

# 1. Datenschutz in Selbsthilfe

- Worum gehts?
- Die eigene Maschine
- Die eigenen Daten
- Netzwerke

## Wichtige Unterscheidung:

- Abwehr von gezielten Angriffen oder
- Datenhygiene

□ Wenn jemand, insbesondere staatliche Stellen, wirklich eure Daten haben will, ist es *sehr* schwer, sie daran zu hindern. Nötig dafür ist weit mehr als nur der Wechsel des Betriebssystems – nötig wäre durchgängige Verschlüsselung, weitgehende vor allem physische Sicherung der Maschine, ggf. Folterresistenz usf. All das braucht umfangreiche Kenntnisse und viel Geduld. Zum Glück ist das im Augenblick in der Regel nicht nötig – wir sind kein Geheimdienst.

Mit der Datenhygiene ist das was ganz anderes – hier geht es darum, die Kosten für Daten hochzutreiben. Ziel ist, Staat und Wirtschaft nicht unnötig Daten zu schenken oder jedenfalls mit nur geringen Investitionen zugänglich zu machen, um sie daran zu hindern, Data Mining (das ist quasi Rasterfahndung mit wissenschaftlichen Mitteln) zu machen, über allerlei Zufallsfunde seltsame Theorien zu entwickeln oder ähnliches.

Hier hilft schon etwas Wissen, gesunder Menschenverstand und manchmal auch etwas Software.

U

## Die goldene Regel: Nutzt euer Hirn.

□ Das bedeutet einerseits, dass ihr auch am Rechner erst überlegen und dann handeln solltet – insbesondere solltet ihr keinen OK-Klick-Reflex haben und lesen, was euch der Rechner sagt (ich gebe zu, dass das speziell unter Windows oft etwas nervt). Es bedeutet auf der anderen Seite, dass ihr wenn irgend möglich nicht einfach mal Sachen probiert und pfriemelt, sondern dass ihr verstehen solltet, was ihr wann tut und was es bedeutet (ich gebe zu, dass auch das speziell unter Windows oft eine frustrierende Zumutung ist).

Es gibt noch ein paar weitere einfache Regeln, die eigentlich alle aus der Master-Regel folgen. Dazu gehören etwa:

- Seid nicht gierig – es mag ja nett sein, 150 raubkodierte Spiele auf der Platte zu haben, wirklich nützlich ist es nicht, und es erhöht jedenfalls die Wahrscheinlichkeit, dass ihr unnötigen Ärger bekommt und Daten preisgebt.
- Seid im Netz so misstrauisch wie im realen Leben – den Leuten, die euch im Supermarkt Unfug andrehen müssen, gebt ihr auch nicht beliebig eure Adresse. Im Netz redet ihr immer mit Computern, und die haben ein weit besseres Gedächtnis als die Drucker. Seht euch also an, wer da was macht, bevor ihr irgendwelche Netzdienste benutzt. Informationen, die ihr nicht auch an euren Hauseingang hängen würdet (Urlaubsfotos?) haben auf Webseiten meistens nichts verloren. Vergesst nicht, dass auch der Staatsschutz googlen kann (oder das jedenfalls in ein paar Jahren gelernt haben wird).
- Schaut, dass euer Spieltrieb nicht eure Kenntnisse überholt – nur weil ihr irgendeinen Kram einfach durch Ok-Klicken installieren könnt, heißt das noch lange nicht, dass es eine gute Idee ist, das zu tun. Überlegt euch vorher, ob ihr etwas braucht, bevor ihr es installiert.

U

## 2. Die eigene Maschine I

- ⌋ Der typische Angriff der Staatsgewalt auf einzelne Rechner ist vorläufig die Beschlagnahme. Bei Hausdurchsuchungen gehen heute ganz üblich die Rechner, Mobiltelefone und PDAs mit. Einen Rechner gegen eine Beschlagnahme zu sichern ist jedenfalls extrem schwierig – mit euren Daten mag das eine andere Sache sein.

Zunächst wollt ihr aber selbst wenig Datenspuren hinterlassen und es anderen jedenfalls nicht allzu leicht machen, sich auf eurem Rechner umzusehen. Was dazu zu tun ist, ist praktischerweise nicht weit von dem entfernt, was ihr als gute BürgerInnen des Netzes ohnehin tun wollt und läuft grob unter „Rechnersicherheit“. Hintergrund ist, dass sich zwar der Staat unseres Wissens noch nicht aktiv im Bereich von Datensammeln durch die Hintertür betätigt, dass allerdings Daten, die Private haben, schnell (z.B. anlässlich einer Rasterfahndung) staatliche Daten werden können.

- ⌋ Viele Programme werden zur „Sicherheit“ auf dem Rechner empfohlen. Viele davon haben eher die Wirksamkeit von Kameraüberwachung.
- ⌋
  - Virenchecker – in den meisten Fällen sinnvoll, wenn auch Menschen, die die Goldene Regel befolgen, keine CPU-fressende Online-Überwachung brauchen und einfach einmal am Tag oder so die Platte durchscannen lassen sollten. Ansonsten ist das Virenproblem eher gering, wenn mensch nicht Outlook und nicht MS Word verwendet und die Hinweise unten beachtet.
  - ⌋
    - Personal Firewalls – Quatsch, es sei denn, ihr wärt NetzwerkspezialistInnen und könntet wirklich kompetent beurteilen, ob es ok ist, wenn das Programm `unix.srv` auf Port 515 und die Maschine 134.254.222.5 auf Port 22 zugreift.
    - ⌋
      - Webwasher – das sind Programme, die beispielsweise die Übertragung von Cookies oder Referrern unterdrücken, Javascript filtern usw. Das ist nicht schlecht, taugt aber nur, wenn mensch nicht die Kontrollen sukzessive wieder abstellt, weil irgendwelche Webseiten damit nicht mehr funktionieren.
      - ⌋
        - Verschlüsselungsprogramme – richtig eingesetzt ist sowas prima. Leider wird und wurde da viel Mist verkloppt, und so oder so kann auch das beste Verschlüsselungsprogramm nichts gegen ungeschicktes Datenmanagement tun.

**Grundsatz: Kein Programm ersetzt Nachdenken**

## 3. Die eigene Maschine II

Sinnvolle Maßnahmen zur Sicherung der eigenen Maschine:

- ⌋
  - Updates einspielen – das ist die wichtigste Maßnahme überhaupt. Macht regelmäßig euer Windows-Update, das `apt-get update && apt-get -u upgrade` oder was immer euer System braucht. Speziell unter Windows handelt mensch sich dabei zwar des öfteren unglaubliche Lizenzbestimmungen bis hin zur Autorisierung für Microsoft, sich nach Belieben auf der Maschine umzusehen, ein, aber wer Windows verwendet, sollte sich daran nicht stören.
  - ⌋
    - „Aktive“ Inhalte wann immer möglich ausschalten. Leider gibt es von denen immer mehr, weil sie natürlich allerlei Magie ermöglichen. Viele Webseiten, selbst „Textverarbeitung“ gehen nicht mehr ohne. Fragt euch selbst, ob ihr das jeweils haben wollt und aktiviert es nur, wenn ihr diese Frage mit Ja beantwortet. Aktive Inhalte sind:
      - ActiveX unter Windows – das sollte immer aus sein, es gibt keinen guten Grund für Unfug dieser Art
      - Javascript – hier bauen viele Webseiten darauf, dass Javascript läuft, so dass ein komplettes Abschalten häufig unbequem ist. Auf jeden Fall sollte die Ausführung von Javascript für HTML in E-Mails aus sein. Übrigens sollte auch die Verwendung von Plugins in HTML für E-Mails immer verboten sein.

- VBA-Kram – Makros in Office-Dokumenten sind eine endlose Krankheit (hier hilft übrigens auch nicht, auf Openoffice oder ähnliches umzusteigen). Schaltet, wo möglich, „Makros“ für Office-Kram aus und tauscht Dateien nicht in Office-Formaten aus.
- Java – Java ist eine ganz ordentliche Technologie und normalerweise eher harmlos. Allerdings gilt auch hier: In Mails haben Java-Applets nichts verloren.
- Flash/Shockwave – als proprietäre Technologien sind die ohnehin nicht so prall, wenn der Kram vom Netz kommt, ist nach unserer Kenntnis die Gefährdung nur unwesentlich höher als bei Java.

U

- Automaten wann immer möglich ausschalten – dazu gehört insbesondere das automatische Interpretieren von Mail-Attachments, das Einfallstor Nummer Eins für Viren und Würmer. Wenn ihr zu faul seid, ein Attachment manuell zu bearbeiten, solltet ihr auch zu faul sein, den Rechner einzuschalten. Blöd ist weiter, automatisch Programme von CD starten lassen, wenn eine eingelegt wird (auf die Weise hat sich z.B. der Sony-Rootkit verbreitet).

U

- Im Zweifel die hässlichere Darstellung wählen – Klassiker hierbei ist die Unart von Windows Explorer oder Outlook, die Datei-Erweiterungen nicht anzuzeigen, so dass eine Datei bla.gif.exe nur als bla.gif erscheint. Schaltet dieses Verhalten unbedingt aus, wenn ihr schon so einen Monk verwendet.

U

- Keine HTML-Mail – wenn euer Mailprogramm erlaubt, zwischen HTML- und Textdarstellung zu wählen (die wenigsten tun das), wählt in jedem Fall Text. HTML ist in Mails überflüssig wie ein Kropf und ist eine kaum versiegende Quelle von Sicherheitslücken. Verschickt natürlich auch selbst keine HTML-Mails. Wenn ihr welche bekommt, pöbelt die AutorInnen an.

U

- Keine Office-Dokumente verschicken – dazu kommen wir noch unten.

□

- Cookies kontrollieren – Cookies sind an sich erstmal nicht wild, es handelt sich einfach um ein paar hundert Byte, die eine Webseite bei euch hinterlegt und die ihr danach bei jedem Zugriff wieder geschickt werden. Damit *kann* mensch nette Dinge tun, aber auch reichlich blödes Zeug (z.B. werden Cookies auch zu Bildern übertragen; platziert nun eine Werbeagentur auf möglichst vielen Webseiten Bilder, kann sie, wenn ihr Referrer nicht unterdrückt, erfassen, auf welchen Webseiten ihr wart). Ihr solltet das automatische Setzen von Cookies sperren und euch für jeden Cookie fragen lassen, ob ihr ihn haben wollt.

U

- Hardware-Router – die üblichen DSL-Router sind so konfiguriert, dass Maschinen von außen nur dann Zugang auf eure Mühle geben, wenn ihr die betreffenden Maschinen vorher schon „angerufen“ habt. Das ist eine sinnvolle Maßnahme, und die DSL-Router sind noch dazu recht praktisch. Sie kosten nicht viel, kauft euch einen (wenn ihr DSL habt...)

U

## 4. Eigene Daten: Verschlüsselung

Für eure eigenen Daten lohnt sich unter Umständen eine lokale Verschlüsselung. Die Verschlüsselungsfunktionen der üblichen Office-Pakete sind meistens Quatsch.

- ⊞ Ihr könnt mit PGP und gnupg einzelne Dateien verschlüsseln, das kommerzielle PGP kommt mit einem Programm zur Verschlüsselung einer ganzen Partition. Anderen Verschlüsselungsprogrammen solltet ihr nur trauen, wenn ihr wisst, was sie tun – es ist leicht, beim Design oder der Implementation kryptographischer Software Fehler zu machen, die den ganzen Zirkus unwirksam machen, und das kann, wenn man sich auf die Verschlüsselung verlässt, schlimmer sein als gar keine Verschlüsselung.

Klar ist, dass ihr den Schlüssel (das „Passwort“) besser nicht auf den Rechner klebt. . .

- ⊞ Besser als verschlüsselte Daten sind allerdings Daten, die gar nicht mehr auf dem Rechner sind. Nutzt die Möglichkeit, sensible Daten auszulagern, etwa auf USB-Sticks, und hebt sensible Daten nicht länger auf als nötig.

Es gibt wilde Geschichten, wie richtig zu löschen sei. Tatsache ist, dass abhängig von verwendeten Dateisystem gelöschte Dateien noch eine Weile mit Bordmitteln rekonstruierbar bleiben können. Mit erheblichem Aufwand können selbst mehrfach überschriebene Daten wiederhergestellt werden. Für Rechner, die die Polizei einfach so aus Spaß mitnimmt, wird wenigstens Letzteres garantiert nicht gemacht, weil es teuer ist und die Platte dabei in der Regel zerstört wird.

Für den täglichen Betrieb ist die Löschfunktion des Betriebssystems dennoch meist ausreichend. Wenn ihr, etwa nach der Verteilung von Fluggis zweifelhafter Legalität, schon mit einer Hausdurchsuchung rechnet, lohnt sich eine sorgfältigere Löschung mit entsprechenden Hilfsprogrammen – für moderne Betriebssysteme und Oberflächen ist es allerdings häufig recht schwierig, alle Stellen zu finden, an denen mal kritische Daten standen, solche Maßnahmen sollten also nicht überbewertet werden.

- ⊞ Andererseits könnt ihr wetten, dass die Staatsgewalt als erstes in den „Papierkorb“ oder ähnliche Löschrückstellungen guckt. Deren „Leerung“ ist also mal eine wirklich gute Idee.

## 5. Eigene Daten: Formate

Verwendet, wann immer möglich, schlichten Plain Text (notepad erzeugt sowas, für Tabellen kommt z.B. csv in Frage). Nur dabei wisst ihr wirklich, was der Rechner speichert bzw. überträgt.

- ⊞ In Office-Dateien werden regelmäßig Metadaten gespeichert, die Rückschlüsse auf die AutorInnen der Dateien zulassen (der Autor des Iloveyou-Wurms wurde auf diese Weise gefangen).

Wenn ihr unbedingt formatierten Kram austauschen wollt, nehmt PDF oder HTML o.ä., in der größten Not RTF (und guckt mit einem Editor nach, was euer Programm dort so reinschreibt).

- ⊞ Es gibt übrigens viele weitere gute Gründe, keine Office-Dateien auszutauschen, nicht zuletzt, dass mensch eben die zugehörigen Programme braucht, um etwas mit solchen Dateien anfangen zu können. Das ist heute ein Problem für die, die mit Windows nichts zu tun haben wollen, und in zehn Jahren ist es ein Problem für alle. Also: Wenn ihr schon meint, auf Word nicht verzichten zu können, behaltet die Dateien, die ihr damit erzeugt, wenigstens für euch.

In dieser Hinsicht ist übrigens Openoffice den Microsoft-Alternativen deutlich vorzuziehen, weil sein natives Format dokumentiert ist und auch ohne Openoffice recht einfach zu verarbeiten ist.

⊞

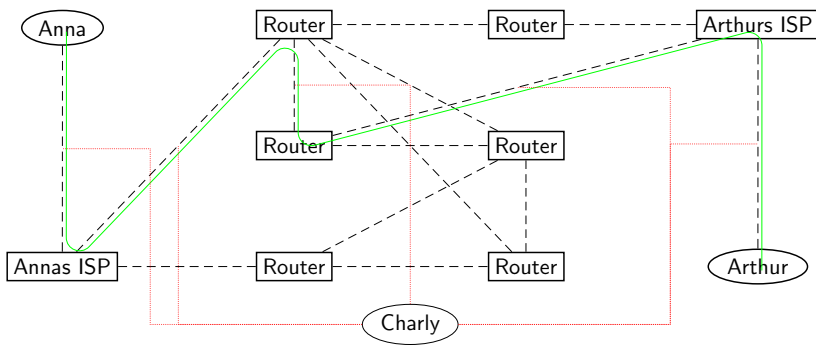


Fig. 1

## 6. Eigene Daten: Spuren

Euer Rechner speichert häufig, was ihr so tut – welche Webseiten ihr besucht, welche Programme ihr gestartet, was ihr in Formulare eingetragen habt.

- Seid euch bewusst, dass diese Daten existieren und ausgewertet werden, wenn eure Kiste beschlagnahmt wird. Versucht, sie regelmäßig zu löschen. Firefox hat z.B. unter Edit/Preferences/Privacy ein „Clear all information stored while browsing“. Andere Programme, Windows selbst eingeschlossen, haben sowas nicht, und man ist da etwas ausgeliefert. Für Unix-Shells und Editoren wie vim hingegen kann die Speicherung solcher Infos ganz unterbunden werden – ihr solltet das auf jeden Fall tun, wenn ihr damit rechnet, mit der Staatsgewalt in Konflikt zu kommen.
  - Wenn ihr Unix-Systeme habt, sorgt dafür, dass euer logrotate die Daten rasch löscht.
- Wenn ihr selbst Kram ins Netz stellt, tut das, wo ihr wisst, dass die Leute verantwortlich mit Logs umgehen. Nadir ist ein guter Tipp.

## 7. Das Netz

(vgl. Fig. 1)

Das Netz besteht aus vielen Teilen, zwischen denen Router Pakete verschieben.

- Im Bild möchte Charly die Verbindung zwischen Anna und Arthur überwachen. Er kann dazu an vielen Stellen ansetzen (rote Linien).
- Die übliche legale Überwachung ist aber an Personen gebunden. Wird Anna überwacht, wird normalerweise eine „Black Box“ (ein Überwachungsrechner) an der Leitung von Annas ISP (Internet Service Provider, also der Laden, der euch mit Netzzugang versorgt) in den Rest des Netzes aktiv. ISPs sind verpflichtet, derartige Geräte vorzuhalten, reden aber meist nicht gerne darüber.
- Es gibt allerdings etliche Variationen dieses Themas. Macht Anna etwa Webmail über web.de, so wird die Black Box von web.de die Mails speichern.
- Polizei und VS dürfen sich (noch) nicht auf Backbones (das sind Leitungen zwischen den Routern) setzen und dort alle Daten durchscannen. Es ist davon auszugehen, dass sie sich an diese Regelungen halten.
- Der BND darf sich auf Leitungen ins Ausland setzen und dort scannen. Es ist davon auszugehen, dass er das tut.
- Beim Scannen ist alles von der Schlüsselwortsuche bis zur Erfassung von Kommunikationsprofilen und Data Mining darin denkbar. Was wirklich passiert, wissen wir nicht (das ist der Trick bei Geheimdiensten).

## 8. Vorratsdatenspeicherung

Bei der Vorratsdatenspeicherung werden die Kommunikationsdaten aller NutzerInnen flächen-deckend für mindestens sechs Monate gespeichert.

Vorläufig sollen diese Daten nur für rückwirkende personenbezogene Anfragen verwendet werden.

Richtig spannend werden diese Daten aber erst, wenn auf ihnen Data Mining betrieben wird.

U Ich nehme Wetten an, dass dies beim nächsten eine Rasterfahndung rechtfertigenden Anlass geschehen wird.

Gespeichert werden nach der gegenwärtigen EU-Richtlinie Mail- und VoIP-Verbindungen, wobei die Definition im Gesetz eher seltsam gehalten ist.

U Wie sollen wir mit der Vorratsdatenspeicherung umgehen? Es ist schwierig, der Erfassung von Verbindungsdaten zu entgehen (insbesondere helfen Anonymizer dabei nur dann, wenn die Verbindung mit ihnen verschlüsselt abläuft). Ansätze dazu gibt es (Mixmaster, Tor), aber sie sind vorläufig nur für Leute brauchbar, die es ernst meinen.

Daher: Die Vorratsdatenspeicherung wäre ein prima Kandidat für eine politische Kampagne gegen Überwachungswut. Ob sie wirklich noch zu stoppen ist, ist offen, aber es wäre wirklich gut, es wenigstens zu versuchen.

## 9. Verschlüsselung am Netz

Verschlüsselung ist sinnvoll, weil sie der Staatsgewalt den Zugang zu Kommunikationsinhalten jedenfalls um Größenordnungen erschwert.

U • Für Mail: PGP – es hat sich mittlerweile herumgesprochen, dass das eine gute Idee ist. Allerdings müssen beide Seiten mit PGP umgehen können, und es braucht eine Infrastruktur zum Schlüsselaustausch. Die Mühe damit ist vor allem sozialer Natur.

U • Fürs Web: https – praktisch alle Browser unterstützen das – es muss aber auch der Server unterstützen. Solange die URL eindeutig die Inhalte bezeichnet, ist https relativ wertlos (die Staatsgewalt kann sich die Seiten ja normalerweise auch ansehen), im Zusammenhang mit Formularen u.ä. sollte es aber verwendet werden, wann immer möglich.

U • Weitere Einzelprotokolle – zum Mailabruf gibt es z.B. pops (was nicht so arg nützlich ist, wenn ihr PGP verwendet, es sei denn, um die Authentifizierung zu schützen), zum Mailverschicken Erweiterungen von smtp, fürs remote login ssh (das ihr aus vielen Gründen unbedingt verwenden solltet, wenn ihr sowas tut). Schließlich: Wenn ihr eure Webseiten immer noch mit ftp pflegt, stellt so bald als möglich auf sftp um (das setzt auf ssh auf).

U • Für alles: Tor – Tor wird irgendwann mal ein Netzwerk von Servern sein, die Daten verschlüsselt austauschen und dabei auch noch für das verwischen von Verbindungsdaten sorgen. Vorerst aber ist die Verwendung von Tor mit erheblichen Einbußen an Komfort und Geschwindigkeit verbunden.

## 10. Zum Abschluss

Überwachung in erster Linie ein politisches Problem und sollte politisch bekämpft werden.

Trotz allem: Keine Panik!

Wer sich Arbeit sparen möchte: Es ist gar nicht so dumm, den eigenen Rechner nicht ans Netz zu hängen, alle eigenen Daten auf einem USB-Stick zu halten und bei Bedarf ins Internetcafe zu gehen.

Weitere Infos und Links auf <http://www.datenschmutz.de>

Links zu sinnvollen Programmen:

<http://www.argh-it.de/crypto/>