Karin Schuler

Wer nicht kämpft, hat schon verloren

Dieses Zitat von Bert Brecht, besser gesagt: sein zweiter Teil, kommt mir in letzter Zeit häufiger in den Sinn, wenn ich Diskussionen über die Auswirkungen der geheimdienstlichen Ausspähskandale führe. Was kann man angesichts immer neuer Erkenntnisse über das Ausmaß der Überwachungsmaßnahmen überhaupt noch tun? Welche Chancen hat man gegenüber einer offensichtlich mit unbegrenzten Finanzmitteln ausgestatteten Hydra, die sich Rechenzentren, Supercomputer und Energie mit beliebigem Potenzial leisten kann? Welche Hoffnung kann man angesichts einer hilflos bis devot agierenden politischen Klasse noch haben, dass unseren Vorstellungen von Grundrechtsschutz wieder Geltung verschafft wird?

Was an politischer Einflussnahme nötig ist, soll hier nicht erörtert werden. Vielmehr ein Aspekt, der in der Diskussion immer noch sehr knapp wegkommt: nämlich die Einflussmöglichkeiten jedes und jeder Einzelnen. Wir dürfen uns nicht erschreckt zurücklehnen: weder der Gesetzgeber noch Fatalismus bringen uns unsere Grundrechte zurück, wenn wir nicht auch die Möglichkeiten des Selbstdatenschutzes ausschöpfen.

Ohne Ölspur durchs Internet

Natürlich ist es einfach, den neuen Laptop oder das schöne Tablet einfach mit den Voreinstellungen zu nutzen, die es von zu Hause aus mitbringt. Es funktioniert ja auch alles. Leider sind die Endgeräte bei der Hatz durchs Internet aber ziemlich undicht. Eine breite Spur zieht sich hinter uns her, wenn wir Seiten besuchen, Suchmaschinen abfragen oder Waren bestellen. Wen interessiert, welche Spuren man auf dem virtuellen Asphalt hinterlässt, dem sei das Firefox-Plug-In *Lightbeam*[1] empfohlen. Dieses Tool zeigt, grafisch aufbereitet, welche Seiten man besucht hat – und, viel aufschlussreicher, welche davon man gar nicht selbst aufgerufen hat, sondern die über eine besuchte Website unbemerkt dazugeschaltet wurden. Lässt man Lightbeam ein paar Tage mitlaufen, erreicht der visualisierende Graph eine beeindruckende Größe. Für Aha-Effekte sorgt auch das Plug-In *Ghostery*[2], das anzeigt, welche Tracking-Programme auf der jeweils aktuellen Seite *versteckt* sind. Es erlaubt sehr komfortabel per Schiebeschalter das Ein- und Ausschalten jedes Trackingdienstes. Achtung: von der Aktivierung von *Ghostrank* sollte abgesehen werden, da nicht hinreichend geklärt ist, wer die resultierenden Nutzungsdaten von *Evidon*, der Firma hinter Ghostery erhält.

Wem bei den gewonnenen Erkenntnissen mulmig wird, der kann sich der Hilfe diverser Tools bedienen, die die Geschwätzigkeit des eigenen Browsers zumindest eindämmen. *NoScript*[3] ermöglicht das gezielte, seitenbezogene An- und Ausschalten von JavaScript und Java und schützt so nicht nur vor unerwünschten Skripten sondern auch vor den Auswirkungen von Sicherheitslücken der Skriptsprachen. *BetterPrivacy*[4] schützt vor den umgangssprachlich als *Super-Cookies* bezeichneten *local shared objects (LSO)*, einer besonders unerfreulichen Form der Dateninvasion auf der Festplatte: der Flashplayer legt dabei kleine Infodateien in zentralen Ordnern des Rechners ab, ohne dass sie in der Standard-Browserverwaltung als Cookie erkannt werden. Ein Plug-In, das ursprünglich für Webentwickler gedacht war, ist *Counterpixel*[5]. Es sollte die Platzierung von Zählpixeln auf Webseiten erleichtern, indem erkannt wird, welche Tracking- oder Statistiksoftware eingesetzt wird. Auch wenn, dem ursprünglichen Zweck entsprechend, kein Blockieren von Zählpixeln angeboten wird, bringt das Tool einen Transparenzgewinn: Von *eTracker* über *Google Analytics* und *IVW* zu *PIWIK* und vielen weiteren wird angezeigt, welche Dienste Zählpixel versteckt haben.

Wen die Erkenntnisse aus dem Lightbeam-Graphen erschrecken, der sollte sich einen Überblick über domainübergreifende Anfragen verschaffen. Meist bleibt man nicht auf der Seite *xyz.de*, wenn man diese aufgerufen hat. So genannte *cross-site-requests* sind zu einem massenhaft auftretenden Phänomen geworden, seit Schriften, Medien und andere Objekte von Drittseiten nachgeladen werden. Wer lieber selbst kontrolliert, welchen Seiten er die Unterverweisung erlauben will und welchen nicht, der sollte sich das sehr mächtige Plug-In *RequestPolicy*[6] ansehen. Dessen Einsatz ermöglicht die vollständige Kontrolle über Nachladevorgänge und schützt bei restriktiver Einstellung vor *Cross-Site-Scripting*-Angriffen, bei denen durch untergeschobenen Aufruf einer URL Schadcode auf dem Rechner des Nutzers ausgeführt wird.

Eine gute Informationsquelle zum Thema Tracking findet sich auf den Seiten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.[7]

Nur Max Mustermann war da

Wem auch die beschriebenen Maßnahmen nicht ausreichen, kann auf die verfügbaren Anonymisierungsdienste zurückgreifen und sich so weitgehend unsichtbar machen. Auch wenn es Grenzen der durch diese Dienste gewährten Anonymität gibt, wirkt die Vermeidung von profilgebenden, personenbezogenen Daten grundsätzlich persönlichkeitsschützend.

Da man dem Anbieter des Anonymisierungsdienstes vertrauen muss, fühlt sich wahrscheinlich nicht jede/r mit allen auf dem Markt befindlichen Produkten gleichermaßen wohl. Zwei kostenlose Angebote, die sich in der Netzgemeinde großen Vertrauens erfreuen, sollen beispielhaft genannt werden.

JAP[8], eine kostenlose Softwarelösung, die im Rahmen des Projekts *AN.ON (Anonymity Online)* entwickelt wurde, ist leider nicht die schnellste, genießt aber einen untadeligen Ruf. Hat man die Software installiert, führen eigene Webseitenaufrufe nicht mehr zu einer direkten Anfrage beim zugehörigen Server. Stattdessen wird der Aufruf in ein Netzwerk teilnehmender Verteilserver (Mixe) geschickt und darin mehrfach weitergeleitet, ehe die Anfrage beim eigentlich angefragten Server landet. Dieser sieht jedoch nur noch die IP-Adresse des letzten Verteilservers und kann keine Rückschlüsse auf den anfragenden Nutzer

mehr ziehen. Schöner Effekt: Keiner der beteiligten Mixe kann Rückschlüsse auf einzelne Nutzer ziehen, da er jeweils nur weiß, von welchem vorigen Mix die Anfrage kam und wohin er sie weiterleiten soll. Die Nutzer können die zur Verfügung stehenden Mixe bzw. deren Betreiber einsehen und gezielt eigene Mixkaskaden auswählen.

Eine weitere gut beleumundete Open-Source-Lösung bietet das *TOR-Netzwerk*[9], das grundsätzlich ähnlich wie JAP arbeitet, die Anfragen von Nutzern aber mittels *onion routing* aufteilt und weiterleitet. Hierbei werden keine festen Routen über Mixe verwendet (Mix-Kaskaden) sondern die Route wird jeweils individuell neu festgelegt.

Beide Verfahren haben aus Sicherheitssicht Vor- und Nachteile: der Zentralismus der Mix-Kaskaden schützt besser vor schleichender Übernahme von Verteilservern durch Anbieter, die als Maulwurf agieren. Andererseits bietet die größere Verteilung und Verschleierung der Übertragungswege beim *onion routing* weniger Angriffsfläche, falls einzelne Server angegriffen werden.

Googlen ohne Google

Was haben *Tempo*, *Knirps*, *Uhu*, *Maggi* und *Google* gemeinsam? Bei allen handelt es sich um so genannte generalisierte Markennamen: der Markenbegriff wird als Bezeichnung für eine ganze Produktgruppe verwendet. Nun weiß jeder, dass es Konkurrenzprodukte für Taschentücher, Taschenschirme und Suppenwürze gibt. Dass man jedoch auch ohne Googles Suchmaschine *googlen* kann, hat sich noch nicht weit genug herumgesprochen.

Dabei gibt es schon seit vielen Jahren datenschutzfreundliche Alternativen zu datenhungrigen Suchdiensten wie Google, Bing, Yahoo und Co.

Zu den Pionieren auf diesem Gebiet zählen die Dienste der Firma IxQuick, die zweierlei Suchmaschinen anbietet: *Ixquick*[10], eine Metasuchmaschine und *Startpage*[11], ein Proxydienst für die Suche über Google. Beide speichern keine IP-Adressen und vermeiden so die Profilbildung anhand der durchgeführten Suchanfragen.

Die Dienste sind gut in Browser integrierbar und bieten hohe Qualität. Es gibt also keinen Grund, sich weiterhin beim Namensgeber Google aushorchen zu lassen.

Passworte gehören in den Tresor

Wie viele unterschiedliche Passworte benötigt man als Nutzer?

Schätzungsweise hat ein durchschnittlicher Nutzer zwischen 50 und 200 Zugänge, wovon einige vielleicht nur ein einziges Mal genutzt werden (weil man z. B. kein zweites Mal in einem Online-Shop einkauft). Kommt in Diskussionen die Rede auf die Anzahl verwendeter Passwörter, hat man jedoch meist schnell das Gefühl, dass vielen Leuten vier bis fünf unterschiedliche ausreichen, um eine große Anzahl von Zugängen zu schützen.

Alternative zum Kämpfen? Foto: Benjamin Kees

Die jüngste Alarmmeldung des BSI[12], dass eine Datenbank mit Zugangsdaten entdeckt wurde, die 16 Mio. Einträge enthält, ist da nur ein besonders eindrucksvoller Fall.

Die Antwort auf die Eingangsfrage muss daher lauten: So viele, wie man persönliche Zugänge hat. Seien es Zugänge zu Rechnern, Online-Shops, Bank-Portalen, Online-Netzwerken, Cloud-Anwendungen, Providern, Nutzerportalen oder sonstigen Dienstleistungen: Jeder sollte ein eigenes Passwort haben. Denn sobald ein Zugang kompromittiert und das Passwort bekannt wurde, ist dieses *verbrannt*. Insbesondere in Fällen, in denen der Benutzername aus einer E-Mail-Adresse besteht, kann der Besitzer geknackter Passwörter auf die Person rückschließen und so deren weitere Zugänge ausprobieren. Wurde dann mehrfach das gleiche Passwort verwendet, sind auch alle anderen Zugänge mit diesem Schlüssel kompromittiert.

Aber wie schafft man den Spagat, einerseits gute Passworte zu verwenden (größer als 8 Stellen, Ziffern, Sonderzeichen, Groß- und Kleinschreibung), die in keinem Wörterbuch stehen (damit man sie nicht mittels *Wörterbuch-brute force*-Angriff errechnen kann) und sich andererseits diese Passworte so zu merken, dass man sie im Bedarfsfalle kennt, ohne sie auf gelbe Zettel an den Bildschirm zu kleben?

Die Helfer, die einem zur Lösung dieses Problems dienen, nennen sich Passworttresore. Die Idee ist recht einfach: man legt seine Benutzername/Passwort-Kombinationen im Regal eines durch starke kryptografische Verfahren gesicherten Containers ab und sorgt dafür, dass der einzige Schlüssel zum Container einen hohen Sicherheitsstandard hat. Diesen Schlüssel trägt man nur bei sich und nutzt ihn ausschließlich kurzzeitig um den Container zu öffnen, ein Passwort in einer Schublade des Regals nachzuschlagen und dieses zu verwenden. Der Container hat eine Türe, die sofort nach Verlassen automatisch zurück ins Schloss fällt. Noch besser: im Container befindet sich ein Generator, der einem gute Passworte im obigen Sinne erzeugt und sofort in die Schublade für einen neuen Zugang legt.

Eines der Programme, die so funktionieren, wurde von *Bruce Schneider* entwickelt, einem der bekanntesten Kryptografie-Experten. Er ist außerdem seit vielen Jahren bürgerrechtlich im Vorstand der *Electronic Frontier Foundation* engagiert und ist bei der Zeitung *The Guardian* Mitglied des Redaktionsteams, das Ed Snowdens Unterlagen sichtet und beurteilt.

Passwordsafe[13] bietet einem die Möglichkeit, komfortabel für jeden Zugang ein eigenes, gutes Passwort zu generieren und sicher abzulegen. Der Generalschlüssel, der den Zugang zum Safe ermöglicht, sollte lang und komplex sein. Aber da man sich nur diesen einen Schlüssel merken muss, sind sowohl Sicherheits- als auch Komfortgewinn enorm.

Keine Postkarten für die Späher

Jeder hat den Spruch schon mal gehört: „Eine E-Mail ist einer mit Bleistift geschriebenen Postkarte vergleichbar." Obwohl vermutlich niemand seiner Freundin heikle Krankheiten auf Postkarte mitteilen würde, haben viele Menschen keinerlei Skrupel, dies in aller Ausführlichkeit per E-Mail zu tun. Das Gefühl, dass man selbst nicht durchblickt, wie die Mail vom eigenen Rechner auf den Rechner des Freundes gelangt, führt anscheinend zur trügerischen, unreflektierten Überzeugung, dass das auch sonst niemandem gelingt. In IT-Fachkreisen wiederum begegnet man teilweise einer Art von Fatalismus, der in der Ansicht „ist doch eh alles knackbar" gipfelt. Beiden Haltungen ist gemein, dass sie passiv und uninformiert vermeiden, das Heft in die eigene Hand zu nehmen. Selbstdatenschutz sieht anders aus!

Zugegeben: die ergonomische Güte von E-Mail-Verschlüsselungsprogrammen ist noch immer ausbaufähig, aber die Zeiten unbedienbarer Produkte sind vorbei. Unabhängig von Betriebssystem und Mailprogramm stehen Verschlüsselungsmöglichkeiten zur Verfügung, die durch gewissenhaften Gebrauch durchaus Sicherheit vor unerwünschten Lauschern bieten.

Beispielhaft sei auf das gut zu handhabende und kostenlose Distributionspaket *GnuPG-Pack*[14] für Windows hingewiesen, das die offene Version der Verschlüsselungstechnik *pretty good privacy (pgp)* ermöglicht und Schlüssel größer als 4096 bit erzeugen kann. Ein Plug-In für die Mail-Software Thunderbird ist ebenfalls enthalten, so dass per Mausklick ver- und entschlüsselt werden kann.

Für Outlook-Nutzer bietet das Distributionspaket *Gpg4win*[15] ein Plug-In für die Mailsoftware Outlook.

My computer is my castle

Ergänzend zu den asymmetrischen (*public-key*-)Verfahren, bei denen jeder Teilnehmer zunächst ein Schlüsselpaar erzeugen muss, um am verschlüsselten Datenaustausch teilzunehmen, gibt es auch Verfahren der symmetrischen Verschlüsselung. Symmetrische Verfahren kommen aufgrund der Sensibilität ihrer Schlüssel meist in anderen Einsatzbereichen zum Einsatz, zum Beispiel bei der Sicherung von Daten auf der eigenen Festplatte. Gerade bei Laptops oder anderen mobilen Geräten oder Medien (USB-Sticks!), die jährlich in großer Zahl verloren gehen, ist die Sicherung der darauf enthaltenen Daten durch Verschlüsselung sehr zu empfehlen. Nicht nur bei Verlust des Rechners muss man sich so wenigstens keine Sorgen um die Vertraulichkeit der Daten machen, sondern auch beim Bewegen im Internet lassen sich definierte Bereiche der Festplatte so für die Dauer der Online-Verbindung vor unberechtigtem Zugriff schützen.

Eines der Programme, die kostenlose Festplatten-, Container- oder Ordnerverschlüsselung anbieten, ist **Truecrypt**[16], ein Tool, dessen Quellcode verfügbar ist (auch wenn es nicht vollständig der open-source-Definition entspricht).

Was bringt's?

Wer die vorstehend skizzierten Möglichkeiten nutzt, um sich und seine Daten nicht mehr auf dem Präsentierteller anzubieten, hat schon einiges in Sachen Selbstdatenschutz getan. Weitere Schritte können folgen, indem Chats gesichert, sichere Cloud-Austauschdienste verwendet oder Webcams deaktiviert werden.

Natürlich stellen die beschriebenen Maßnahmen und Mechanismen alleine kein Allheilmittel dar, um uns vor der Datengier von Geheimdiensten und profitierenden Wirtschaftsunternehmen zu schützen. Aber umgekehrt reicht der Weg über politische Einflussnahme alleine dazu auch nicht aus. Und vor allem sind die darauf erzielten Schritte sehr kurz, schwerfällig, und nicht immer auf das Ziel des Grundrechtsschutzes ausgerichtet. Wir müssen daher Eigenverantwortung übernehmen, uns aus dem Status des *blinden Nutzers* befreien, lernen, was wir tun, wie wir es tun und wie wir uns dabei bestmöglich selbst schützen können. Für diejenigen, die in der IT arbeiten, gilt es, das Wissen über Schutzmöglichkeiten möglichst breit unter nicht-fachkundigen Nutzern zu verbreiten – und selber mit gutem Beispiel voranzugehen.

Natürlich gibt es keine Garantie, dass wir uns auf diese Weise vor den Zudringlichkeiten selbst ernannter *Bedarfsträger* schützen und natürlich kann ohne wirksame staatliche Durchsetzung von Grundrechten kein vollkommener Schutz entstehen. Aber wo man sich selbst helfen kann, sollte man es auch tun, und für den Rest sollte es so schwer wie möglich sein, jedermanns Daten *einfach so* abzuzapfen. Getreu Brechts Motto: *Wer kämpft, kann verlieren. Wer nicht kämpft, hat schon verloren*.

Karin Schuler

Karin Schuler ist Vorsitzende der Deutschen Vereinigung für Datenschutz e.V., langjähriges FIfF-Mitglied, Beraterin für Datenschutz und IT-Sicherheit und vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannte Sachverständige für IT-Produkte.
Kontakt: *buero@schuler-ds.de · www.schuler-ds.de*

Anmerkungen

1 *https://www.mozilla.org/de/lightbeam/*
2 *https://www.ghostery.com*
3 *https://addons.mozilla.org/de/firefox/addon/noscript/*
4 *https://addons.mozilla.org/de/firefox/addon/betterprivacy/*
5 *https://addons.mozilla.org/de/firefox/addon/counterpixel/*
6 *https://addons.mozilla.org/de/firefox/addon/requestpolicy/*
7 *https://www.datenschutzzentrum.de/tracking/*
8 *http://anon.inf.tu-dresden.de*
9 *https://www.torproject.org*
10 *https://ixquick.com/deu/*
11 *https://startpage.com/deu/*
12 *https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html*
13 *http://passwordsafe.sourceforge.net*
14 *http://home.arcor.de/rose-indorf/*
15 *http://www.gpg4win.org*
16 *http://www.truecrypt.org*

Paul Schäfer

Deutsche Sicherheitspolitik, Bundeswehr und Cyber Warfare

In der jüngsten Vergangenheit hatten wir es im Zusammenhang mit der NSA-Abhöraffäre insbesondere mit drei Aufregern zu tun:

1. Dem Ausspionieren des Handys der Bundeskanzlerin.

2. Der Kooperation deutscher Dienste wie Verfassungsschutz und Bundesnachrichtendienst mit dem US-amerikanischen Geheimdienst NSA, bei der große Datenmengen weitergegeben wurden, was vorgeblich im Rahmen des Anti-Terrorkampfes dringend nötig gewesen sei.

3. Und in diesem Rahmen insbesondere der Weitergabe von Daten, um Drohnenangriffe gegen vermeintliche Terroristen (v.a. in Pakistan) optimieren zu können. Damit war unweigerlich die Frage verknüpft, inwieweit zumindest von einer indirekten Beteiligung deutscher Behörden an extralegalen „gezielten Tötungen" ausgegangen werden müsse.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Die Aufregung war nachvollziehb… fiziellen Stellen die Rede ist, aber … – nicht frei von Bigotterie. Dass … *den Terror*, den der damalige U… nach den Terroranschlägen 2001 ausgerufen hatte, nicht unbeträchtlich beteiligt war, war doch bekannt. Es war die böse, aber konsequente Folge des Kanzler-Wortes von der „uneingeschränkten Solidarität". Dass aus Kreisen der US-Administration lapidar auf Übereinkünfte in diesem Rahmen hingewiesen wurde, war daher nur folgerichtig. Denn man konnte, ja musste davon ausgehen, dass zwischen den *Nachrichtendiensten* Vereinbarungen getroffen worden waren, die weit über die in diesem Milieu üblichen Deals (*Do ut des*; Gib und dir wird gegeben) hinausgingen.

Inwieweit ist Deutschland am Anti-Terror-Krieg beteiligt?

Die Beteiligung an dem von den USA geführten Anti-Terrorkrieg hatte immer verschiedene Seiten: Gesetzgeberisch, und damit in der Politik nach innen, wurden die empfindlichen Einschränkungen demokratischer Freiheitsrechte, die in den USA mit dem *US Patriot Act* vorgemacht wurden, *cum grano salis* hier übernommen. Nach außen war die Bundesrepublik bereit, sich an bestimmten Formen der Terrorbekämpfung zu beteiligen, beispielsweise am Krieg in Afghanistan, auch durch den Einsatz militärischer Spezialkräfte. Insgesamt war man bereit, das militärische und geheimdienstliche Zusammenwirken bei der Bekämpfung der Terroristen (bzw. derjenigen, die man entsprechend zuordnete) intensiv zu betreiben.

Dabei bewegte man sich gerne in Grauzonen und bevorzugte doppelbödiges Agieren: Von manchen Exzessen des *War On Terror* setzte man sich rhetorisch ab und erklärte im Zweifelsfalle auch, dass man sich nicht überall beteiligen müsse. Aber auf lauteren Widerspruch wurde bewusst verzichtet und das Mitmachen bei den diversen Unternehmungen wollte man nicht aufgeben. Die heutigen Absetzbewegungen von den NSA-Abhöraktionen entbehren daher nicht der Scheinheiligkeit.

Die illegalen Praktiken des *War On Terror*, wie die geheimen Verschleppungen (*rendition flights*) und Folterungen, hat man … auch, wie im Falle des Bremers …nme Dinge verstrickt. Den US- … offiziell nicht mitgetragen, hin- …zungsleistungen erbracht. Während man sich rhetorisch mehr und mehr vom Anti-Terrorkrieg absetzte, hat man sich noch bis ins Jahr 2010 an der völkerrechtlich unhaltbaren Mission *Enduring Freedom* in Afghanistan beteiligt. An der maritimen Anti-Terror-Mission *Active Endeavour* im Mittelmeer ist man trotz öffentlich immer wieder bekundeten Unbehagens bis heute beteiligt. Bei den Verhandlungen vorm Bundesverfassungsgericht über den Einsatz der Tornado-Aufklärungsflugzeuge, legte die Bundesregierung größten Wert auf die Feststellung, diese Flugzeuge kämen nur im Rahmen des völkerrechtlich gesicherten ISAF-Mandats zum Einsatz, und ISAF und *Enduring Freedom* blieben streng getrennt. Wie sich eine solche Trennung vor Ort *on the ground* tatsächlich aufrechterhalten ließ, bleibt bis heute ein Buch mit sieben Siegeln.

Vor allem in Afghanistan operierten bestimmte deutsche Militär-Einheiten auch im Grauzonenbereich. Was die speziellen *Task Forces* im Einzelnen getan haben, woran sie sich beteiligten, woran nicht, ist nicht restlos aufzuklären. Denn diese Spezialeinheiten haben ihrerseits immer eng mit den *US Special Forces* agiert. Tatsache ist zum Beispiel, dass sich die Bundesrepublik an der Erstellung von Listen besonders übler und gefährlicher Feinde in