Computer, Internet, Handy -

Was bedeuten Snowdens Enthüllungen für eine widerständige Praxis?

Bild- und Textverarbeitung, Internetrecherche und -veröffentlichungen, Mails und Instant Messaging, Handykommunikation und sogar Smartphones und sogenannte soziale Netzwerke... All dies spielt auch in der politischen Arbeit und im Alltag vieler Aktivist_innen eine große Rolle. Nun konnten wir in den letzten Monaten, dank immer neuer Enthüllungen des ehemaligen Mitarbeiters der National Security Agency (NSA) Edward Snowden, viel über die Arbeitsweise von Geheimdiensten lernen. Dieser Text versucht eine Einschätzung der Enthüllungen bzw. ihrer Bedeutung für die Praxis und den Alltag derjenigen, die sich nicht konform verhalten. Wir wollen einen groben Überblick über die aktuellen Enthüllungen und ältere Erkenntnisse zum Stand technischer Überwachungsmaßnahmen geben. Dabei versuchen wir den Spagat zwischen dem Anspruch eine praktische Hilfestellung zu formulieren und so weit wie möglich auf technische Details zu verzichten. Konkret geht es um die Fragen: Was bedeuten die Snowden-Enthüllungen für Computer-, Internet- und Handynutzung? Welche Risiken beinhalten die einzelnen Nutzungsmöglichkeiten und welchen Schutz gewähren z.B. die Nutzung von TOR zur Verschleierung der Identität oder die Verschlüsselung von Mails und Daten? Wir versuchen verständliche Einschätzungen zu den einzelnen Bereichen und Tipps für eine sicherere Nutzung abzugeben. Denn jede_r, der_die diese Technologien nutzt, sollte zumindest die Risiken für sich und andere kennen, um entscheiden zu können ob sie in kauf zu nehmen sind.

Eins noch vorweg: Trotz allem Gezeter deutscher/ europäischer Politiker_innen über das Abhören von Merkels Handy, arbeiten die verschiedenen Geheimdienste gut zusammen. Z.B. stellt die NSA das wohl wichtigste Programm zur Überwachung des Internets XKeystore, auch Verfassungsschutz (VS) und Bundesnachrichtendienst (BND) zu Verfügung. Es ist also davon auszugehen, dass das Level an Überwachung auch in Zukunft zunimmt und von allen Diensten je nach Situation mal gemeinsam und mal in Konkurrenz zueinander vorangetrieben wird. Debatten um Datenschutzrichtlinien sind Scheingefechte. So ist die ganze Debatte über Vorratsdatenspeicherung, wenn überhaupt, nur noch für die juristische Verwendung der gewonnenen Daten relevant. Wir müssen immer davon ausgehen, dass das, was technisch möglich ist, auch eingesetzt wird.

Wie wird überwacht?

Von verdachtsunabhängiger und gezielter Überwachung

Es macht Sinn zwischen zwei Arten der Überwachung zu unterscheiden. Die erste ist die umfassende, verdachtsunabhängige, die Alle betrifft. Sie dient einerseits der Erstellung von Lagebildern, der Einschätzung politischer Stimmungen in der Bevölkerung und der Prognose von gesellschaftlichen Entwicklungen. Andererseits liefert sie, neben weiteren Erkenntnissen aus polizeilichen und geheimdienstlichen Tätigkeiten, die Grundlage für die zweite Art der Überwachung, die sich gezielt gegen einzelne Personen, Gruppen, Homepages und Internetzugänge richtet. Aus einer emanzipatorischen Perspektive sind beide Arten der Überwachung eine Bedrohung.

Während die verdachtsunabhängige Überwachung gesellschaftliche Entwicklungen vorhersehen und langfristige Strategien der Herrschaftsabsicherung ermöglichen soll, dient die gezielte Überwachung der direkten Repression gegen Nicht-Konforme. Wir erwähnen das so explizit, da wir den Eindruck haben, dass auch linke Zusammenhänge die Bedeutung der verdachtsunabhängigen Überwachung unterschätzen. Als Beispiel dafür sei angeführt, dass die Nutzung von sog. sozialen Netzwerken und (Mobil-)Telefonen oft nur dann als Problem angesehen wird, wenn über strafrechtlich Relevantes gequatscht würde. Diese Sichtweise unterschätzt das staatliche und immer mehr auch kommerzielle Interesse an „privaten“ Daten. Denn sie vernachlässigt sie die mittel- und langfristige Wirkung staatlicher Allwissenheit, sowie die daraus resultierende Fähigkeit, Prognosen für zukünftige gesellschaftliche Entwicklungen abzugeben. Hinzu kommt, dass die Übergänge, zwischen den beiden Arten der Überwachung, sowieso fließend sind und die_der Einzelne nie wissen kann ob ihr_sein Status gerade die Basisversion der Überwachung oder ein Upgrade auf noch umfassendere Durchleuchtung rechtfertigt.

Totale Überwachung gegen Alle

Vieles von dem, was auch wir vor den Enthüllungen nicht für möglich gehalten haben, ist offensichtlich längst Realität. Sowohl die Masse der Daten, die gespeichert werden können, als auch die Möglichkeiten sie automatisiert aus-

zuwerten, sind weit größer als wir dachten. Niemand sollte noch davon ausgehen, dass er_sie nicht wichtig genug ist, um unter Beobachtung zu stehen. Große Teile der Überwachung laufen ununterbrochen automatisiert ab. Erst bei speziellem Interesse ist es nötig, zusätzliche menschliche Kapazitäten aufzubringen.

Wir gehen davon aus, dass die sogenannten Metadaten elektronischer Kommunikation sowieso für immer gespeichert bleiben. So wurde z.B. berichtet, dass die Metadaten aller Anrufe innerhalb der USA, seit den 1980ern bis heute, gespeichert sind. Das heißt, wer wen wann und wie lange anruft, bleibt ebenso gespeichert, wie wer wem wann eine e-Mail oder Nachricht über ein sog. soziales Netzwerk schreibt. Auch jede Überweisung oder Kartenzahlung wird erfasst. Ebenso wird jeder Brief fotografiert und Absender_in, Empfänger_in und Datum werden gespeichert.

Über diese Metadaten hinaus, sind für diese Art der Überwachung, die sich verdachtsunabhängig gegen alle richtet, auch Formen der automatisierten inhaltlichen Auswertung bekannt. Technisch ist es durchaus möglich SMS, Mails und auch Telefonate nach Stichwörtern zu durchsuchen. Sprach-Software ist seit langem so weit auch gesprochene Stichwörter zu finden und Sprecher_innen eindeutig wiederzuerkennen.
Im Bezug aufs Internet verdeutlichen Snowdens Enthüllungen im besonderen Maße welche Qualität die automatisierte Überwachung hat. So ist es offenbar möglich, Komplettkopien des Internet-Traffics mit allen Inhalten zu erstellten. Unklar ist dabei, ob dies nur für einige besonders interessante Staaten/Bereiche gilt und wie lange diese vollständige Aufzeichnungen des Datenverkehrs gespeichert werden kann. Allerdings können Suchaufträge formuliert werden und damit sozusagen bestimmte Teile aus dem gesamten Internet-Traffic herausgefiltert und beliebig lange gespeichert werden. In einer vom Guardian veröffentlichten NSA-Präsentation steht wörtlich „Wir sind dabei das Internet zu beherrschen“ („to ‚master‘ the internet“). Um zu verdeutlichen, dass dies durchaus nicht zu großkotzig, sondern eine realistische Selbsteinschätzung ist, werden wir zunächst die Möglichkeiten des wohl wichtigsten Programms XKeystore erläutern.

XKeystore – Das Werkzeug, das die Totalüberwachung des Internets spezifiziert

Alle Zitate im folgenden Absatz stammen aus NSA-Präsentations-Folien zum Programm XKeystore. Dort wird die Frage „Was kann gespeichert werden?“ mit „Alles, was Sie extrahieren wollen.“ beantwortet. Dieser Datenstrom kann in Echtzeit nach „abweichenden Ereignissen“ durchsucht werden. So können Verdächtige, die bislang unbekannt waren, ausfindig gemacht werden. Interessant ist z.B. „jemand, dessen Sprache deplaziert an dem Ort ist, wo er sich aufhält“, „jemand, der Verschlüsselungstechnik nutzt“, „jemand, der im Web nach verdächtigen Inhalten sucht“ oder sie weiter verbreitet. Das Programm ermöglicht es, **Inhalte digitaler Kommunikation** nach sogenannten starken Suchkriterien zu durchsuchen (zum Beispiel einer konkreten E-Mail-Adresse oder bestimmten Stichwörtern), aber auch nach „weichen Kriterien“ (etwa der benutzten Sprache oder einem bestimmten Such-String). Das System erlaubt zudem die Erfassung von **„Ziel-Aktivität in Echtzeit“** also live und bietet einen „durchlaufenden Pufferspeicher“, der „ALLE ungefilterten Daten“ umfasst, die das System erreichen.

Ein paar konkrete Beispiele für Abfragen aus der Präsentation:

- „Zeige mir alle verschlüsselten Word-Dokumente im Iran.“

- „Zeige mir die gesamte PGP-Nutzung im Iran.“ PGP ist ein System zur Verschlüsselung von E-Mails und anderen Dokumenten.

- „Zeige mir alle Microsoft-Excel-Tabellen, mit MAC-Adressen aus dem Irak, so dass ich Netzwerke kartieren kann.“ MAC-Adressen gehören zu Netzwerkkarten, so lassen sich die genutzten Endgeräte identifizieren.

Weitere Beispiele für das, was XKeyscore aus dem Traffic fischen und noch leisten kann:

- von welchen IP-Adressen beliebige Websites aufgerufen worden sind

- Telefonnummern, E-Mail-Adressen, Logins Nutzer_innennamen, Kontaktlisten, Adressbücher, Cookies in Verbindung mit Webmail und Chats

- Google-Suchanfragen samt IP-Adresse, Sprache und benutztem Browser

- jeden Aufbau einer verschlüsselten VPN-Verbindung (zur „Entschlüsselung und zum Entdecken der Nutzer“)

- Aufspüren von Nutzer_innen, die online eine in der Region ungewöhnliche Sprache nutzen (als Beispiel genannt wird Deutsch in Pakistan)

- Suchanfragen nach bestimmten Orten auf Google Maps und darüber hinaus alle weiteren Suchanfragen dieses_dieser Nutzer_in sowie ihre_seine E-Mail-Adresse

- Zurückverfolgen eines bestimmten online weitergereichten Dokuments zur Quelle

- alle online übertragenen Dokumente, in denen zum Beispiel „Osama bin Laden“, „IAEO“ oder beliebige andere Stichwörter vorkommen, und zwar auch auf „Arabisch und Chinesisch“

Gezielte Überwachung gegen einige

Ergibt diese verdachtsunabhängige Überwachung oder Erkenntnisse aus anderen Quellen etwas Interessantes, werden gezielter weitere Maßnahmen ergriffen. Mit wenigen Klicks „ist die Zielperson für elektronische Überwachung markiert, und **der Analyst kann sich die Inhalte ihrer Kommunikation ansehen**“. Für „gängige Dateiformate“ hält XKeyscore zudem Betrachtungssoftware bereit, so dass der_die Analyst_in

das System nicht verlassen muss, um sich E-Mails oder andere Inhalte direkt anzusehen. Außerdem heißt es in einer Folie der Präsentation, man könnte über XKeyscore eine Liste aller angreifbaren Rechner und Telekom-Infrastrukturen in einem Staat aufrufen. Diese Datenbank von Schwachstellen auf Computersystemen weltweit könnte u.a. dazu dienen interessante Rechner, Router usw. mit weiterer Spionagesoftware zu infizieren um z.B. Passwörter für Verschlüsselungen und offline gespeicherte Informationen abzugreifen.

Bruce Schneiers, der mit dem Guardian Snowdens Enthüllungen auswertet, schreibt dazu folgendes (gekürzt):

„Es handelt sich hierbei um riesige Datenmengen, doch die NSA hat entsprechend starke Fähigkeiten, diese auf interessanten Datenverkehr hin schnell zu durchsuchen. Jedes individuelle Problem - die Gewinnung elektronischer Signale aus Glasfaserkabeln, das Schritthalten mit den Terabyte-großen Datenströmen, während sie entstehen, das Herausfiltern der interessanten Sachen - hat eine eigene Arbeitsgruppe, die sich mit seiner Lösung beschäftigt. Das Ausmaß ist global. [...]

Die NSA attackiert auch direkt die Netzwerkgeräte: Router, Switches, Firewalls, usw. Die meisten dieser Geräte haben bereits Überwachungskapazitäten von den Herstellern eingebaut bekommen und der Trick ist nur, sie heimlich anzuschalten. Es handelt sich hier um eine besonders vielversprechende Methode; Router werden viel seltener mit Updates versehen oder durch Sicherheitssoftware geschützt, und sind eine allgemein ignorierte Schwachstelle. [...]

Die NSA wendet bei speziellem Interesse außerdem beträchtliche Ressourcen für das Angreifen von individuellen Computern auf. Diese Angriffe werden von der „Tailored Access Operations"-Gruppe (TAO) durchgeführt. Die TAO kennt eine Anzahl von Schwachstellen, über die sie gegen eure Computer vorgehen kann - völlig egal, ob ihr Windows, Mac OS, Linux, iOS oder irgendetwas anderes benutzt. Eure Anti-Virenprogramme werden nicht anschlagen und ihr hättet Probleme, diese Schwachstellen zu entdecken, selbst wenn ihr wüsstet, wonach ihr suchen müsst. Die NSA nutzt Hackertools, welche von Hackern entwickelt wurden und das mit einem im Grunde unbegrenzten Budget. Wenn ich vom Lesen der Snowdendokumente etwas mitbekommen habe, dann das: ***Wenn die NSA in eure Computer will, dann schafft sie das. Punkt.*** *[...]*

Geht immer davon aus, dass euer Rechner von der NSA kompromittiert werden kann. Wenn ihr etwas wirklich wichtiges habt, nutzt ein „Luftloch". Seit ich angefangen habe mit den Snowdendokumenten zu arbeiten, habe ich einen neuen PC gekauft, der niemals Zugang zum Internet hatte. Wenn ich eine Datei versenden will, verschlüssele ich sie auf dem sicheren Computer und laufe dann mit einem USB-Stick zu meinem internetfähigen Rechner. Will ich etwas entschlüsseln, drehe ich diese Prozess um. Das ist nicht todsicher, aber es ist ziemlich gut."

Was bedeutet das für die einzelnen Nutzungsmöglichkeiten?

Zunächst sollte jede_r wissen, wobei, wann und wo Daten erhoben und gespeichert werden. Auch der zweite Schritt sollte eigentlich unstrittig sein: Datenspuren müssen wann immer möglich vermieden werden! In der Praxis ist dieser Punkt dann vermutlich leider doch strittig, denn er beinhaltet, dass einige Nutzungsmöglichkeiten ausgeschlossen werden müssen und andere nur mit mehr Aufwand zu realisieren sind. Denn wer ein Smartphone oder sog. soziale Netzwerke nutzt, unverschlüsselte Mails verschickt oder ohne TOR im Internet surft, liefert immer eine riesige Menge an Daten. Doch auch wer sich um Schutzmaßnahmen bemüht, muss auf einiges achten, um sich nicht in falscher Sicherheit zu wiegen und Anhaltspunkte für weiterreichende Überwachung zu schaffen.

Computer sicher nutzen?!

Wir kommen zu dem selben Schluss wie Bruce Schneiers in dem vorangestellten Zitat: Es gibt für die vielen spezifischen Nutzungen von Computern keine generellen Lösungen. Für unterschiedliche Nutzungen und unterschiedliche Sicherheitsbedürfnisse, braucht es unterschiedliche Computer. Die Frage, wann was sicher ist, lässt sich nicht allgemein beantworten. Denn nicht nur die Art der Nutzung muss berücksichtigt werden, sondern auch welcher Rechner von wo benutzt wird. Z.B. ist zur Beantwortung der Frage, ob eine Verschlüsselung sicher ist, nicht nur die Art der Verschlüsselung und das Passwort entscheidend, sondern auch, ob der Computer, den du nutzt, unter deiner Kontrolle ist (das heißt, dass niemand sonst Zugang zu ihm bekommen kann). Dies gilt auch für andere Nutzungsmöglichkeiten. Ein weiteres Beispiel: Selbst wenn man davon ausgehen würde, dass TOR deine Identität im Internet unangreifbar verschleiert, hilft dir das nicht, wenn dein personifiziertes Endgerät mit Spionage Software infiziert ist. Das gleiche gilt für Rechner und Router in linken Szeneläden, Hausprojekten oder im Internetcafé, das vielleicht auch schon mal von irgendwem anders, der _die von Interesse ist, genutzt wurde. Denkbar wären dann z.B. das Mitlesen aller Tastatureingaben oder die regelmäßige Übermittlung von Bildschirmfotos.

Diese Vielzahl von Variablen ergibt so viele unterschiedliche Angriffsmöglichkeiten, dass es für eine sichere Nutzung nur individuelle Lösungen geben kann. Das heißt wiederum, dass wir an dieser Stelle nur auf potentielle Fallstricke bei dem Versuch sich abzusichern hinweisen und Tipps geben können, wie sie auszuschließen sind. Denn wenn wir auf alle Eventualitäten eingehen und für alle genannten Programme und Praktiken ausführliche Anleitungen schreiben wollten, würde unser Text eher den Umfang eines Buches annehmen. Stattdessen geben wir im Anhang Tipps, wo nähere Infos und ausführliche Anleitungen zu finden sind. Wer wert auf Sicherheit legt, kommt nicht drum-

herum, sich bei jeder Nutzungsmöglichkeit, selbst zu überlegen wie schutzbedürftig sie ist und sich letztlich auch mit technischen Details der einzelnen Soft- und Hardwarekomponenten auseinanderzusetzen. Dass dies einige Abschrecken wird, wissen wir, aber für eine realistische Einschätzung der Situation müssen wir das so klar sagen.

Offline arbeiten

Wer auf Computer nicht verzichten kann und jede potentielle Angriffsmöglichkeit ausschließen will, muss ihn vor jedem möglichen Zugriff schützen. Jeder Computer der jemals am Internet war, kann demnach nicht mehr als 100% sicher angesehen werden. Auch sonst musst der Rechner permanent unter deiner Kontrolle sein. Also darf es keine Möglichkeit geben, mal eben unbemerkt fremde Hardware einzubauen oder mit einem USB-Stick Software zu installieren. Eine Komplettverschlüsselung der Festplatte, sodass das Betriebssystem nur nach Passworteingabe und Entschlüsselung hochfährt, minimiert das Risiko der heimlichen Manipulation und des Auslesens der Daten, wenn der Computer z.B. bei einer Hausdurchsuchung mitgenommen wird (siehe Absatz zu Verschlüsselung).

Wer nicht will, dass ihre_seine Texte oder was auch immer bekannt werden, muss sich also einen Rechner besorgen, der nicht ans Internet geht. Sehr praktisch sind auch Live-Betriebssysteme (wie z.B. TAILS), die sich von USB-Stick oder CD starten lassen und schon viele gängige Programme integriert haben. So kannst du den Rechner auch ganz ohne Festplatte nutzen und nur das Betriebssystem laufen lassen. Dies macht auch Sinn für einen (anderen) Rechner, den du fürs Internet benutzt. (siehe Absatz: zu Internetnutzung)

Doch auch dabei gibt es Fallstricke. Denn auch ein Betriebssystem musst du in der Regel aus dem Internet herunter laden, um es auf einem Stick zu installieren oder auf eine CD zu brennen. Die Probleme ergeben sich also eigentlich aus der Internetnutzung. Da du sie aber auch beachten solltest, um ein Betriebssystem für deinen offline Rechner zu bekommen, erklären wir sie kurz an dieser Stelle.

1. Von einer vertrauenswürdigen Seite runter laden und wenn möglich OPEN-PGP-Signaturen vergleichen. So stellst du sicher, dass das, was du heruntergeladen hast, auch das ist, was du haben wolltest und nicht ausgetauscht wurde. Das OPEN-PGP-Protokoll wird mittlerweile von vielen Produkten unterstützt. Empfehlenswert ist das Open-Source-Programm GnuPG, das zum Verschlüsseln von Mails, Instant Messaging, Daten und eben zum Vergleich von Signaturen verwendet werden kann.

2. Mit einem USB-Stick nicht in beide Richtungen arbeiten. Also einen neuen Stick besorgen, Programm/Betriebssystem runter laden, auf deinem „sicheren“ Rechner installieren bzw. laufen lassen und danach den Stick nicht erneut an anderen Rechnern verwenden. Oder ein Betriebssystem auf CD brennen und deinen Rechner nur davon laufen lassen. Dies erhöht die Sicherheit, da auf einer CD im Gegensatz zu einem USB-Stick nicht im Nachhinein gespeichert werden kann, also auch nichts manipuliert werden kann. Andererseits ist es unkomfortabler, da du selbst auch keine Änderungen vornehmen oder neuen Programme installieren kannst und für jedes Update eine neue CD brennen musst.

Verschlüsselung? Aber sicher!

Snowden erklärte in einer Onlinefragestunde für Guardianleser_innen, kurz nachdem er die ersten Dokumente enthüllt hatte: „Verschlüsselung funktioniert. Richtig implementierte, starke Kryptosysteme sind eines der wenigen Dinge, auf die man sich verlassen kann. Unglücklicherweise ist die Sicherheit am Endpunkt so erschreckend schwach, dass die NSA regelmäßig Wege darum herum findet.“

Der Endpunkt bezeichnet die Software, die du benutzt, den Computer, auf dem du sie benutzt und das lokale Netzwerk, in dem du das tust. Wenn Geheimdienste Verschlüsselungsalgorithmen verändern können oder einen Trojaner auf deinem Rechner installieren, ist die beste Kryptographie nichts mehr wert. Wenn du sicher sein willst, musst du dein Bestes geben, damit die Verschlüsselungsprogramme auf deinem Rechner unbeeinflusst arbeiten können. Da sind wir wieder an dem Punkt, dass Verschlüsselung nur auf einem Computer, der vor jedem direktem Zugriff geschützt ist und nie am Internet war, vertrauenswürdig ist. Sonst kann das Verschlüsselungsprogramm manipuliert werden, das Passwort geklaut werden oder was auch immer...

So ist zum Beispiel die Verschlüsselung von Mails mit GnuPG, die mit den richtigen Einstellungen (höchst wahrscheinlich) nicht so bald gebrochen werden kann, nutzlos, wenn deine Tastatureingaben mitgelesen werden. Anfang September berichteten Guardian und New York Times über die Anstrengungen der NSA und des britischen Government Communications Headquarters (GCHQ) bei ihrem Kampf gegen Verschlüsselung im Internet. Diese dringen demnach zum Beispiel in Geräte ein, um die noch unverschlüsselte Kommunikation abzugreifen. Darüber hinaus besorgen sich die Geheimdienste auf unterschiedlichen Wegen Schlüssel, nutzen bekannte Lücken oder veranlassen Hersteller, Hintertüren in Krypto-Hard- und Software einzubauen. Welche Hersteller betroffen sind, ist unbekannt. Deshalb muss davon ausgegangen werden, dass alle

kommerziellen Produkte potentiell manipuliert sind. Das Risiko bei Open Source oder wenigstens Quell Code offenen Programmen ist geringer, da sie auf Hintertüren überprüft werden können.

Also sauberen Rechner und Verschlüsselungsprogramme, deren Quellcode öffentlich oder besser noch Open Source ist, verwenden.
Und natürlich musst du ein gutes Passwort wählen. Also möglichst lang und fast noch wichtiger: keine Wörter, egal in welcher Sprache, keine für Computer erkennbare Logik. Am besten eine lange Zeichenfolge ohne erkennbare Logik.

Allgemein kann man auch sagen, dass immer die stärkste Verschlüsselung gewählt werden sollte. Bei der asymmetrischen RSA-Verschlüsselung die z.B. GnuPG nutzt sind das 4.096 Bit, bei der symmetrischen AES-Verschlüsselung 256 Bit. Außerdem ist es sinnvoll Festplatten und USB-Sticks komplett und nicht nur Ordner oder Dateien zu verschlüsseln oder beides zu kombinieren. TRUE-CRYPT bietet außerdem die Möglichkeiten versteckte verschlüsselte Ordner anzulegen und beim Erstellen der Verschlüsselung eine Kombination der Algorithmen AES, Twofish und Serpent zu verwenden. Allerdings ist TRUE-CRYPT zwar Quellcode offen, weit verbreitet und für alle gängigen Betriebssysteme verfügbar, aber nicht als Open Source anerkannt. Alternativen sind FREE-OTFE für Windows- und DM-CRYPT bzw. LUKS für Linuxbetriebssysteme. Beide Programme sind miteinander kompatibel, sie können also Verschlüsselungen, die mit dem jeweils anderen Programm erstellt wurde, öffnen.

Doch für alle, die große Sicherheit brauchen, ist zudem eine Beschäftigung mit der Funktionsweise unterschiedlicher Krypto-Verfahren unumgänglich. Erst recht wenn die verschlüsselten Daten eine solche Relevanz haben, dass sie auch in 20 Jahren nicht geknackt werden sollen. Denn ein verschlüsseltes Datenpaket, das im Anhang einer Mail abgefangen wurde oder eine verschlüsselte Festplatte, die bei einer Hausdurchsuchung mit genommen wurde, können lange auf ihre Entschlüsslung warten und neue Rechnerarchitekturen ermöglichen immer größere Rechenleistungen. Wer sich für Verschlüsselung interessiert, findet z.B. auf der Hompage www.golem.de unter dem Titel „Verschlüsselung - Was noch sicher ist“ ein Überblick über kryptographische Algorithmen und deren mögliche Probleme. Doch wie gesagt, leider nur verständlich und in die Praxis zu übersetzen wenn man sich damit etwas beschäftigt.

Kostprobe: *„AES gibt es in drei Varianten: 128, 192 oder 256 Bit. 2012 wurde versucht auszurechnen, wie aufwendig ein Angriff auf AES mit 128 Bit mit Hilfe von Supercomputern wäre. Das Ergebnis hinterlässt zumindest ein ungutes Gefühl: Die Kosten für die Chipproduktion lägen im Bereich von etwa 80 Milliarden Dollar. Der größte Flaschenhals wäre jedoch die Energieversorgung. Ein solcher Spezialrechner würde die Leistung von 4 Terawatt benötigen. Fazit: Es ist zwar enorm aufwendig, aber nicht unmöglich.[…] Einen Quantencomputer zu bauen, der zur Faktorisierung von Schlüsseln geeignet ist, ist eine gigantische Herausforderung. Man müsste einen Quantencomputer bauen, der einen gesamten RSA-Schlüssel auf einmal angreifen kann - also 2.048 oder 4.096 Bit. Ein interessanter Aspekt ergibt sich daraus allerdings: Verfahren mit elliptischen Kurven sind aufgrund ihrer kurzen Schlüssel gegenüber Quantencomputern deutlich verwundbarer. Für symmetrische Verfahren sind Quantencomputer keine wirkliche Bedrohung. Sie würden die Schwierigkeit eines Angriffs nur auf die Quadratwurzel reduzieren. Ein Angriff auf AES-256 wäre also so schwer wie ein klassischer Angriff auf AES-128.“*

Daten und Metadaten sicher löschen

Wenn du einen Datenträger auf normalen Weg löscht, bleiben die Daten erhalten!
Sie werden lediglich nicht mehr angezeigt und der Speicherplatz wo sie sich befinden wird zum Überschreiben freigegeben. Die Daten sind aber einfach wiederherzustellen. Deshalb musst du den Speicherplatz überschreiben. Je nachdem wen man fragt, reicht einfaches Überschreiben mit Nullen oder wird bis zu 35-faches mit Zufallszahlen empfohlen. Sicher ist sicher, also lieber öfter Überschreiben. Für Windows erledigt das z.B. das auch von USB-Sticks startbare Programm ERASER. Du kannst Dateien überschreiben oder auch freien Speicher. Wenn du freien Speicher überschreibst, musst du vorher die Standarteinstellung ändern, damit 35 Mal überschrieben wird.

In Linuxbetriebssystemen gibt es mehrere kleine Programme zum sicheren Löschen von Daten (-trägern). Einige sind im SECURE-DELETE-PACKAGE zusammengefasst und werden über den Terminal gesteuert (bei TAILS ist das vorinstalliert). Es umfasst SECURE-REMOVE „srm“ 35-faches Überschreiben von Dateien, SECURE-FREE-SPACE-WIPER „sfill“ für freien Speicherplatz und weitere Befehle für das Säubern des Arbeitsspeichers (RAM) und des Swap.
Wenn du im Terminal nur „srm“ oder „sfill“ eingibst, öffnet eine Liste mit verfügbaren Optionen der jeweiligen Funktion. Der Befehl „srm -vr Stickname/Ordnername/Dateiname“ würde z.B. die ausgewählte Datei auf einem Stick, löschen. Die Option „-v“ bedeutet, dass dir angezeigt wird was passiert, „-r“ löscht rekursiv Verweise auf die Datei. Wenn du was auf einem Stick löschen willst, kannst du es auch mit Befehl “cd /media“ anwählbar machen, anstatt den Pfad selbst einzutippen.

Je nach dem welches Betriebssystem, Speichermedium und Dateisystem du verwendest, können allerdings Verweise auf die überschriebenen Daten erhalten bleiben. Auch können bei längerer Nutzung kleine Bereiche des Speichers beschädigt werden. Diese werden, von dir unbemerkt, nicht mehr benutzt und auch nicht mit überschrieben, können aber (Teile von) Daten enthalten.Wenn du ganz sicher gehen willst, solltest du ein Betriebssystem von CD laufen lassen, da dort nichts gespeichert werden kann und den Datenträger auf dem du gespeichert hattest, physisch vernichten. Physische Vernichtung kann zum Beispiel das Ausbrennen der Speicherchips mit einem Mini-Lötkolben und die anschließende Zertrümmerung sein. Ersäufen oder einmal mit dem Hammer draufhauen reicht nicht! Also im Zweifel den Computer, unter Umgehung der Festplatte, von CD betreiben und auf USB-Sticks o.ä. speichern und ab und zu oder aus gegebenen Anlass einen neuen besorgen.

Außerdem musst du darauf achten, dass viele Dateitypen auch Metadaten enthalten. Bei jpeg Fotos z.B. Erstellzeit, Kamera- bzw. Gerätetyp und vor allem bei Smartphones oft auch GPS-Daten des Aufnahmeorts. Bei pdf z.B. Erstelldatum, Benutzername und z.T. verwendete Programme. Gleiches gilt für viele Textdateiformate. Für Linux gibt es das METADATA-ANONYMISATION-TOOLKIT (MAT), das vom TOR-Projekt mitentwickelt wurde (bei TAILS im Zubehör). Es kann die Metadaten sehr vieler Dateitypen löschen. Für Windows gibt es nur Dateispezifische Programme. Informiere dich welche Metadaten bei den einzelnen Programmen und Dateitypen angelegt werden und wie du sie löscht, bevor du deine Datei veröffentlichst oder verschickst.

Online arbeiten

Deinen personifizierten Internetanschluss solltest du nur für persönliche Sachen nutzen. (Was das ist, darüber lässt sich streiten, siehe Absatz Facebook, Google und Co.) Doch auch öffentlich zugängliche bzw. nicht personalisierte Internetanschlüsse haben unterschiedliche Tücken.

Da es sehr viel unterschiedliche Nutzungsmöglichkeiten gibt, stellen sich auch sehr viele Fragen. Zunächst ist es wichtig, dass du dir überlegst wie schutzbedürftig deine Tätigkeit ist.
Die nächste Frage ist, welche Art von Sicherheit du brauchst. Wenn du zum Beispiel für eine lokal verankerte, öffentlich agierende Gruppe eine Homepage pflegst, geht es dir wahrscheinlich hauptsächlich darum, deine Identität zu schützen. Es ist aber nicht so wichtig, dass feststellbar ist, das dein Posting am öffentlichen Rechner eines lokalen Szenetreffs verfasst wurde und welchen Inhalt es hat (wenn es sowieso direkt veröffentlicht wird).

Etwas anderes ist es, wenn du deine verschlüsselten Mails abholst und nicht willst, dass sie mitgelesen werden oder wenn du etwas recherchierst oder veröffentlichst und nicht lokalisierbar sein willst. Du musst dir also für jede spezifische Nutzung überlegen in welche Richtung du dich wie stark absichern willst. Wenn du das weißt, kannst du dir überlegen welchen Internetanschluss du benutzt, welchen Computer und wie du deine Verbindung schützt. Entweder du benutzt öffentliche Computer mit Internetzugang oder ein eigenes Gerät an einem Zugang der öffentlich oder zumindest offen ist. Es gibt viele verschiedene Wege. Du musst entscheiden was für dich geeignet ist. Wenn du einen Zugang gefunden hast, der dir nicht zugeordnet werden kann, hast du dementsprechend unterschiedliche Möglichkeiten.

In jedem Fall solltest du TOR verwenden um deine IP-Adresse zu verschleiern. (Sieh Absatz: TOR? Ja, aber...) Wenn du an einem öffentlichen Computer bist, kannst du ganz einfach das TOR-BROWSER-BUNDLE benutzen. Der Vorteil davon ist, dass es sehr einfach zu handhaben ist und du es auf einem USB-Stick mitbringen kannst. Der Nachteil ist, dass du ein Betriebssystem und einen Computer benutzt, die du nicht einschätzen kannst.

Eine weitergehende Alternative ist das, vom TOR-Projekt mitentwickelte, Linuxbetriebssystem TAILS. Es legt den Fokus auf Sicherheit und funktioniert von CD oder USB-Stick. Dabei hinterlässt es keine Spuren auf dem genutzten Computer, es sei den du speicherst selber etwas. Viele nützliche Programme und Funktionen zum Verschlüsseln von Daten und Kommunikation sind schon integriert und jede ausgehende Verbindung wird automatisch über TOR hergestellt. So ist TAILS für alle Arten abgesicherter Internet-Anwendungen, vom verschlüsselt Chaten über Mails bis hin zu Recherche und Veröffentlichungen, das umfassendste und dabei praktischste System.

Du kannst einen fremden/öffentlichen Rechner von deiner TAILS-CD/USB-Stick booten lassen. Dazu musst du, bevor das auf der Festplatte installierte Betriebssystem startet, ins BIOS-Menü des Computers zu wechseln. Direkt nachdem der Computer startet, wird dir angezeigt welche Taste du drücken musst, um ins BIOS zu wechseln. Je nach Computer unterscheidet sich das. Dort änderst du die Bootreihenfolge, sodass der Computer zuerst von CD/USB-Stick startet.

Du kannst natürlich auch einen eigenen Computer mit TAILS betreiben, wenn du unbemerkt einen öffentlich/offen zugänglichen Netzzugang nutzen willst. Dies funktioniert auch ohne Festplatte. Allerdings solltest du bei einem eigenen Rechner, den du vermutlich mehrfach nutzen willst, darauf achten, dass du ihn von Anfang an und immer auf diese abgesicherte Weise nutzt. Außerdem solltest du jedes Mal die MAC-Adresse der Netzwerkkarte manuell ändern, weil du den Rechner ja wieder mitnimmst und sonst deine eindeutig zugeordnete MAC-Adresse im Router hinterlässt. (siehe Absatz: MAC-Adresse manipulieren)

Tor? Ja, aber...

„Für die meisten Gelegenheiten stellt TOR den besten verfügbaren Schutz vor einem gut ausgerüsteten Angreifer dar. Es ist jedoch ungeklärt, wie stark TOR (oder irgendein anderes existierendes anonymes Kommunikationswerkzeug) Schutz vor der flächendeckenden Überwachung der NSA bietet."

TOR-Blog-Mitteilung vom 21.09.2013

Glenn Greenwald, der die Snowden-Enthüllungen für den Guardian auswertet, schreibt dazu folgendes (gekürzt):

„Die NSA hat wiederholt versucht, Angriffsmethoden zu entwickeln, mit denen die Nutzer des TOR-Anonymisierungsnetzwerkes getroffen werden können [...]. Geheime Dokumente haben enthüllt, dass die derzeitigen Erfolge der NSA auf dem Identifizieren von Anwendern und dem anschließenden Angreifen von Schwachstellen in deren Software beruhen. Eine Methode zielte auf die TOR-Variante des Firefox-Browsers, wobei die NSA volle Kontrolle über den Zielcomputer erlangte, inklusive des Zugriffs auf alle Dateien, Speicherung der Tastenschläge und die Onlineaktivität. Die bekanntgewordenen Dokumente deuten jedoch auch darauf hin, dass die grundsätzliche Arbeitsweise von TOR nicht kompromittiert ist. Eine interne NSA-Präsentationsfolie trägt dann auch die Überschrift „TOR stinkt". Weiter ist dort aufgeführt, dass man „mit manueller Analyse in der Lage ist, eine sehr kleine Anzahl von TOR-Nutzern zu identifizieren", aber dass die Behörde „keinen Erfolg dabei hatte, einen Nutzer mittels einer spezifischen Anfrage zu de-anonymisieren." Eine weitere Folie bezeichnet TOR als „den König hoch-sicherer Internetanonymität mit geringer Latenz". [...]

Doch auch wenn es so aussieht, als wenn die NSA die TOR-Software selbst nicht hat kompromittieren können, enthalten Dokumente Details über theoretische Angriffskonzepte, von denen mehrere auf einer großflächigen Überwachung des Internets beruhen, wie sie durch das Anzapfen der Internetkabel durch die NSA und das britische GCHQ gegeben ist.

Einer dieser Angriffe basiert auf dem Versuch, identische Muster bei den ein und aus dem Netzwerk gehenden Signalen zu entdecken, wobei der Anwender de-anonymisiert werden kann. Es handelt sich hierbei um eine bereits relativ lange diskutierte theoretische Schwäche des Netzwerkes: Dass ein großer Teil des Datenverkehrs identifiziert werden könnte, wenn eine Behörde nur eine genügend große Anzahl von TOR-Exitnodes kontrollieren würde. Das in dem Dokument beschriebene theoretische Angriffskonzept wäre dabei einerseits abhängig von der umfassenden Überwachung des Datenverkehrs und andererseits von einer Anzahl von der NSA selbst betriebener TOR-Knotenpunkte (eng. Nodes). Auf einer anderen NSA-Präsentationsfolie steht jedoch, dass der Erfolg dieser Methode „vernachlässigbar" sei, da die NSA „nur zu wenigen Knotenpunkten Zugang habe", und dass „es schwierig sei, die Daten sinnvoll mit passiver Sigint zu verbinden."

Andere von den Behörden genutzte Methoden sind der Versuch, Datenanfragen auf von der NSA betriebene Server umzuleiten oder andere Software auf dem Rechner der Zielperson anzugreifen. Eine Folie mit dem Titel „TOR: Übersicht über verschiedene Techniken" verweist außerdem auf Versuche, in Kooperation mit dem GCHQ, die weitere Entwicklung von TOR zu beeinflussen.

Eine weitere Methode, um Nutzer zu identifizieren ist das Messen der Zeitpunkte, an denen eine Nachricht in das TOR-Netzwerk geht und wann sie hinausgeht (Korrelationsangriff). Eine andere Methode ist das Schwächen oder Lähmen der Knotenpunkte (z.B. DDoS-Attacke, Botnetz??) des Netzwerkes, um Benutzer dazu zu bringen, ihre Anonymität zu verlassen. [...]

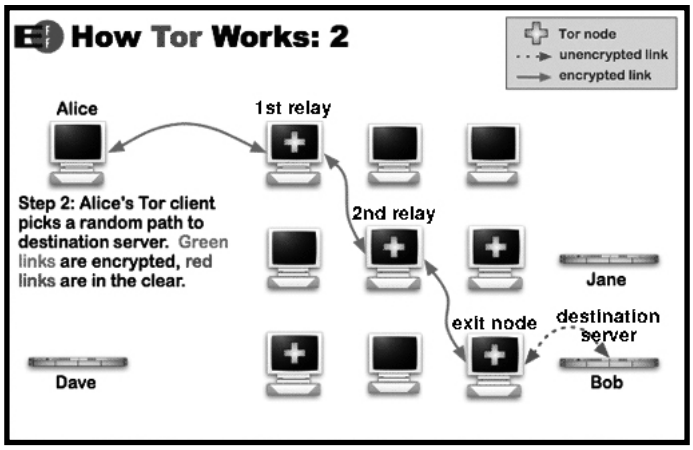
Viele Angriffe führen auch dazu, dass Schadsoftware auf den Computern von TOR-Nutzern, die bestimmte Webseiten besuchen, installiert wird. [...] Eine Methode, welche die NSA entwickelt hat, um TOR-Nutzer durch verwundbare Software auf ihrem Rechner zu enttarnen, trägt den Namen „EgotisticalGiraffe". Es geht dabei um das Ausnutzen einer Schwachstelle im Tor Browser Bundle, einer Gruppe von Programmen, die es Anwendern leichter machen sollen, TOR zu installieren. Eines dieser Programme ist eine TOR-Variante des Firefox-Browsers. Diese Technik, welche in einer streng geheimen Präsentation mit dem Titel „Die Schichten von TOR mit EgotisticalGiraffe abziehen" beschrieben wurde, identifizierte die Besucher von Webseiten, welche den Anonymisierungsdienst nutzten, und attackierte auch nur diese, unter Ausnutzung einer Schwachstelle in einer alten Firefox-Version. Bei diesem Ansatz wird TOR also nicht direkt attackiert. Es geht eher darum die TOR-Nutzer zu identifizieren und dann ihre Browser zu infizieren. Anhand der Dokumente von Edward Snowden ist bekannt, dass diese spezielle Firefox-Schwachstelle von dem Browserentwickler Mozilla ab der Firefox-Version 17 vom November 2012 behoben wurde. Zum Zeitpunkt als die NSA-Folie geschrieben wurde (Januar 2013), war es der NSA noch nicht gelungen, diese Hintertür wieder zu öffnen. Alle TOR-Nutzer, die ihre Software nicht regelmäßig mit Updates auf den neuesten Stand gebracht hatten, waren jedoch noch angreifbar. Eine ähnliche, wenn auch weniger komplexe Ausnutzung einer Schwachstelle im Firefox-Browser wurde von Sicherheitsexperten im Juli 2013 bekannt gemacht. [...]

Roger Dingledine, der Präsident des TOR-Projekts, sagte, dass die Anstrengungen der NSA zeigten, dass TOR alleine keinen ausreichenden Schutz vor der De-Anonymisierung durch Geheimdienste bieten könnte. Die Ereignisse würden aber auch zeigen, dass TOR eine große Hilfe sei, um Massenüberwachung zu bekämpfen. „Die gute Nachricht ist, dass sie eine Browserschwachstelle nutzten, was bedeutet, dass nicht erkennbar ist, dass sie das TOR-Protokoll brechen können oder eine Datenanalyse des TOR-Datenverkehrs möglich ist," sagte Dingledine. „Es ist immer noch das einfachste, den Laptop,

das Telefon, oder den Rechner zu infizieren, um mehr über die Person hinter dem Keyboard herauszukriegen. TOR hilft hier immer noch: Du kannst Einzelpersonen über Browserschwachstellen attackieren, aber wenn du zu viele Nutzer angreifst, wird es jemand merken. Also selbst, wenn die NSA darauf abzielt, jeden überall zu überwachen, so muss sie immer noch viel genauer überlegen, welche TOR-Nutzer sie auswählt.“

Er fügte jedoch weiter hinzu: „Einfach nur TOR zu benutzen ist nicht genug, um jemanden in allen Situationen sicher zu halten. Browser-Schwachstellen, Massenüberwachung und allgemeine Anwendersicherheit sind Herausforderungen für den durchschnittlichen Internetsurfer. Diese Angriffe machen klar, dass wir, die gesamte Internetcommunity, an besserer Sicherheit für Browser und andere Internetanwendungen arbeiten müssen.“ […]“

So, was können wir daraus ziehen? Zunächst ist es wichtig festzuhalten, dass es nichts gibt, dass größere Anonymität gewährt, der Einsatz von TOR auch die Geheimdienste vor Probleme stellt und die Nutzung deshalb auf jeden Fall sinnvoll ist. Wie bei allem vorher Beschrieben ist die wichtigste Frage, wie groß dein Schutzbedürfnis ist. Wenn es groß ist und du potentielle Angriffsmöglichkeiten ausschließen willst, scheinen uns Ort, Zeit und Dauer der Nutzung entscheidende Faktoren zu sein. Doch gucken wir uns die unterschiedlichen Angriffsszenarien an.



Ein großer Teil des Datenverkehrs könnte identifiziert werden, wenn eine Behörde nur eine genügend große Anzahl von TOR-Ausgangsknoten kontrolliert. Denn sobald sowohl der Verkehr am Eintritts- als auch am Austrittsknoten protokolliert wird, lässt sich die Herkunft der Datenpakete rekonstruieren. Diese Angriffsmöglichkeiten würde weite Teile des TOR-Netzwerks enttarnen, ist aber in den NSA-Folien als theoretische, vernachlässigbare Variante benannt. Wie lange das gilt, ist von uns nicht abzuschätzen. Aber da es sehr viele Leute betreffen würde, ist davon auszugehen, dass es sobald es einmal zu repressiven Zwecken genutzt würde, bekannt wäre. Es bleibt also nicht anderes übrig als davon auszugehen, dass diese theoretische Möglichkeit (noch) nicht umsetzbar ist. Durchsucht regelmäßig den TOR-Blog und andere Foren auf Hinweise darauf, ob sich daran etwas geändert hat.

Die zweite Möglichkeit, das Ausnutzen von Schwachstellen in der verwendeten Software. Der beschriebene Angriff funktionierte aus der Kombination aus der Ausnutzung einer Firefox-Browser Schwachstelle und der Manipulation einer Homepage. Wer also eine bestimmte Version des TOR-BROWSER-BUNDLE benutzte und die manipulierte Homepage besuchte, konnte identifiziert werden. Also ist insbesondere beim Besuch von Homepages, die wahrscheinlich beobachtet werden Vorsicht angesagt. Wie bei jeder sicherheitsrelevanten Software muss außerdem darauf geachtet werden, immer die aktuellste Version zu nutzen. Wobei Sicherheitslücken, die noch nicht bekanntermaßen ausgenutzt wurden, trotzdem enthalten sein können und du dies erst im Nachhinein erfährst. Deswegen sind weitere Schutzmaßnahmen nötig, doch dazu später mehr. Wir wollen erst noch weitere Angriffsmöglichkeiten anführen.

Die Liste der normalen TOR-Knoten ist öffentlich, da die Auswahlmöglichkeit aus vielen Knoten eine Voraussetzung für die Funktionsweise von TOR ist. Das sich daraus ergebene Problem wird vor allem in Bezug auf Zensur diskutiert. Denn einige Staaten, die verhindern wollen, dass ihre allgemeine Internetzensur durch die Nutzung von TOR umgangen wird, sperren das TOR-Protokoll bzw. den Zugriff zu den bekannten Knotenpunkten. Die Nutzung eines TOR-Bridge-Relays kann dies erschweren, da du einen Eingangsknoten als Brücke (Bridge) nutzt, der nicht öffentlich bekannt ist. Allerdings musst du dafür einer Zentralinstanz (bridge authority) vertrauen, eine vertrauenswürdige Verbindung zu ihr herstellen und dir von ihr einen Zugang zuteilen lassen. Da die Nutzung eines Bridge-Relays neue Probleme aufwirft und die eigentlich niedrige Hürde, TOR (z.B. mit dem BROWSER-BUNDLE) zu bedienen, erhöht, ist das wohl eher eine Überlegung für Leute, die sich damit intensiv beschäftigen wollen. Das würde sich ändern wenn auch hierzulande die Nutzung von TOR gesperrt werden würde.

Ein Korrelationsangriff, also ein zeitlicher Abgleich der ins TOR-Netzwerk ein- und ausgehenden Datenpakete. Eine im Jahr 2013 veröffentlichte Studie von Wissenschaftler_innen des U.S. Naval Research Laboratory und der Georgetown University befasste sich mit dem bereits bekannten Problem der ausgedehnten Protokollierung des Netzwerkverkehrs von TOR. Ziel war es, unter realistischen Bedingungen die Wahrscheinlichkeit und den Zeitraum einschätzen zu können, der benötigt wird, um genügend Daten für eine Zerstörung der Anonymität zu sammeln. Dabei gelang es in 6 Monaten durch den Betrieb eines einzigen mittleren Tor-Relays, die Anonymität von 80% der verfolgten Benutzer_innen zu brechen. Hinsichtlich der Snowden-Enthüllungen betonten die Wissenschaftler_innen, dass eine größere Infrastruktur (wie die von Geheimdiensten) die benötigte Zeit deutlich reduzieren kann.

Was heißt das jetzt für die Praxis? Die Wahl des Ortes und des Zeitpunkts spielen für viele Angriffsmethoden eine Rolle. Je länger du TOR von ein und dem selben Ort nutzt, desto unsicherer ist es. Dies ist also vor allem ein Problem wenn du TOR für regelmäßige Tätigkeiten vom selben Ort aus nutzt. Also z.B. von deinem personalisierten Internetanschluss oder wenn du regelmäßig vom selben öffentlichen Anschluss e-Mails abrufst, eine Homepage pflegst o.ä.. Je mehr du durch ein Muster in deiner Nutzung eingekreist bist und je weniger andere TOR-Nutzer_innen in der Nähe sind, desto einfacher bist du zu finden. Problematisch könnte es z.B. sein wenn du zwar noch nicht identifiziert bist, aber deine frühere Aktivität bereits aufgefallen und als interessant eingestuft wurde. Wenn dann nach bestimmten Mustern erwartet wird, dass du sie fortsetzt bzw. wiederholst, könntest du enttarnt werden. Wenn wir bei dem Beispiel der Pflege einer Homepage bleiben, könnte das erkannte Muster sein, dass die Homepage einmal die Woche in der Regel am frühen Freitagabend über eine TOR-Verbindung aktualisiert wird. Wenn die Homepage zudem geographisch zugeordnet ist, etwa weil sie einer lokalen Gruppe gehört, trifft das Muster auf weit weniger Nutzer_innen zu. Noch einfacher wird es wenn du irgendwo bist, wo du weit und breit die_der Einzige bist, die_der TOR nutzt.

Für alle Angriffsmöglichkeiten gilt: wenn du größere Sicherheit willst, solltest du dir Gedanken dazu machen, von wo, wie lange und wie regelmäßig du was über TOR machst. Also muss du nicht nur deine Verbindung über die Nutzung von TOR absichern, sondern auch den genutzten Rechner schützen und im Zweifel, dafür sorgen, dass du im Real Life nicht gefunden wirst, selbst wenn deine Verbindung aufgedröselt wurde. Also solltest du gucken, dass du am Ort, an dem du dich einwählst, keine Spuren hinterlässt. Z.B. deine MAC-Adresse im Router oder dein Gesicht in der Kamera eines Internetcafés oder...

Unabhängig von den genannten Angriffsmöglichkeiten solltest du dir die Tipps auf der Seite torproject.org durchlesen und sie beachten. Unter dem Titel „Want Tor to really work?“ wird, leider nur auf Englisch, erklärt was du beachten musst. z.B. nur den vorkonfigurierten Browser mit TOR nutzen, dort keine Browserplugins erlauben oder installieren, https-Versionen von Homepages verwenden, keine runtergeladenen Dokumente im Browser öffnen. Also z.B. ein pdf über Rechtsklick und die Auswahl „Ziel speichern unter“ speichern und es nur offline betrachten. Das TOR-BROWSER-BUNDLE schützt nur deinen Browser, wenn du für das pdf z.B. dem Adobe Reader erlaubst mit dem Internet zu kommunizieren, ist dies nicht geschützt. Bei TAILS ist das anders, da jede Nicht-TOR Verbindung geblockt wird. Im TOR-Browser kannst du auch Skripte allgemein verbieten, bzw. nur zulassen wenn du auf einer vertrauenswürdigen Seite java oder flash benötigst.

Bei manchen Aktivitäten kann es auch nützlich sein, über die Auswahl „Neue Identität“ innerhalb einer Sitzung die IP-Adresse zu ändern. z.B. wenn du unterschiedliche Sachen machst und keine Verknüpfungen wünschst. Dies funktioniert beliebig oft. Trotzdem solltest du personalisierte und nicht personalisierte Nutzungen nicht kombinieren.

Außerdem anonymisiert TOR lediglich deinen Standort und worauf du zugreifst, die Inhalte deiner Kommunikation, z.B. e-Mails, Chats etc. sind deshalb nicht verschlüsselt. Wir sagen das nur nochmal um Missverständnissen vorzugreifen. Du solltest Kommunikation also zudem verschlüsseln. (siehe Absätze zu e-Mails und Chat)

MAC-Adresse manipulieren

Da in den NSA-Folien von Angriffen auf Router und Kartierung von Netzwerken anhand von MAC-Adressen die Rede ist, haben wir uns mal angeschaut, was damit gemeint sein könnte.
Die Netzwerkkarte deines Endgerätes übermittelt ihre eindeutige MAC-Adresse an den Router, der sie speichert und ihr anhand dieser die angefragten Daten übermittelt. Bei manchen W-LAN-Verbindungen wird sie auch an einen zentralen Server übermittelt. Darüber hinaus wird sie eigentlich nicht in die Weiten des Internets übermittelt. Wenn aber Server oder Router gehackt oder beschlagnahmt werden, ist sie auslesbar. Es scheint also zusätzlich zur Nutzung von TOR auch notwendig zu sein diese MAC-Adresse zu manipulieren. Allerdings nur wenn du ein eigenes Gerät, an einem nicht personifizierten Zugang benutzt. An einem öffentlichen Rechner, wie im Internetcafé, macht das keinen Sinn. Schließlich lässt du den Rechner sowieso da. Außerdem würdest du wahrscheinlich das Problem haben, dass die Router/Server nur ihnen bekannte MAC-Adressen zulassen. Auf dieses Problem kannst du aber immer stoßen, wenn ein Netzwerk nur bekannte Rechner zulässt.

Die MAC-Adresse der Netzwerkkarte kann nicht geändert werden, da sie in der Hardware festgelegt ist. Du kannst aber mit Software dafür sorgen, dass sie nicht übermittelt wird, bzw. dass stattdessen eine virtuelle für die Dauer deiner Sitzung erzeugte MAC-Adresse übermittelt wird. Dafür musst du sie jedes Mal, sobald du dein Computer hochgefahren hast und bevor! du irgendeine Verbindung herstellst, ändern. Du musst sicherstellen, dass der Computer nicht automatisch eine Verbindung herstellt, bevor du die MAC-Adresse manipuliert hast. Also Netzwerkkabel abziehen und/oder W-LAN-Adapter abstellen bis du die Adresse geändert hast. Wenn du dann eine Verbindung herstellst, übermittelt dein Computer diese manipulierte MAC-Adresse anstatt der, die auf

deiner Netzwerkkarte steht. Für viele Betriebssysteme gibt es kleine Programme die dies erledigen. Für Linuxbetriebssystem ist das der MAC-CHANGER, der über den Terminal gesteuert wird (bei TAILS schon dabei).

Der Terminal-Befehl „macchanger -h“ zeigt dir die Optionen. Du kannst dir die aktuelle MAC-Adresse anzeigen lassen und deiner Netzwerkkarte eine zufällige oder eine des selben Herstellers zuweisen lassen. Du kannst dir auch eine Liste mit Tausenden existierenden MAC-Adressen anzeigen lassen und eine daraus benutzen. Denn eine zufällige ist fast immer eine, die gar nicht existiert und somit im Falle einer Überprüfung schneller als manipuliert auffällt.
Der Befehl „macchanger -a eth0“ würde z.B. der mit „eth0“ bezeichneten Netzwerkkarte eine MAC-Adresse des selben Herstellers und der selben Art zuordnen. Wenn du nicht weißt wie deine Netzwerkkarte bezeichnet ist, kannst du dir dies mit dem Befehl „ls /sys/class/net“ anzeigen lassen.

Du kannst dir aber auch die graphische Benutzeroberfläche MAC-CHANGER-GTK installieren. Dann musst du nur den Befehl „macchanger -gtk“ im Terminal eingeben und kannst anschließend bequemer, mit der sich öffnenden Programmoberfläche, arbeiten.

Für Windows XP, Windows Vista und Windows 7 ist ebenfalls ein MACCHANGER mit graphischer Benutzeroberfläche verfügbar. Und auch ohne diese Programme gibt es, sowohl in Windows- als auch in Linuxbetriebssystemen, Möglichkeiten die MAC-Adresse zu manipulieren. Dies erfordert allerdings wieder etwas Beschäftigung mit dem Thema, während die Programme es recht einfach machen.

E-Mail-Kommunikation

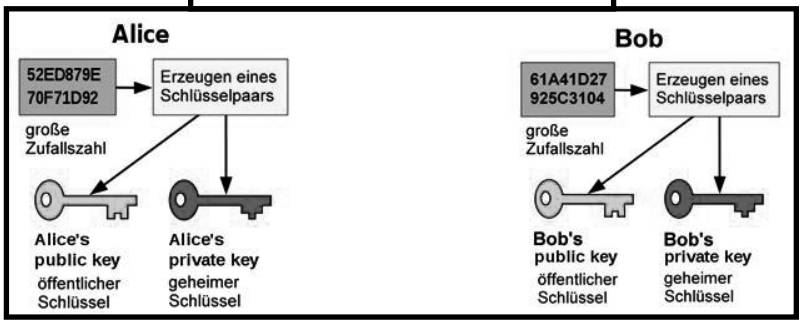
Du kannst davon ausgehen, dass alle großen, kommerziellen Anbieter mit Geheimdiensten kooperieren und bereitwillig alles rausrücken. Also ist es zunächst sinnvoll dir einen guten Mailanbieter zu suchen, z.B. kleine linke Serverbetreiber wie Riseup oder Nadir. Außerdem ist es sinnvoll deine Mails zu verschlüsseln. Denn bei unverschlüsselten Mails ist wie gesagt eine automatisierte inhaltliche Auswertung einfach umzusetzen. Ein weit verbreitetes und gutes Verschlüsselungsprogramm ist GnuPG.
Doch wie gesagt die Metadaten bleiben immer erhalten. Auch bei verschlüsselten Mails!
Auch die Betreffzeile ist bei verschlüsselten Mails immer sichtbar. Gleichzeitig ist die Nutzung von Verschlüsselungstechnik etwas, dass dich interessanter macht. Dadurch steigt die Wahrscheinlichkeit, dass nicht nur deine Metadaten gespeichert werden, sondern dein Rechner gezielt angegriffen wird. Dabei spielt dann natürlich auch wieder eine Rolle von wo aus und mit welchem Rechner du ins Netz gehst. Die beschriebene Variante mit TAILS von irgendwo ist sicherer als der öffentliche Windows-Rechner im Szenetreff.

Die Vorgehensweise, die in dem langen Zitat von Bruce Schneiers beschrieben wird, USB-Sticks an Rechnern mit und Rechnern ohne Internetzugang zu benutzen erhöht zusätzlich die Sicherheit, dass die Verschlüsselung nicht z.B. durch Stehlen des Passworts umgangen wird. Dazu verschlüsselst du deine Daten an einem Rechner, der nie am Internet war und die_der Empfänger_in holt sie sich aus ihrem Postfach auf einen Stick und geht zur Entschlüsselung auch wieder an einen Rechner ohne Internetanschluss. Dazu müsst ihr aber entweder offline bzw. ohne Abhörmöglichkeit ein gemeinsames Passwort ausgemacht haben (wenn ihr z.B. TRUE-CRYPT-Container verschickt) oder Schlüssel austauschen, ohne dass sie manipuliert worden sein könnten (z.B. wenn ihr mit GnuPG verschlüsselte Dateien verschickt.) Dieses vorgeschlagene Vorgehen eröffnet allerdings gleichzeitig eine potentielle Möglichkeit den Rechner ohne Internetzugang zu infizieren, weil ihr mit den Sticks hin und her geht. Trotzdem ist die beschrieben Vorgehensweise für verschlüsselte Mails das sicherste. Erst recht wenn du zum Entschlüsseln ein Rechner nimmst, der nur von CD läuft. Außer offline Kommunikation gibt es nichts sichereres. Es bleibt aber dabei: **Was wirklich wichtig ist, gehört nicht in Mails bzw. überhaupt in Computer mit Internetanschluss!**

Chat und Instant Messaging

Eigentlich gilt das gleiche wie für Mails. Such dir einen guten unkommerziellen Anbieter und verschlüssele ordentlich. Neben GnuPG bietet sich hierfür vor allem OFF-THE-RECORD (OTR) – Messaging an. Es bietet im Vergleich zu OPEN-PGP (wie von GnuPG verwendet), zwei Vorteile. Für das Signieren und Verschlüsseln von Nachrichten werden kurzlebige Schlüssel verwendet und anschließend gelöscht. So kann auch bei Verlust des langlebigen Schlüssels vorherige Kommunikation nicht kompromittiert werden. Außerdem wird nur die erste Kontaktaufnahme mit einer eigenen Signatur versehen. Anschließend wird eine gemeinsame Signatur verwendet, die durch ein gemeinsames Geheimnis geschützt ist. Während eines Gespräches können beide Teilnehmer_innen sicher sein, dass die empfangenen Nachrichten authentisch und unverändert sind. Aber keine_r von beiden kann beweisen, dass eine Aussage von der_dem jeweilig Anderen stammt, denn beide könnten sie genauso gut selbst

Asymmetrische Verschlüsslung:



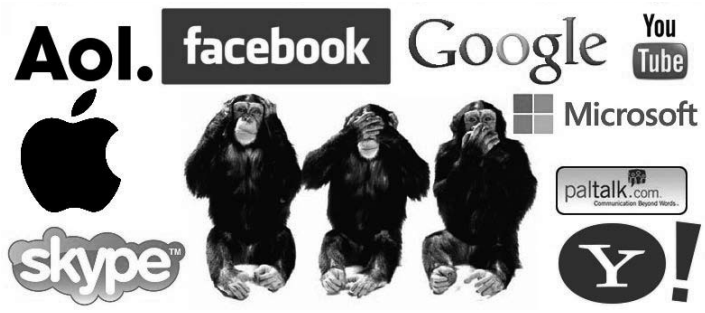
signiert haben. Wenn das Gespräch beendet ist, wird diese Signatur veröffentlicht. Im Fall einer Entschlüsselung des Gesprächs kann keine der getätigten Aussagen irgendwem bewiesen werden, da nun jede_r die Signatur verwenden kann und somit die Nachrichten fälschen.

Sei dir trotzdem bewusst, dass Rechner und Betriebssystem sowie Ort und Schutz deiner Verbindung, wie schon beschrieben, Einfluss darauf haben, wie sicher deine Verschlüsselung ist. Außerdem bleiben auch hier immer Metadaten hängen.

Facebook, Google und Co.

Für Facebook und andere sog. soziale Netzwerke und auch kommerzielle Suchmaschinen und Mailanbieter ist die Frage, wie lange Geheimdienste den kopierten Traffic speichern, gar nicht so wichtig, da sie selbst den gesamten bei ihnen anfallenden Traffic speichern. Dies gilt auch für wieder gelöschte Beiträge/Nachrichten z.B. bei Facebook. Die Geheimdienste müssen also nicht ihren Speicherplatz belasten sondern können, auch im Nachhinein, den des Unternehmens einsehen. Bei Facebook müssen sie dazu lediglich den Nutzer_innennamen eines Mitglieds eingeben und auswählen, aus welchem Zeitraum sie alle Privatgespräche lesen wollen.

Außerdem wirst du hier doppelt bespitzelt: aus kommerziellem und aus geheimdienstlichem oder polizeilichem Interesse. Da hilft es kaum, dir ein Pseudonym zuzulegen oder TOR zu verwenden. Denn durch die Art deiner Nutzung, deine „Freundschaften“ usw. bist du sowieso recht schnell identifiziert. Wir werden hier also keine Tipps geben wie dieser Schrott sicherer zu gestalten ist, es wären sowieso nur Illusionen. Macht eure Accounds dicht! Sie gefährden euch und andere. Und nutzt unkommerzielle Suchmaschinen, die keine IP-Adressen speichern.



Homepages betreiben

Wie du eine Homepage pflegst und dabei das Risiko einer Identifizierung verringerst, haben wir ja schon beschrieben. Doch wir wollen an dieser Stelle auch darauf hinweisen, dass alles was wir bisher geschrieben haben, meist deiner eigenen Sicherheit diente. Wenn du aber selber Angebote im Netz schaffst, hast du auch eine Verantwortung für diejenigen, die sie nutzen. Also sorge dafür, dass du sie nicht unnötig in Gefahr bringst. Besorge dir Webspace, bei dem nicht automatisch IP-Adressen gespeichert werden und bau z.B. in Blogs keinen Zugriffszähler ein, der dann doch wieder die IPs festhält. Noch unverantwortlicher sind Facebook-Accounds von politischen Gruppen/Projekten oder für Mobilisierungen. Wer so was macht ist naiv oder ein_e im besten Fall unfreiwillige_r Hilfspolizist_in bzw. Lockspitzel. Denn alle möglichen unbedarften Nutzer_innen „befreunden“ sich mit dir und geben gleichzeitig ihr Interesse an deiner Thematik bekannt. Du lieferst also Listen mit potentiellen Teilnehmer_innen an Demos oder was auch immer. Diese können verwendet werden um die Betroffenen weiter zu beobachten oder auch um sie als Spitzel anzuwerben.

Das gleiche gilt für Quick-Response (QR) Codes auf Flyern, Plakaten, Aufklebern. Jede_ r unbedarfte Smartphone-Nutzer_in, die_der sie fotografiert, „registriert“ sich für die Demo oder das was du sonst gerade bewirbst.

(Mobil-)Telefonie und Smartphones

Wie gesagt, es ist davon auszugehen, dass verdachtsunabhängig die Metadaten aller Telefonate und SMS gespeichert werden. Das umfasst bei Handys sowohl die Handynummer, die auf der SIM-Karte gespeichert ist, als auch eine Gerätenummer und natürlich die Verbindungsdaten. Darüber hinaus ist eine permanente Ortung der Geräte und damit auch ihrer Nutzer_innen möglich. Wie bereits erwähnt, ist auch eine automatisierte verdachtsunabhängige Stichwortsuche denkbar. Bei einem Upgrade der Relevanz einer Person können dann die ganzen Inhalte der Kommunikation ausgespäht werden. Klassisches Abhören. Auch schon länger bekannt ist, dass Handys zur Wanze umfunktioniert werden können, indem das Mikro dauerhaft aufnimmt. Auch für die integrierten Kameras ist ein Dauerbetrieb denkbar. Das gilt übrigens auch für alle Geräte mit Internetanschluss die Mikros und/oder Kameras integriert haben. Nur Akku raus hilft.

Bei Smartphones sind die Zugriffsmöglichkeiten noch umfassender. Laut den Snowden- Enthüllungen entwickeln spezialisierte Arbeitsgruppen Möglichkeiten, die einzelnen Betriebssysteme zu hacken. Ausgelesen werden können alle gespeicherten Informationen. Also Kontaktlisten, Passwörter, Notizen, Bilder usw. Smartphones sind genauso einzuordnen wie Computer, die ans Internet angeschlossen sind. Mit dem Unterschied, dass sie die Möglichkeit der Verknüpfung einzelner Datensammlungen erleichtern. Also z.B. Bewegungsprofile/Aufenthaltsort, Googlesuchen, SMS und Telefonbuch.

In Abwesenheit von Telefonen zu reden ist also am besten; in Anwesenheit von welchen zu reden birgt die Gefahr abgehört zu werden. Am Telefon zu reden erhöht die Gefahr. Außerdem erzeugst du Bewegungsprofile, wenn du mit einem Handy rumläufst. Wenn dein Handy ein Smartphone ist, bietest du den Diensten zusätzlich zahlreiche weitere Informationen an. Nimm dein Handy (auch im Alltag) nur mit wenn du es wirklich brauchst. Wenn du eins brauchst aber

nicht identifiziert werden willst, besorge dir für Demos o.ä. ein nicht personalisiertes Handy inklusive einer eben solchen SIM-Karte. Im Alltag oder über einen längeren Zeitraum bringt das relativ wenig, außer dass es für die Polizei vielleicht juristisch etwas schwerer ist. Keine Illusionen: über Bewegungsprofile und deine Nutzungsart wirst du relativ schnell gefunden. Denk außerdem daran, dass Stimmen auch automatisiert wieder erkannt werden können und dass es nicht reicht SIM-Karten zu wechseln, da auch das Gerät eine eindeutige Nummer übermittelt.

Fazit

Wir hoffen, dass du bis hier her durchgehalten hast und dass dir das Geschriebene eine Einschätzung der Arbeitsweise und der Möglichkeiten von Geheimdiensten erleichtert. Aber vor allem hoffen wir, dass dir dieser Text dabei hilft für dich Wege zu finden, dir die Sicherheit herzustellen, die du für deine spezifische Nutzung brauchst. Das kann ja wie beschrieben stark variieren. Trotz des Umfang des Textes konnten wir nur auf einige gängige Nutzungsarten eingehen und haben bestimmt auch dabei das ein oder andere Erwähnenswerte vergessen. Wir würden uns freuen, wenn auch andere versuchen würden ihr Wissen zugänglich zu machen.

Bei allen Sicherheits-Warnungen geht es uns nicht darum als Moralapostel aufzutreten und irgendwem, aus erzieherischen Gründen, die Spielzeuge (Smartpohone, Facebook usw.) wegzunehmen. Welche Selbst- und Fremdgefährdung für welchen Nutzen vertretbar ist, entscheidet im Alltag jede_r selbst. Die privatisierte Verantwortung, wie sie diese Gesellschaft ständig predigt, hat allerdings ihre Kehrseite. So weißt du meist nicht, wie dein_e Kommunikationspartner_in mit deiner Datensicherheit umgeht. Kollektive (Lösungs-) Ansätze rücken in weite Ferne. Dies gilt aber nicht nur für das Ausmaß der Beteiligung an der Selbst- und Fremdbespitzelung. Wir werfen das ein, um zu verdeutlichen, dass die sich ergebenen Fragen nicht moralisch oder gar technisch zu beantworten sind, sondern nur politisch. So ist auch die technische Überwachung jeder_jedes Einzelnen ein Problem, dass die_der Einzelne nicht lösen kann. Eine politische Einschätzung der umfassenden Überwachungsmaßnahmen und ihrer Wirkung auf die betroffenen Gesellschaften, ist nicht zu trennen von einer Kritik an Technologie und den gesellschaftlichen Umständen; z.B. dem War on Terror, der Krieg der niemals aufhört und die Überwachung rechtfertigt. Diese Dimension hat unser Text bewusst vernachlässigt. Eine solche Analyse ist nötig, aber eine noch umfassendere Angelegenheit als dieser Text. Und nicht zuletzt: Passt auf euch auf!

Nerds, Subversive, Anarchist_innen - Bande für ein Nachrichtendienstliches Desaster/Vereinigte Saboteure NSA-BND/VS

Anhang - Einige empfehlenswerte Seiten:

torproject.org - Die Seite des TOR-Projektes, stellt TOR in den verschiedenen Varianten und für alle gängigen Betriebssysteme zu Verfügung. Außerdem auch das empfehlenswerte Betriebssystem TAILS. Auf der Seite gibt es grundsätzliche Einführungen in TOR und TAILS und auf dem TOR-Blog aktuelle Nachrichten und Sicherheitswarnungen. Leider beides Größtenteils auf Englisch.

gnupg.org – Die Anbieter_innen Seite von GnuPG. Alle Infos auch auf deutsch.

otr.cypherpunks.ca – Die Seite der Hersteller_innen von OTR. Mit vielen nützlichen Infos und Listen von unterstützenden Programmen/Anbietern. Leider nur in Englisch.

prism-break.org - Seite mit Softwareprodukten, die Überwachung erschweren und vielen Tipps auch auf Deutsch

selbstdatenschutz.info - versammelt Anleitungen, Tutorials und Tipps sowie Hintergründe, Links und News rund um Datensparsamkeit, Datenschutz, Datensicherheit, IT-Sicherheit & Verschlüsselung

de.wikipedia.org und de.wikibooks.org – Da Programmbeschreibungen von den Hersteller_innen oder Anbieter_innen oft nur auf Englisch angeboten werden, kann ein Blick in die deutschsprachige Version von Wikipedia bzw. Wikibooks hilfreich sein. z.B. TOR und verschiedene Verschlüsselungssysteme und -programme werden ausführlich erklärt.

theguardian.com/world/the-nsa-files - Themenseite des Guardian zu den Enthüllungen (engl.)

golem.de – Nachrichten rund um IT-Sicherheit. z.B. haben wir dort gerade gelesen, dass die Anbieter_innen von Lavabit und Silent Circle, die ihre Dienste dicht machten um nicht mit der NSA kooperieren zu müssen, eine Dark Mail Alliance gegründet haben, um eine neue Open Source basierte Form der e-Mail zu entwickeln. Diese soll nicht nur verschlüsselt sein, sondern auch Metadaten schützen. Auch erfuhren wir, dass einige Wissenschaftler_innen gerade Spenden sammeln, um TRUE CRYPT auf mögliche Hintertüren zu überprüfen. Lohnt also immer einen Blick, um aktuelle Entwicklungen mit zubekommen.

cybererrorism.noblogs.org - ist ein Projekt von anarchistischen Geeks, Haecksen und Menschen, die sich einfach mit Technik beschäftigen.

netzpolitik.org - ist eine Plattform für digitale Bürgerrechte.

Offlineseiten - z.B. die von Büchern und Zeitungen