tor

Dass du diesen Text lesen kannst, zeugt davon, dass du weißt, wie man Tor benutzt.
Falls du es noch nicht mitbekommen hast, sind Angriffe auf das Tor-Netzwerk nichts Neues. Tor kann mit Bad-Exit-Nodes zu phischen genutzt werden. Russische, britische und US-amerikanische Geheimdienste versuchen die Verschlüsselung von Tor aufzubrechen. Diese und andere Meldungen zeugen davon, das Tor alleine deine Anonymität nur bedingt schützt. Eine Kaskadierung, also Hintereinanderschaltung mehrerer Anonymisierungsdienste, steigert die Sicherheit. Ein VPN-Dienst bietet sich da als eine gute Wahl an.

4.2 JonDo

JonDo ist ein weiterer Anonymisierungs-Anbieter. Sein Vorteil ist, dass die Server in einem geschlossenen System kaskadiert werden. So kann kein Bad-Exit-Node von außen eingesetzt werden. Der Nachteil ist, dass die seit 2003 Aufrufe von bestimmten Webseiten Flagen und an Strafverfolgung übergeben. Ein Bericht über die zur Strafverfolgung durchgeführten Überwachungen kannst du auf deren Seite nachlesen.

4.3 VPN-Provider

Virtual Private Network (VPN) ist ein Verfahren in einer unsicheren Umgebung, einen verschlüsselten und somit sicheren Tunnel einzurichten. Dadurch kann ein Dritter dein Traffic von außen nicht anschauen. Eigentlich eine geniale Sache, hätte sie nicht einen gravierenden Fehler. Vertrauen!

VPN-Anbieter gibt es wie Sand am Meer. Und alle behaupten, keine Log-Files zu speichern. Aber wie schon unter Punkt 1.3 erwähnt, kannst du dir weder sicher sein, ob die Provider nicht doch mit den Behörden und Agenturen zusammenarbeiten, noch ob sie diesen Dienst nicht selber anbieten. Sozusagen den Mittelsmann umgehen.

Lese weiter, wie du dich davor schützen kannst.

4.4 VPN/Tor Kaskadierung

grugq schrieb:

TOR Connection to a VPN => OK VPN Connection to TOR => GOTO JAIL

Diese Behauptung wurde schon in diesem Thread diskutiert.

Da hier jedoch vom Worst Case ausgegangen wird, wird das Thema nochmal ausführlich behandelt.

Da du niemandem vertrauen kannst und darfst, musst du davon ausgehen, dass der VPN- Provider deine reale IP-Adresse speichern und weitergeben wird. Damit er das nicht kann, musst du seine Dienste anonym in Anspruch nehmen. Dies ist am einfachsten über einen Router, mit OpenWRT oder P O R T A L realisiert. Somit hast du einen Hardware-Basierten Zugang zum Internet. Der Router sollte so konfiguriert werden, dass es alle Pakte nur über Tor leitet und bei Abbruch der Verbindung zum Tor nicht über deine reale IP-Adresse weiter surft. Ist das gewährleistet, kannst du dich mit dem VPN-Provider verbinden. Somit hast du mit dem Tor deine Anonymität verschleiert und mit dem VPN-Tunnel nochmal den gesamten Traffic verschlüsselt. Sollten jetzt die Exit-Nods korrupt sein, sind die Daten vom VPN verschlüsselt und für den Angreifer nicht zu ersehen. Sollte sich bei dem Angreifer um eine Behörde handeln, wird sie nur die IP-Adresse deines VPN-Providers und nicht deine eigene erhalten. Da dieser jedoch deine Identität nicht kennt, ist die Anonymität weitgehend gewährleistet.

Ein weiterer Vorteil ist, dass manche Dienste, z.B. PayPal oder eBay, Nutzer von Tor sperren. Meldest du dich mit Tor in einem PayPal-Konto an, wird es kurze Zeit später gesperrt. Verwendest du hingegen ein VPN-Tunnel, ist die Wahrscheinlichkeit höher, dass die zugeteilte IP nicht indexiert ist. Bei VPN-Diensten solltest du deswegen darauf achten, dass die Server ihre IP nicht statisch, sondern dynamisch zugewiesen bekommen. So ist die Indexierung der Proxys und Vorabsperrung deiner Accounts so gut wie ausgeschlossen. Nachteil ist, dass du nicht mehr onion Seiten aufrufen kannst. Dazu muss der letzte Verbindungspunkt ein Ton-Exit-Node sein. Willst du sie doch anzeigen lassen, musst du nur noch ein Tor-Browser einsetzen. Dadurch hast du eine Kaskadierung von Tor->VPN->Tor, was mit Geschwindigkeitseinbußen quittiert wird, dir jedoch eine sicherere Verbindung garantiert.

4.5 Internetverbindung

Sollten alle Stricke reißen, wird deine IP offengelegt. Deswegen solltest du dafür sorgen, dass es nicht deine IP ist. Wie du ins Internet kommst, ohne deinen privaten Zugang zu benutzen, erfährst du in den folgenden Zeilen.

4.5.1 Offene Café WLAN

Das neue Gesetz zur "Störer Haftung" soll Cafés und Bars ermöglichen bedenkenlos offene WLAN-Spots anzubieten. Die WLANs in Hotels sind oft verschlüsselt und nur den Gästen zugänglich gemacht. McDonald‘s bietet meistens ein WLAN Zugang an. Empfehlenswert ist es dennoch nicht dort seine Jobs zu erledigen. Die Kameras im Store, die auf die Gäste gerichtet sind, können Aufnahmen zur späteren Identifizierung liefern. Bis das neue Gesetz beschlossen und umgesetzt wird, dauert es wohl noch eine Weile. Du musst also ein offenes AP suchen. Da man generell keinem offenen AP trauen darf, sollte man auch hier stets Tor oder/und VPN benutzen.

4.5.2 Wardriving

Bei Wardriving (Wireless Access Revolution driving) geht es darum, offene Netze, mit Hilfe eines Fahrzeugs und eines Notebooks zu finden. Natürlich muss nicht unbedingt ein Auto dafür benutzt werden. Du kannst es mit Hilfe eines Smartphones, PDAs oder die PlayStation Portable machen. Zu fuß, mit dem Fahrrad oder mit einer Drohne. Wenn du eine Katze hast, auch mit der. So entdeckte offene Access Points, kannst du für deine verdeckten Jobs benutzen.

Vorsicht ist jedoch geboten, wenn du lange Zeit im Auto mit einem Notebook sitzt. Vor allem nachts, wenn der Bildschirm dein Gesicht gespenstisch beleuchtet, kann der eine oder andere besorgte Bürger, dir die

Ordnungshüter auf den Hals hetzen.

Da man generell keinem offenen AP trauen darf, sollte man vor allem hier stets Tor oder/und VPN benutzen. Übrigens, das Surfen in ungesicherten WLANs ist nicht strafbar.

4.5.3 Freifunk

Mit freifunk.net kommst du kostenlos ins Internet. Die Netze dieser ehrenamtlichen und privaten Organisation sind in den meisten Städten vorhanden. Auf deren Webseite kannst du die Orte, an den du ein Netz brauchst, suchen. Es ist ein Verbund freiwilliger, privater Personen, die ein unabhängiges Netz, neben dem Internet, aufbauen und verwalten. Manche von ihnen bieten ebenfalls einen Zugang zum Internet an. Wenn du deren Dienst in Anspruch nimmst, sei dir im Klaren, dass, solltest du deine Spuren schlecht verschleiern, der Betreiber des Zugangs für deine Taten zur Verantwortung gezogen werden kann. Dadurch wird eine gute Sache in den Schmutz gezogen.

4.5.4 Mobile Verbindung über anonyme SIM

Willst du mobil und nicht auf offene WLAN Hotspots angewiesen sein, kaufst du dir Prepaid SIM-Karten. Mit einem UMTS Modem, kannst du dann im Park unter Linden deine Jobs erledigen.
Wie du es sicher betreibst, findest du unter Punkt 7. Sichere Hardware. Was jedoch für Handy gilt, gilt auch für die UMTS-Modems. Sie können trianguliert und somit geortet werden. Bei Fonic z.B. kannst du für 10€ eine Monats-Flat bekommen. Da die Karten meistens billiger zu haben sind (bei Media-Markt waren sie für 5€ und bei dm für 8€ zu haben) hast du einen relativ günstigen und flexiblen Internet-Zugang. Dabei gilt auch, dass du es nie in der Nähe deines Wohnortes verwenden darfst! Auch die zeitlich begrenzte Nutzung sollte klar sein. Auf Dauer kann diese Variante ein "Teurer" Spaß sein.

4.6 Sicherheitsrisiko IPv6

Da die Internet-Adressen langsam knapp werden, soll das neue IPv6 Protokoll, das bereits in die Jahre gekommenes IPv4, ablösen. Damit kann jedes Gerät direkt mit dem Internet verbunden sein, ohne aus einem privaten LAN über einen Router in das Internet geleitet werden zu müssen. Und genau das kann sich als ein Nachteil erweisen, denn damit wird es möglich jedem Gerät eine feste IP zu geben. Somit kann man jedes an dich versendete Internet-Paket identifizieren.

Ein weiteres Problem stellt die Handhabung der Heade-Extensions dar, die nicht näher definiert worden ist. Die Probleme entstehen dadurch, dass die Firewalls und Router nicht in diese Header reinschauen dürfen. Diese Regel öffnet Tür und Tor für Attacken auf das System.

Außerdem wird die Handhabung der Sicherheitseinstellungen komplexer und dadurch Fehleranfälliger.
Da es zurzeit nicht nötig ist IPv6 zu verwenden, solltest du es bei dir abschalten!

4.6.1 Deaktivierung der IPv6

"In Ubuntu 10.04 und 12.04 ist IPv6 direkt in den Kernel kompiliert und wird nicht als Modul geladen. Die einfachste Methode um IPv6 zu deaktivieren ist den passenden sysctl Parameter zu setzen. Temporär kann dies mit folgendem Kommando erfolgen:

```
echo 1 > /proc/sys/net/ipv6/conf/all/disable_ipv6
```

Um diese Einstellung dauerhaft vorzunehmen bietet es sich an auf die sysctl Funktionalitäten zurückzugreifen. Dafür einfach eine Datei namens /etc/sysctl.d/01-disable-ipv6.conf anlegen mit folgendem Inhalt:

```
Net.ipv6.conf.all.disable_ipv6 = 1
```

Nach dem nächsten Reboot ist IPv6 dann deaktiviert.

Am besten kann dies mit dem Kommando »ip addr show« überprüft werden. Es darf dann keine Einträge mit dem Text »inet6« mehr geben.

ip addr show | grep inet6

In RHEL 4 / CentOS 4 ist IPv6 als Modul integriert.

Um dies zu deaktivieren einfach folgende Zeile in der Datei /etc/modprobe.conf hinzufügen: install ipv6

/bin/true

Die Überprüfung ob es geklappt hat kann wie unter Ubuntu 10.04 mit dem Kommando »ip addr show | grep inet6« oder alternativ mit dem Kommando

lsmod | grep -i ipv6

erfolgen.

Windows Vista, Windows 7, Windows Server 2008

Informationen zum abschaltet des IPv6 bei Microsoft Produkten, erhältst du im MS Support."
Quelle: Thomas Krenn

5. Browser absichern

Die zwei Browser, die deine Privatsphäre am meisten schützen, sind Firefox und Chrom. Auch wenn Chrom gegenüber Firefox eine Sandbox anbietet, ist die Erweiterung von JonDoFox die bessere Wahl. Sie kann kostenlos von der JonDo Webseite bezogen werden und sichert Firefox so weit ab, dass kaum Spuren hinterlassen werden. Die zahlreichen Addons, die mit installiert werden, sind gut gewählt. Der Browser kann über ein JonDo, Tor oder benutzerdefinierten Proxy geleitet werden. Du kannst sie auch ohne Proxy betreiben, was mit dem präparierten Router ohne Bedenken gemacht werden kann. (Punkt 4.4 VPN/Tor Kaskadierung)

5.1 Automatische Absicherung

JonDoFox erstellt ein vermeintlich sicheres Profil in deinem Firefox Browser.
Es ist kostenlos und ohne Bedenken von JonDo GmbH, CHIP oder Heise.de zu beziehen. Nach der Installation wirst du gefragt, ob die JonDo Software installiert werden soll. Das beantwortest du natürlich mit einem klaren NEIN.
Zum Schluss wählst du unter "JonDoFox Einstellungen" "Kein Proxy" aus.

Solltest du Windows benutzen, füge im "Ziel" des Firefox Links "-no-remote -P" hinter dem Pfad. Es muss also in etwa so aussehen "C:\ Program Files\ Mozilla Firefox\ firefox.exe« -noremote -P"
Dadurch wirst du jedes Mal gefragt, welches Profil du öffnen möchtest.

5.2 Manuelle Absicherung

Mit den folgenden Einstellungen kannst du Firefox Manuel an deine Sicherheitsbedürfnisse anpassen.

About:config Einstellungen

geo.enabled = false geo.wifi.uri = [leer
lassen] network.http.accept.default =
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
network.http.use-cache = false network.http.keep-alive.timeout = 600
network.http.max-persistent-connections-per-proxy = 16
network.proxy.socks_remote_dns = true network.cookie.lifetimePolicy = 2
network.http.sendRefererHeader = 0 network.http.sendSecureXSiteReferrer
= false
network.protocol-handler.external = false [default und alle weiteren Sub-Einstellungen auf false]
network.protocol-handler.warn-external = true [default und alle weiteren Sub-Einstellungen auf true]
network.http.pipelining = true

network.http.pipelining.maxrequests = 8
network.http.proxy.keep-alive = true
network.http.proxy.pipelining = true
network.prefetch-next = false
browser.cache.disk.enable = false
browser.cache.offline.enable = false
browser.sessionstore.privacy_level = 2
browser.sessionhistory.max_entries = 2 browser.display.use_document_fonts = 0
intl.charsetmenu.browser.cache = ISO-8859-9, windows-1252, windows-1251, ISO-88591, UTF-8
dom.storage.enabled = false extensions.blocklist.enabled = false

Andere Einstellungen

Alle Plug-Ins ausschalten [Extras -> Addons -> Plug-Ins]
Chronik ausschalten [Chronik -> Chronik toolbar -> R/Click neuste Chronik löschen -> löschen]
Alle Updates ausschalten [Extras -> Einstellungen -> erweitert -> update]
'Do not track' Einschalten [Extras -> Einstellungen -> Datenschutz]
Privaten Modus Einschalten, Einstellen auf »nicht anlegen« & Cookies von Drittanbietern ausschalten. [Extras -> Einstellungen -> Datenschutz]

6. Kommunikation

Die Kommunikation mit deinen Partnern, den Opfern oder zur Informationsabfragung muss immer anonym stattfinden. Neben der E-Mail werden noch Torchat, IRC, Bitmassage und andere verwendet. Da nicht alle vom Hause aus deine Sicherheit und Anonymität gewährleisten, musst du selber dafür sorgen.

6.1 Sicherer E-Mail-Verkehr

Es gibt viele Provider, die mit vermeintlich sicheren E-Mail Account werben. Sie behaupten, dass die Mails auf den Servern verschlüsselt werden und sie somit keinen Zugriff auf die abgelegten E-Mails haben. Dass man ihnen nicht glauben darf, sollte jedem klar sein. "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. Nach Ansicht der US-Behörden reicht es aus, wenn die Server in den USA stehen." Damit sollte man auch von in den USA ansässigen Providern Abstand nehmen.

Aber auch in Deutschland kann ein Provider mit einem Richterbeschluss zur Aushändigung der Daten gezwungen werden. Deswegen sind folgende Maßnahmen zur Sicherstellung deiner Anonymität wichtig.

6.1.1 Anonyme E-Mail Accounts aus dem Clearnet

Hier eine Liste der Provider, die die Verschlüsselung ihrer Server richtig handhaben.

JPBerlin
Standort: BRD Kosten: 1€/Monat
Besonderheit: Bezahlung per Brief und Bitcoin möglich

MyKolab.com Standort: Schweiz
Kosten: 10 CHF/ Monat

Private DE Mail Standort: BRD
Kosten: kostenlos
Besonderheiten: Betreiber unbekannt.
Tor Hidden Services für alle Protokolle

VFEmail
Standort: USA!!!
Kosten: kostenlos
Besonderheit: Tor Hidden Service vorhanden.
IP-Adressen der Absender werden für Premium Nutzer versteckt. Hosting in

Niederlande wählbar für Silber-Account (15$/Jahr)

Posteo
Standort: BRD Kosten: 1€/Monat
Besonderheit: anonyme Bezahlung per Brief möglich

Posteo veröffentlicht als erster deutscher Mailanbieter einen Transparenzbericht Secure-Mail.biz
Standort: Unbekannt. Server stehen in Russland und Norwegen Kosten: z.Z. Kostenlos
Besonderheit: wurde an Perfect Privacy VPN-Provider übergeben. Wird gerade umgestellt. (Stand 2014)

Vorsicht ist bei Safe-Mail.Net geboten. Auch wenn die Betreiber der israelischen Gesetzgebung unterliegen, hat FBI die Benutzer bereits im Visier.

6.1.2 PGP

Manche Provider bieten an, die E-Mail mit PGP-Verschlüsselung über den Web-Frontends zu erledigen. Davon sollte man KEIN Gebrauch machen. Die E-Mails sind nur dann sicher, wenn sie Ende-zu-Ende-Verschlüsselt (E2EE) werden. Der private Schlüssel darf nicht aus der Hand gegeben werden. Deswegen musst du einen E-Mail-Client benutzen. Thunderbird bietet sich dafür wunderbar an.

Um nicht das Rad nochmal erfinden zu müssen, folgt hier eine einfache Beschreibung wie man mit Thunderbird E-Mails verschlüsselt.

Heise Magazin schrieb:

Persönliche Nachrichten sollten verschlüsselt versendet werden. S/MIME ist bei Thunderbird bereits integriert, OpenPGP kann mit dem Add-on Enigmail von Patrick Brunschwig nachgerüstet werden. Außerdem muss GnuPG auf dem Rechner installiert werden: Für Windows gibt es dafür Gpg4Win und für Mac OS GPGTools, womit sich die Einrichtung komfortabel erledigen lässt. Ist das getan und Enigmail installiert, findet sich in Thunderbirds Menüleiste der Punkt „OpenPGP“. In den dortigen Einstellungen muss eventuell der Pfad zur gpg.exe nachgetragen werden. Bei der weiteren Anpassung hilft der OpenPGP-Assistent, der ebenfalls über das OpenPGP-Menü aufzurufen ist. Weil längst nicht alle Mail-Nutzer Nachrichten auch entschlüsseln können, sollten Sie die Option „Nein, ich möchte in Empfängerregeln festlegen, wann verschlüsselt werden soll“ auswählen. Der Assistent bietet zum Schluss an, ein Schlüsselpaar zu erzeugen, bestehend aus einem geheimen und einem öffentlichen Schlüssel. Das Prinzip lässt sich mit einem Vorhängeschloss vergleichen: Der öffentliche Key ist das Schloss, mit dem Nachrichten an Sie gesichert werden; den Schlüssel zur Entsperrung haben nur Sie. Zur Absicherung des privaten Schlüssels empfiehlt sich die Festlegung einer Passphrase. Das kann und soll durchaus ein kompletter Satz sein (und nicht nur ein einzelnes Passwort), idealerweise mit exotischen Sonderzeichen garniert. Enigmail erzeugt nicht nur das Schlüsselpaar, sondern auch das passende Widerrufszertifikat, womit kompromittierte Schlüssel entwertet werden. Den öffentlichen Schlüssel können Sie anschließend verteilen und auf einen Schlüssel-Server wie sks-keyservers.net laden, wo andere ihn herunterladen können.
Um aus einer Mail eine Geheimbotschaft zu machen, rufen Sie in der Einzel-Mail-Ansicht den Menüpunkt „OpenPGP/Nachricht verschlüsseln“ (Strg"+"Shiff+"E) auf. Bedenken Sie, dass Sie den öffentlichen Schlüssel des Empfängers benötigen. Auch angehängte Dateien wie vertrauliche Dokumente können auf Wunsch gleich mit verschlüsselt werden.

6.1.3 Meta-Daten anonymisieren

Die beste E2EE verhindert nicht, dass Meta-Daten anfallen. Aus denen kann man Rückschlüsse auf den Sender und Empfänger ziehen. Mit einem an MIT entwickeltem Tool, kannst du die Header-Analyse ausprobieren. Voraussetzung ist ein Microsoft, Google oder Yahoo E-Mail-Konto.

Das Problem mit den Headern kann mir einem Remailer-Dienst behoben werden.
"Der Versand einer Nachricht über Remailer-Kaskaden ist mit der Versendung eines Briefes vergleichbar, der in mehreren Umschlägen steckt. Jeder Empfänger innerhalb der Kaskade öffnet einen Umschlag und sendet den darin enthaltenen Brief ohne Hinweise auf den vorherigen Absender weiter. Der letzte Remailer der Kaskade liefert den Brief an den Empfänger aus."

Konkret handelt es sich dabei »um anonymisierende Internet-Dienste, die E-Mails annehmen, die ursprünglichen Header entfernen und den Rest zum Ziel weiterleiten. Der Empfänger bekommt nur die IP-Adresse des Remailers zu sehen; die IP-Adresse des Absenders bleibt geheim. So kann man unerkannt Nachrichten absenden. Wenn man eine Antwort haben will, kann man natürlich seine Mail-Adresse in den Mail-Inhalt schreiben und diesen verschlüsseln.

Angreifer können aber aus der Beobachtung des ein- und ausgehenden Remailer- Verkehrs dennoch Rückschlüsse darüber ziehen, wer mit wem kommuniziert. Dagegen haben Remailer-Entwickler mehrere Strategien entworfen, unter anderem die Verschlüsselung der gesamten Mail vor dem Versand, das zeitversetzte Weiterversenden oder auch die Verkettung von mehreren Remailern.

Remailer haben aber wie gewöhnliche Mail-Dienste eine zentralisierte Struktur, bei der man dem Anbieter vertrauen muss. Außerdem bleiben bei diesem Verfahren die Empfänger nicht anonym.«

Mit Quicksilver kannst du unter Windows die Mail mit Mixmaster versenden.
Unter Linux ist das Paket Mixmaster bereits enthalten.

6.1.4 Alternative zur E-Mail Accounts

I2P und Tor bieten spezielle Lösungen an:

"Das Invisible Internet Project (I2P) bietet mit Susimail einen anonymen Mailservice inclusive SMTP- und POP3-Zugang und Gateway ins Web oder mit I2P Bote einen serverlosen, verschlüsselten Maildienst. Das Lelantos-Project ist ein E-Mail Dienst, der von Unbekannten als Tor Hidden Service unter der Adresse lelantoss7bcnwbv.onion betrieben wird. Mail2Tor ist ein weiterer E-Mail Dienst, der von Unbekannten unter mail2tor2zyjdctd.onion bereitgestellt wird. Gateways ins normale Web sind bei beiden Projekten vorhanden."

Mit Usnet kannst du ebenfalls Nachrichten versenden. Die Funktion von Usenet kann mit schwarzen Brettern vergleichen werden und ist älter als das WWW. In der Newsgruppe alt.anonymous.messages werden ständig viele Nachrichten gepostet. Jeder Leser muss die für ihn bestimmten Nachrichten selbst erkennen.

6.2 Handykontrolle

Dein Handy verrät ständig, wo du bist. Anders ist die Funktionalität nicht gewährleistet. Und genau das machen sich die Strafverfolgungsbehörden zu Nutze. Haben Sie deine Handy- Nummer, können Abhöranfragen gestellt werden. In dem ersten Halbjahr 2014, wurden 704-mal Telekommunikationsüberwachungsmaßnahmen von der BKA durchgeführt. Des Weiteren hat BKA 35.000 und die Bundespolizei 69.000 Tracking-SMS versendet.

Die Behörden rufen auch die Funkzellen zu einer bestimmten Zeit ab. Damit bekommen sie angezeigt, welche Handys zu einer gewissen Zeit an dieser Zelle und sich damit an diesem Ort befunden haben. In der ersten Jahreshälfte 2014 wurden diese Angaben 50-mal von der Bundespolizei, 3-mal von der BKA und 100-mal vom Zoll abgefragt.

Anhand der IMEI Nummer, die mehr oder weniger einzigartig ist, kann man das Handy erkennen. Taucht die Nummer mehrmals in der Nähe des »Tatortes« auf, so ist das mehr als ein Indiz, dass sie damit zu tun hat.

Konkretes Beispiel könnte das wiederholte, unsachgemäße Geldabheben sein. Auch wenn du dich verschleiert hast und die Cam des Bankautomaten kein verwendbares Foto von dir liefern kann, könnte man dich anhand der IMEI Nummer überführen.

Hat man die IMEI Nummer, kann auch die derzeit eingesetzte SIM und die Handy Nr. ermittelt werden. Dadurch ist das Handy mit der Triangulation leicht zu orten. Da den Behörden untersagt ist Nutzer ständig zu triangulieren, versenden diese Stille-, Test- bzw. 0-_SMS und erstellen somit ein Bewegungsmuster von

dir.

Normallerweise kann man mit deinen "Normalen" Handy keine 0-SMS anzeigen lassen. Mit einem Patch und einer Software, kann man es dann doch tun. Dies geht jedoch nur mit ausgewählten Handys.

Bedenke, dass Jailbreak Smartphones und gekaperte Handys aus der Ferne übernommen und zu einer Wanze umfunktioniert werden können. Das beinhaltet auch das Einschalten des vermeintlich ausgeschalteten Handys.

Benutze deswegen ein altes Anonymes-Handy. Da es zu nichts mehr als SMS empfangen bzw. Telefonieren genutzt werden soll, ist es ausreichend, Eins aus der oben genannten Liste zu benutzen. Damit könnt ihr zwar nicht verhindern geortet zu werden, zu wissen, dass man »aufmerksam« auf euch geworden ist, kann viel wert sein.

Um nicht enttarnt zu werden, halte dich immer an das folgende Verfahren:

- Nehme dein privates Handy nie zur "Arbeit" mit.

Bist du auf ein anonymes Handy angewiesen, folgt für dich:

- Benutze stets Handys, die du auf dem Flohmarkt oder im Second-Hand Handy Laden gekauft hast und diese nicht zu dir zurückgeführt werden können. Wahlweise kannst du auch neues Prepaid Handy, wie es z.B. Congstar anbietet, benutzen.
- Sobald dein Anonymes Handy nicht mehr gebraucht wird, schalte es aus.
- Benutze immer Preepaid Karten, die du anonym angemeldet hast. Die Anmeldung MUSS immer anonym stattfinden! Benutze dazu das Verfahren wie es im Punkt 4. (fast) Anonym durch VPN, Tor, JonDo & Co beschrieben wird.
- Nimm NIE deine AnonSim mit deiner Privaten gleichzeitig in Betrieb.
- Benutze nie deine AnonSim in der Nähe deines Wohnortes.
- Benutze immer ein Handy für einen bestimmten Job.
- Hast du mehrere Anonhandys, halte sie immer getrennt und benutze sie niemals gleichzeitig.

6.3 Messanger

Schnelle und sichere Kommunikation ohne Handy realisierst du am besten mit Messangern. Unten sind die Gängigsten aufgelistet.

6.3.1 Bitmessage

Bitmessage ist ein experimenteller Messanger, der noch mit einigen Schwierigkeiten zu kämpfen hat.
Es ist ein Verschlüsselungsprotokoll, das auf der Bitcoin-Technik basiert und einen vertraulichen und anonymen Austausch von Nachrichten in einem P2P-Netzwerk ermöglicht. Es gibt hier im Forum bereits eine sehr verständliche Anleitung von luckyspax, weswegen an dieser Stelle keine neue erstellt wird.

6.3.2 Torchat

Torchat ist ein einfacher Instant-Messenger, der dich anonym chatten lässt. Es muss nicht installiert werden und ist somit hervorragend für den Einsatz vom USB-Stick geeignet. Beim erstmaligen Start erstellt Torchat, eine eindeutige ID, anhand dieser jeder Benutzer eindeutig erkannt werden kann. Es schützt dennoch deine Anonymität, wie es Tor auch tut.

6.3.3 IRC

Internet Relay Chat (IRC) ist ein sehr beliebtes Chat-System. Es gibt eine Reihe verschiedener Client, mit denen du dich im Chat-System anmelden kannst. Pidgin ist eins davon. Da es nicht von sich aus verschlüsselt, muss du selber für deine Anonymität sorgen. Als Erstes sorgst du für die Anonymität und lässt es ausschließlich über Tor laufen. Als Nächstes installierst du in Pidgin, XChat oder irssi den Off-the-Record (OTR) Plug-In, das die privaten Gespräche, zwischen zwei Teilnehmern, absichert. Ohne diese Absicherungen ist es nicht ratsam, wie Sabu, aus der Anoymos Hacker-Gruppe LulzSec, erfahren musste, zu kommunizieren.

7. Sichere Hardware

7.1 Notebooks

Von Zuhause aus zu arbeiten, ist zwar bequem, aber leider auch riskant. Wie unter Punkt 4.5 Internetverbindung beschrieben wurde, kannst du leicht über fremde Zugänge deine Jobs erledigen. Wenn du nicht gerade einen Transporter mit ausgefeilter Hardware besitzt, greifst du am besten zu einem Notebook. Diese sind schon für wenige Euros zu haben und mit Win7 oder Linux relativ stabil und sicher zu betreiben.

Wenn du den Punkt 2.3 Identitäten erstellen ernst nimmst, wirst du verstehen, dass sie am besten dann gewährleistet ist, wenn du deine Jobs/Identitäten an unterschiedliche Hardware verteilst.

7.2 Handykontrolle

Der Umgang mit Handys wurde schon unter Punkt 6.2 Handykontrolle beschrieben. Der vollständigkeitshalber wird es hier nochmal kopiert.

Dein Handy verrät ständig, wo du bist. Anders ist die Funktionalität nicht gewährleistet. Und genau das machen sich die Strafverfolgungsbehörden zu Nutze. Haben Sie deine Handy- Nummer, können Abhöranfragen gestellt werden. In dem ersten Halbjahr 2014, wurden 704-mal Telekommunikationsüberwachungsmaßnahmen von der BKA durchgeführt. Des Weiteren hat BKA 35.000 und die Bundespolizei 69.000 Tracking-SMS versendet. Die Behörden rufen auch die Funkzellen zu einer bestimmten Zeit ab. Damit bekommen sie angezeigt, welche Handys zu einer gewissen Zeit an dieser Zelle und sich damit an diesem Ort befunden haben. In der ersten Jahreshälfte 2014 wurden diese Angaben 50-mal von der Bundespolizei, 3-mal von der BKA und 100-mal vom Zoll abgefragt. Anhand der IMEI Nummer, die mehr oder weniger einzigartig ist, kann man das Handy erkennen. Taucht die Nummer mehrmals in der Nähe des »Tatortes« auf, so ist das mehr als ein Indiz, dass sie damit zu tun hat. Konkretes Beispiel könnte das wiederholte, unsachgemäße Geldabheben sein. Auch wenn du dich verschleiert hast und die Cam des Bankautomaten kein verwendbares Foto von dir liefern kann, könnte man dich anhand der IMEI Nummer überführen. Hat man die IMEI Nummer, kann auch die derzeit eingesetzte SIM und die Handy Nr. ermittelt werden. Dadurch ist das Handy mit der Triangulation leicht zu orten. Da den Behörden untersagt ist Nutzer ständig zu triangulieren, versenden diese Stille-, Test- bzw. 0- SMS und erstellen somit ein Bewegungsmuster von dir. Normallerweise kann man mit deinen "Normalen" Handy keine 0-SMS anzeigen lassen. Mit einem Patch und einer Software, kann man es dann doch tun. Dies geht jedoch nur mit ausgewählten Handys. Bedenke, dass Jailbreak Smartphones und gekaperte Handys aus der Ferne übernommen und zu einer Wanze umfunktioniert werden können. Das beinhaltet auch das Einschalten des vermeintlich ausgeschalteten Handys. Benutze deswegen ein altes Anonymes-Handy. Da es zu nichts mehr als SMS empfangen bzw. Telefonieren genutzt werden soll, ist es ausreichend, Eins aus der oben genannten Liste zu benutzen. Damit könnt ihr zwar nicht verhindern geortet zu werden, zu wissen, dass man »aufmerksam« auf euch geworden ist, kann viel wert sein.

Um nicht enttarnt zu werden, halte dich immer an das folgende Verfahren:

- Nehme dein privates Handy nie zur "Arbeit" mit.

Bist du auf ein anonymes Handy angewiesen, folgt für dich:

- Benutze stets Handys, die du auf dem Flohmarkt oder im Second-Hand Handy Laden gekauft hast und diese nicht zu dir zurückgeführt werden können. Wahlweise kannst du auch neues Prepaid Handy, wie es z.B. Congstar anbietet, benutzen.
- Sobald dein Anonymes Handy nicht mehr gebraucht wird, schalte es aus.
- Benutze immer Preepaid Karten, die du anonym angemeldet hast. Die Anmeldung MUSS immer anonym stattfinden! Benutze dazu das Verfahren wie es im Punkt 4. (fast) Anonym durch VPN, Tor, JonDo & Co beschrieben wird.
- Nimm NIE deine AnonSim mit deiner Privaten gleichzeitig in Betrieb.
- Benutze nie deine AnonSim in der Nähe deines Wohnortes.
- Benutze immer ein Handy für einen bestimmten Job.
- Hast du mehrere Anonhandys, halte sie immer getrennt und benutze sie niemals gleichzeitig.

7.3 Mobiles Internet

Was für Handy gilt, gilt auch für die UMTS-Modems. Da sie eine IMEI-Nummer besitzen, können sie trianguliert und somit geortet werden. UMTS Modems gibt es als USB-Sticks oder PCMCIA-Karte.
Bei Fonic z.B. kannst du für 10€ eine Monats-Flat bekommen. Da die Karten meistens billiger zu haben sind (bei Media-Markt waren die für 5€ und bei dm für 8€ zu haben) hast du einen relativ günstigen und flexiblen Internet-Zugang.
Dabei gilt auch, dass du es nie in der Nähe deines Wohnortes verwenden darfst. Auch die zeitlich begrenzte Nutzung sollte klar sein. Auf Dauer kann diese Variante ein "Teurer" Spaß sein

8. Sichere Passwörter

Alles steht und fällt mit einem sicheren Passwort.
Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt:

- Es sollte mindestens zwölf Zeichen lang sein. (Ausnahme: bei Verschlüsselungsverfahren wie zum Beispiel WPA und WPA2 für WLAN sollte das Passwort mindestens 20 Zeichen lang sein. Hier sind so genannte Offline-Attacken möglich, die auch ohne stehende Netzverbindung funktionieren - das geht zum Beispiel beim Hacken von Online-Accounts nicht.)
- Es sollte aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern (?!%+...) bestehen. Tabu sind Namen von Familienmitgliedern, des Haustieres, des besten Freundes, des Lieblingsstars oder deren Geburtsdaten und so weiter.
- Wenn möglich sollte es nicht in Wörterbüchern vorkommen.
- Es soll nicht aus gängigen Varianten und Wiederholungs- oder Tastaturmustern bestehen, also nicht asdfgh oder 1234abcd und so weiter.
- Einfache Ziffern am Ende des Passwortes anzuhängen oder eines der üblichen Sonderzeichen $! ? #, am Anfang oder Ende eines ansonsten simplen Passwortes zu ergänzen ist auch nicht empfehlenswert.

Darüber nachgedacht, wie viele Passwörter du benötigst, vor allem wenn du mehrere Identitäten besitzt, erscheint es kaum machbar sich alle zu merken.
Sich alle Passwörter zu notieren wird nicht empfohlen, da einmal den Zettel verloren oder entwendet, kannst du nicht sicher sein, wer danach deine Accounts benutzt. Außerdem kommst du selber nicht mehr rein.
In den weiteren Unterpunkten werden einige Lösungen vorgestellt.

8.1 Zettelalgorithmus

Dass das Aufschreiben deiner Passwörter nicht ohne weiteres sicher ist, wurde oben erwähnt. Abhilfe kann da ein Algorithmus schaffen, mit deren Hilfe, du die Passwörter erstellst. Verlierst du den Zettel, kann keiner was damit anfangen und du kannst du einfach einen neuen Zettel erstellen, mit dem du deine Passwörter generierst.

Heise Verlag schrieb:
Papier-Generator
Schreiben Sie in jedes Feld ein bis drei zufällige Zeichen. Das geht leichter von der Hand, wenn Sie zum Beispiel Wörter oder Telefonnummern schreiben und nach jedem Zeichen zufällig die Zelle wechseln. Beachten Sie, dass Buchstaben wie Y in der deutschen Sprache seltener vorkommen als andere. Sorgen Sie also dafür, dass auch diese Kandidaten in Ihrer Tabelle vertreten sind. Um ein Passwort für eine Site abzulesen, benutzen Sie einfach die Domain: Bei ebay.de lesen Sie beispielsweise in der ersten Tabellenzeile die Zeichenfolge unter E ab, in der zweiten die unter B und so weiter. Bei langen Domains genügt es wahrscheinlich, wenn Sie die ersten fünf Buchstaben benutzen. Die übrigen Zeilen dienen als Reserve: Wenn Sie mal ein zweites oder drittes Passwort für einen bestimmten Dienst benötigen, starten Sie einfach eine Zeile tiefer. Um sicherzustellen, dass die erzeugten Kennwörter auch anspruchsvollen Passwort-Policies genügen, können Sie die Zelle der Tabellen jeweils mit einem Groß- und einem Kleinbuchstaben sowie einer Ziffer ausfüllen. Wenn Sie die Inhalte der Zellen dann auch noch mit einem Sonderzeichen wie dem Minus verbinden, enthält Ihr Passwort in jedem Fall alle Zeichenkategorien. Es hat sich bewährt, Groß und Kleinbuchstaben sowie Ziffern in verschiedenen Farben zu schreiben, weil man die drei Zeichenkategorien so besser auseinanderhalten kann. Da bei diesem Verfahren kein Geheimnis im Spiel

ist, können neugierige Mitmenschen die Passwörter ebenfalls von der Karte ablesen, wenn sie wissen, wo ihr Besitzer angemeldet ist.

Um das zu erschweren, können Sie zum Beispiel die Nummerierung der Zeilen weglassen und mit einer anderen Reihenfolge arbeiten, die nur Sie kennen. Wie auch bei dem zuvor vorgestellten System gilt: je individueller, desto sicherer.

8.2 Cloud Passwort-Manager

Passwörter kann man mit Programmen für den Mac oder Windows oder Apps für iOS verschlüsselt abspeichern. Dazu gibt es ein Haufen mehr oder weniger vertrauenswürdige Anbieter. 1Password ist wohl eins der bekanntesten. Es ist sehr komfortabel und für die meisten Devices vorhanden. Ob iOS oder Android, Mac oder Windows, mit einer Cloud schnell untereinander synchronisiert. Das Problem liegt jedoch auf der Hand: Sollte die Verschlüsselung geknackt werden, sind all die sicheren Accounts und Identitäten verbrannt. Deswegen ist der Gebrauch solcher Manager nicht für deinen Einsatz empfehlenswert. Vor allem auf einem Smartphone. Benutzt du es trotzdem, wirst du zusätzlich noch geortet werden können. Diese Überlegungen legen nahe, dass du deine Passwörter nie aus der Hand geben solltest.
Die Lösung der Password-Manager App, die die Passwörter für dich generiert und verwaltet, ist da weitaus eleganter.

8.3 Password Manager App

Diese App generiert anhand eines Master-Passworts und weiteren Angaben zum Account deiner Passwörter. Der riesen Vorteil ist, dass du dir jetzt nur noch ein sicheres Passwort merken musst. Die Sicherheit wird dadurch gewährleistet, dass die Passwörter für dich aus den Angaben zu der Seite, auf der du dich anmelden willst, und den Master-Passwort generiert werden. Kannst du die beiden Angaben, lässt du sie dir auf einem Mac, Linux, Windows oder aber auch auf mobilen Geräten errechnen. So lässt du deine Passwörter nirgends liegen, wo man sie klauen oder mit einem Richterbeschluss beschaffen kann. Der Nachteil davon ist, dass sich jeder deine Passwörter generieren lassen kann, der dein Masterpasswort und die Account-Seiten kennt. Welcher der vorgestellten Methoden du benutzt, ist dir überlassen. Jede hat ihre Vor- und Nachteile. Bei jeder solltest du darauf achten, dass sie von Dritten nicht erraten werden kann.

Nachtrag 03.09.2014: Am 28.08.2014 hat CCC ein Podcast CR204 Passwörter veröffentlicht.

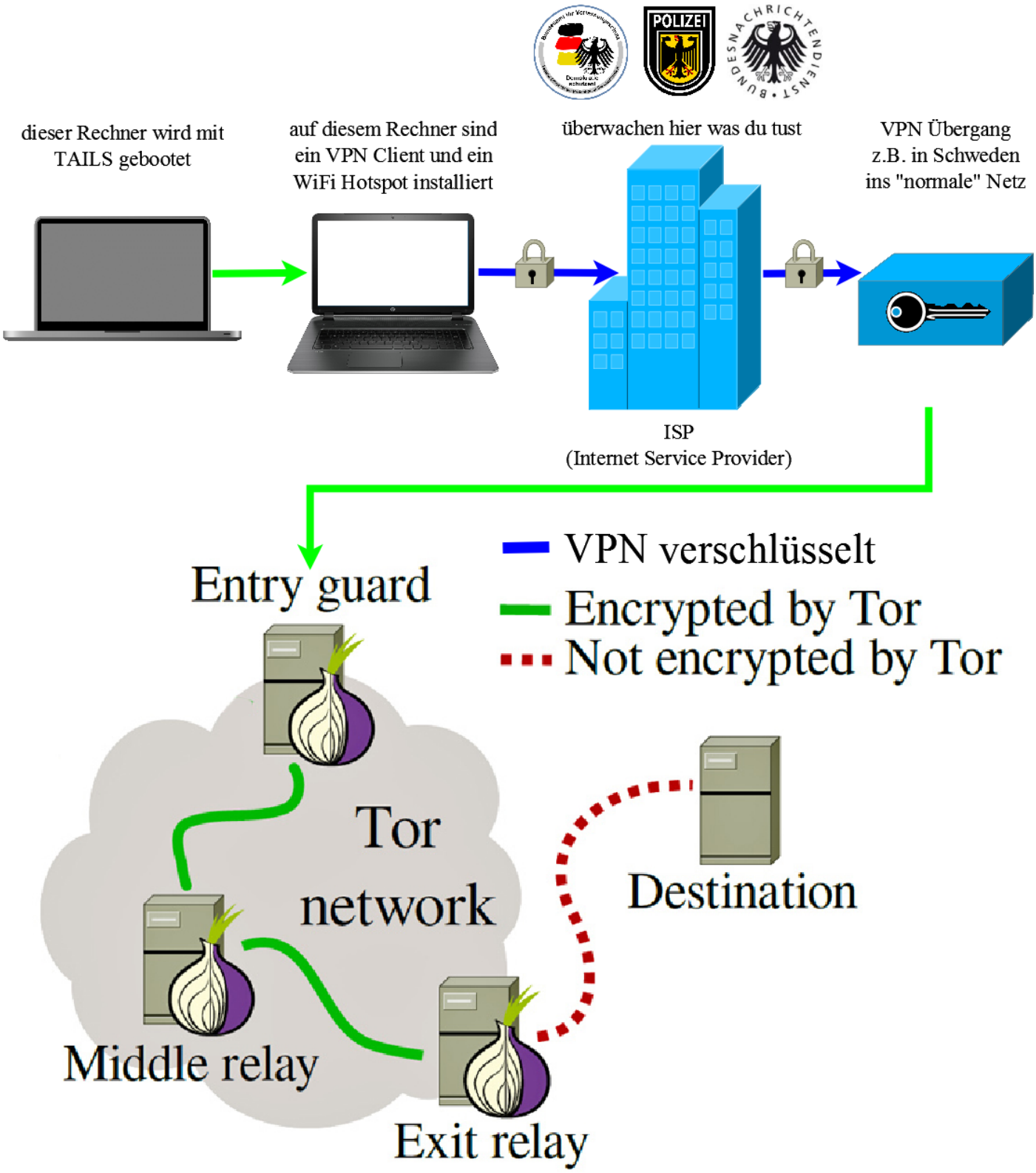
Hier wurde bereits die „Anleitung von Capulcu zur Nutzung des Tails-Live-Betriebssystems für sichere Kommunikation, Recherche, Bearbeitung und Veröffentlichung sensibler Dokumente“ in der Fassung „4. überarbeitete Auflage | April 2017“ veröffentlich. Da ich den Link zu dem Beitrag nicht mehr habe, habe ich die Anleitung nochmal beigefügt.

Dann gab es da noch „Anonym im Internet mit Tor und Tails“. Doch auch dieses Buch stammt aus dem Jahr 2015, ist inhaltlich immer noch richtig aber nicht auf dem neusten Stand.

An dieser Stelle gleich ein Tipp. Es ist durchaus sinnvoll sich z.B. mit dem USB Image Tool mehr oder weniger regelmäßig ein aktuelles Image von seinem Stick anfertigt, denn auch die besten Sticks können kapput gehen oder man verliert ihn. Auch wenn die Daten im persistent volume sicher sind, kann der Verlust / die Beschädigung des Sticks ziemlich ärgerlich sein und man ist froh, wenn man dann auf ein Image zurückgreifen kann.

Wer weitestgehend sicher sein will, dass es den Überwachern nicht so leicht fällt festzustellen wo und was der Nutzer tut kombiniert Tails mit einem VPN. Ich bin nicht der Einzige der zu solchen Mitteln greift / rät, denn im Deepweb gibt es ebenfalls Anleitungen wie „COMBINING TOR WITH A VPN“

Da das für weniger erfahrene Anwender jedoch nicht ganz leicht ist und man Tails normalerweise nicht verändern sollte erkläre ich an dieser Stelle wie man das mit einem 2. Notebook realisiert bekommt. Eine schematische Darstellung seht ihr im Bild **TOR durch VPN**.



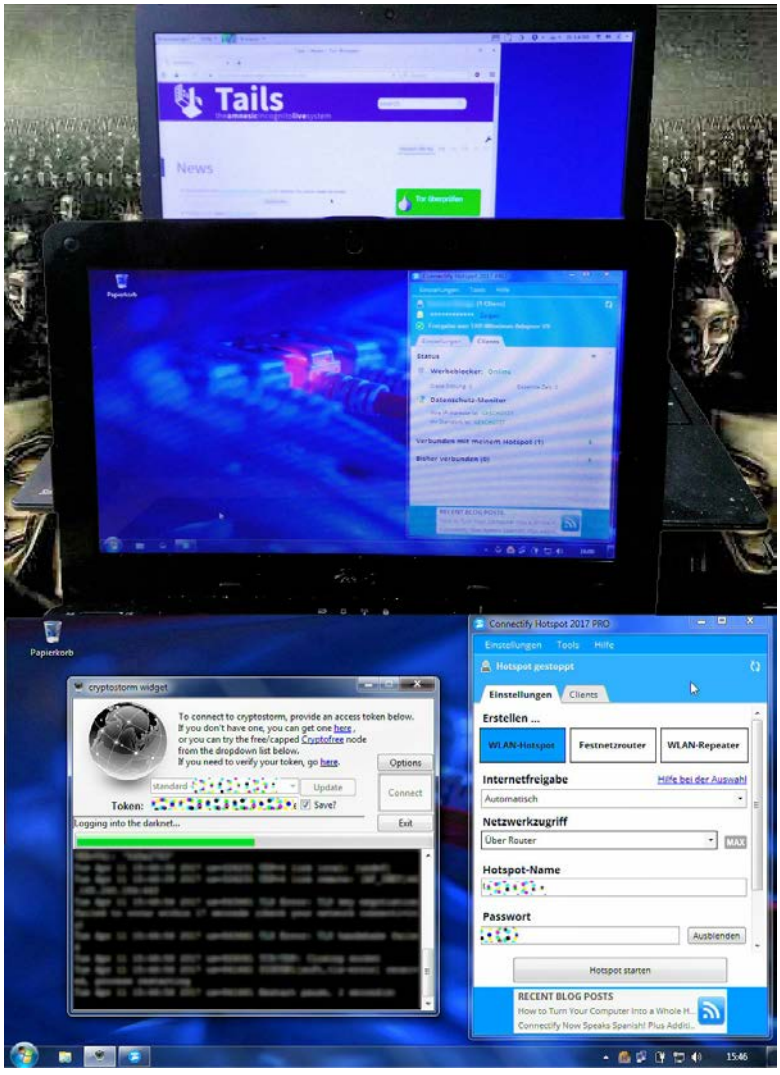
Rechner 1 ist der normale Rechner den man mit einem TAILS USB Stick / einer TAILS DVD bootet. Auf dem Rechner 2 ist ein ziemlich nacktes Windows 7 Home Premium installiert, dass nur mir dem **Simplix Pack to update Live Win7 System** erweitert wurde (enthält nur Security Updates), dass man hier auf der russischen Originalseite oder hier bei My Digital Life (nur nach Anmeldung) bekommt. Nachdem die Updates installiert sind kommt ein enorm wichtiger Punkt, denn man sollte das Internet niemals und unter keinen Umständen als Administrator nutzen, weshalb man in der Benutzerkontensteuerung einen „normalen“ Benutzer einrichtet (der eingeschränkte Rechte hat, nichts installieren kann). Jetzt installiert man die restliche Software als Admin. Man installiert zusätzlich ist einen VPN Client und eine WiFi Hotspot Software (Freeware). Um das Ganze vor Angriffen zu schützen habe ich Microsoft EMET installiert über das man hier und hier mehr Informationen findet. EMET nimmt einige zu schützende Dateien

automatisch auf. Um auf der sicheren Seite zu sein nimmt man (wenn der Rechner fertig installiert ist) alle Exe Dateien die Internet Kontakt haben zusätzlich auf was ich in einer kurzen Anleitung (in der Anlage) erklärt habe . Hier bei Heise gibt es noch einen deutschsprachigen Artikel über die Funktion von EMET. Von irgendeiner Antiviren Software sollte man auf diesen Rechner die Finger lassen, denn 1. surft man mit dem Rechner ja nicht und 2. stellt AV Software keinen wirklichen Schutz dar, verleitet nur zum leichtsinnigen (hirnlosen) rumklicken. Das EMET Userguide kann hier als PDF heruntergeladen werden. Wer noch etwas mehr tun will kann sich Windwos Firewall Controll von BiniSoft installieren, bei der es sich eigentlich nur um eine kompfortable GUI für die zwar gute, aber umständlich zu bedienende Windows Firewall handelt. Eine quasi Anleitung was man wie einstellen sollte findet man unter dem Titel Windows Firewall Configuration - Truly Block EVERYTHING... ebenfalls be My Digital Life.

Dann läd man sich hier noch das Freeware Tool Spybot Anti-Beacon herunter mit dem man den größten Teil der Schnüffelfunktion von Windows abstellen lassen. Keine Sorge damit kann man nichts falsch machen denn es gibt für jede Option eine „Undo“ Funktion falls wieder Erwarten an irgend einer Stelle Probleme auftreten sollten.

Ganz zum Schluss sollte man für den Fall der Fälle nachdem alles getested ist und läuft ein Imgae machen, damit man im Schadensfall nicht die ganze Arbeit neu machen muss. Hier eignet sich die Freeware Version von Macrium gut.

Für diesen 2. Bridge Rechner kann man nahezu jedes Notebook / Netbook nehmen. Ich habe einen uralten ASUS Eee PC verwendet, der unrsächlich mit XP lief und auf dem Win 7 überhaupt erst nach einem Bios Update installiert werden konnte. Das das Ganze funktioniert (selbst mit einem WiFi Netzzugang) kann man auf diesem Bild sehen.



Der einzige Unterschied ist, dass bei mir eine gekaufte Hotspot Software läuft da sie bereits verhanden war. Hat der 2. Rechner seinen ersten Funktionstest bestanden, muss nichts mehr geändert werden, sollte man den Rechner unbedingt mit Veracrypt voll verschlüsseln (falls man in Abwesenheit Besuch bekommt, der einem vielleicht den Staatstrojaner unterjubeln will).

Wenn man will kann man sich ein Crossover Netzwerkkabel kaufen um Rechner 1 mit Rechner 2 zu verbinden (auch W-Lan Verbindungen (Rechner 1 mit 2) können geknackt und abgehört werden, auch wenn die Gefahr nicht sehr groß ist da man solche Aktionen eh nie vom eigenen Anschluss machen darf. Was die Wahl des VPN Anbieters betrifft rate ich dazu sich den VPN Bereich

> **Global Mass Surveillance - The Fourteen Eyes**
> The UKUSA Agreement is an agreement between the United Kingdom, United States, Australia, Canada, and New Zealand to cooperatively collect, analyze, and share intelligence. Members of this group, known as the Five Eyes, focus on gathering and analyzing intelligence from different parts of the world. While Five Eyes countries have agreed to not spy on each other as adversaries, leaks by Snowden have revealed that some Five Eyes members monitor each other's citizens and share intelligence to avoid breaking domestic laws that prohibit them from spying on their own citizens. The Five Eyes alliance also cooperates with groups of third party countries to share intelligence (forming the Nine Eyes and Fourteen Eyes), however Five Eyes and third party countries can and do spy on each other.

der Seite privacytools.io aufmerksam durchzulesen und sich für einen der dort genannten Anbieter zu entscheiden, denn wirkliche Sicherheit in diesem Bereich gibt es nicht kostenlos und die paar vertrauenswürdigen freien VPN's die es gibt sind noch langsamer als kommerzielle Anbieter. Ein weiter Vorteil der dort aufgelisteten VPN Provider ist „All providers listed here are outside the US, use encryption, accept Bitcoin, support OpenVPN and have a no logging policy." Am Ende des VPN Bereichs findet man sehr viele weiterführende Links zum Thema VPN.

Wie das Ganze nun funktioniert ist ziemlich einfach erklärt. Man geht mit Rechner 2 ins Netz und startet den VPN Client und baut so einen verschlüsselten Tunnel z.B. nach Schweden auf (geht dort also erst ins Netz). Dann startet man die Hotspot Software Baidu (die unter den freien Varianten als die beste gilt). Nun bootet man Rechner 1 mit seiner Tails Version. Ist Tails hochgefahren connected man Tails mit dem Baidu Hotspot wodurch Tails erst mal durch den verschlüsselten Tunnel geht um sich (um bei dem Bespiel zu bleiben) von Schweden aus den ersten TOR Knoten sucht. Wer sich nun fragt was das Ganze soll – 1. sehen weder der Internetprovider noch irgend welche Überwacher, dass man TOR verwendet denn der VPN Tunnel ist ja verschlüsselt und 2. wird es selbst bei einer aufwändigen Überwachung der Zielseite und deren Nutzer nahezu unmöglich die echte IP des Zugreifenden herauszufinden, wenn man keine Fehler macht wie sich in eindeutig zuzuordnenden Accounts mit dieser Verbindung einzuloggen.

Wer keine saubere Windows ISO hat kann sich diese direkt von MS mit dem Microsoft Windows ISO Download Tool herunterladen. Aktivieren kann man so ein Windows dann mit dem Reload Acitvator

Wer sich keinen VPN leisten kann / will kann z.B. hier oder hier z.B. nach „Hotspot Shield VPN" oder CyberGhost" suchen. Die beiden Clients habe ich deswegen genannt, weil CyberGhost seinen Sitz in Rumänien und der Anbieter von Hotspot Shield in Kanada und der Schweiz hat. Letzteres ist zwar keineswegs genial aber es gibt ja immer noch die TOR Verschlüsselung. **Keinesfalls darf man irgendeinen VPN Anbieter verwenden, der einen Sitz in Deutschland hat, denn in so einem Fall kann dieser mittels Richterbeschluss gezwungen werden zu loggen.**

Links für Leute die **die Gefahr** nicht sehen wollen

Predictive Policing: Die deutsche Polizei zwischen Cyber-CSI und Minority Report

EU-Kommission treibt Informationsaustausch zwischen Polizei und Geheimdiensten voran

Bundesverfassungsgericht: Vorratsdatenspeicherung bleibt erstmal in Kraft, bis zum endgültigen Urteil

Noch vor der Bundestagswahl: Staatstrojaner soll auch gegen Alltagskriminalität eingesetzt werden

Jeder Mensch in Schleswig-Holstein gerät jedes Quartal in eine Funkzellenabfrage

Bundeskriminalamt möchte Handy-Ortung mit IMSI-Catchern ausbauen

Staatliche Überwachung: Abhören, Orten, Ausspionieren und Bespitzeln

Studie des Europaparlaments: Staatstrojaner bergen erhebliche Risiken für das Grundrecht auf Privatsphäre

Der BND spioniert am größten Internetknoten der Welt (De-Cix Frankfurt)

BND soll Interpol ausgespäht haben