Bürgerrecht auf Verschlüsselung

Udo Vetter (lawblog) in einem Gastbeitrag für Hyperland (ZDF-Blog):

„Aber natürlich sind die Behörden nicht hilflos. Sie dürfen die Verschlüsselung sichergestellter Computer knacken. Darum kümmern sich in den Polizeibehörden zentrale Abteilungen. Allerdings ist auch die beste Technik gegen gut verschlüsselte Hardware derzeit weitgehend machtlos. Schon bei 17-stelligen Passwörtern wird die Entschlüsselung oft gar nicht mehr versucht, weil jede Maßnahme zu viel Rechenpower bindet. Originell erstellte Passwörter mit deutlich mehr Ziffern gelten im Normalfall als unknackbar.

Trotz anders lautender Gerüchte haben die Behörden bislang auch keine Möglichkeit, die gängigen Verschlüsselungsprogramme zu umgehen, auch nicht für das frei erhältliche Truecrypt. Vor diesem Hintergrund ist es natürlich nur eine Frage der Zeit, bis Rufe nach ähnlichen Regelungen wie in England aufkommen. Die Frage nach dem Bürgerrecht auf Verschlüsselung könnte damit zu einem echten Prüfstein für den Rechtsstaat werden.“

AusweisApp gehackt (Malware über Autoupdate)

Jan Schejbal hat den neuen Ausweis auseinandergenommen. „Ein Dolev-Yao-Angreifer, d.h. ein Angreifer, welcher den Netzwerkverkehr beliebig manipulieren kann, jedoch nicht in der Lage ist als sicher geltende Verschlüsselung zu brechen

oder den Client des Opfers vorher zu manipulieren, kann somit aufgrund zweier Implementierungsfehler in der AusweisApp über die Auto-Update-Funktion Schadsoftware einspielen.“

Man muss sich das mal vorstellen: Wie viele „Experten“ haben daran gearbeitet? Spiegel Online schreibt: „…die beteiligten Firmen OpenLimit SignCubes AG und Siemens IT Solutions and Services GmbH werden in Kürze eine neue Version der Software bereitstellen“. Bis zur nächsten Lücke.

Firesheep oder „Hacken“ für jedermann

Zuerst habe ich mich bei der Lektüre des aktuellen Print-Spiegels geärgert, dass jemand unwidersprochen dummes Zeug über das Internet verbreiten durfte. Der „Strafrechtler und Schufa-Ombudsmann Winfried Hassemer: „Wer zwei Stunden im Internet surft, hinterlässt mehr Spuren als bei der Schufa.“ Nein. Stimmt nicht. Gar nicht wahr. Nur DAUs hinterlassen Spuren und erlauben Cookies und Javascript und HTTP referrer. Aber so ist nun mal leider das Niveau der Diskussion. Es ist zum Heulen.

Unter der reißerischen Überschrift „Hacken für jedermann“ lesen wir auf S. 131 etwas über Firesheep, „a Firefox extension that demonstrates HTTP session hijacking attacks“. Kein Wort darüber in Spiegel Offline, was diese Software macht, sondern nur dumpfe Panikmache: „Automatisch schnüffelt sie nach ungesicherten Verbindungen in der Umgebung, zum Beispiel um auszuspähen, der sich im Café über ein ungeschütztes WLAN bei Facebook angemeldet.“ Vermutlich kann man mit diesem „Hacker-Tool“ auch Verkehrsampeln ausstellen….

Warum sollte man jemanden warnen oder mahnen, der bei Facebook ohnehin die Hosen runterlässt und seine Daten in alle Welt verstreut (was war noch mal das Geschäftsmodell von Facebook?)…. Bruce Schneier hat dazu das Nötige gesagt: „Basically, Facebook authenticates clients with cookies. If someone is using a public WiFi connection, the cookies are sniffable. Firesheep uses wincap to capture and display the authentication information for accounts it sees, allowing you to hijack the connection.(…) Protect yourself by forcing the authentication to happen over TLS. *Or stop logging in to Facebook from public networks*.“

Vorratsdatenspeicherung heisst jetzt Mindestspeicherfrist

Schöner Artikel von Kai Biermann in Zeit online über die gegenwärtige PR-Kampagne der Zensur- und Überwachungslobby: „Die Angstkampagne des BKA“.

Skype: Heimlich auf den Rechner spielen

Auf Law blog wird eine Vorausmeldung von Spiegel offline erwähnt: „Zoll hört auch Skype-Telefonate mit“ – „Für die Bundesregierung handelt es sich um einen Fall zulässiger Quellen-Überwachung. Es würden nur laufenden Telekommunikationsvorgänge überwacht. Das kann man allerdings auch anders sehen. Jedenfalls dürften nach der Infiltration des genutzten Computers keine sonderlich großen Hürden bestehen, um das gesamte System auszuspähen.“..

Da schlägt natürlich sofort die Stunde der Verschwörungstheoretiker, die gepflegtes Halbwissen, fehlende Recherche, urbane Märchen und das geheimnisvolle, aber unsubstantiierte Geraune, „sie“ seien schon „drin, wir wüssten das nur nicht, zusammenmischen, bis man endlich „Online-Durchsuchung“ drüber schreiben kann.

Ganz besonders dämlich formuliert Spiegel Offline: „Nach SPIEGEL-Informationen spielen die Ermittler auf die Computer von Verdächtigen heimlich ein Programm zum Mitlauschen auf. (…) Diese Überwachung beziehe sich ‚ausschließlich auf Daten aus laufenden Kommunikationsvorgängen‘ und stehe damit im Einklang mit dem Urteil des Bundesverfassungsgerichts zur sogenannten Online-Durchsuchung.“

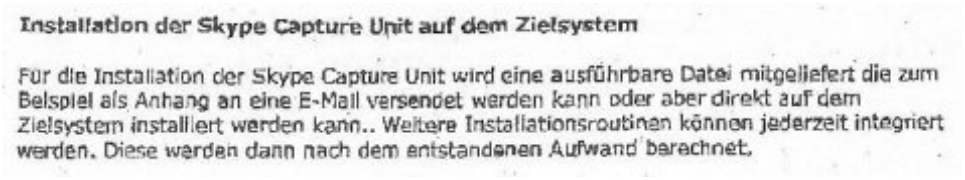
Dieser Quatsch ist gleich mehrfach zu beanstanden. Zum einen ist es kein Journalismus, wenn man zu bestimmten Themen ausschließlich „innenpolitische Sprecher“ und andere

Lobbyisten zu Wort kommen lässt. Es geht nicht darum, wie politische Parteien die Welt sehen wollen, sondern darum, wie sie ist. Ein Journalist sollte den Ehrgeiz haben, die Leserinnen und Leser aufzuklären. Wenn das nicht geschieht, handelt es sich um Propaganda oder um das Verbreiten von Gerüchten.

Bei Compliance-Magazin.de lesen wir zum Beispiel: „Auf die Frage der Liberalen, wodurch sich die Quellen-TKÜ von der Online-Durchsuchung unterscheide, verweist die Regierung darauf, dass bei diesen beiden Maßnahmen ‚lediglich die Technik der Vorgehensweise ähnlich' sei. Durch programmtechnische Vorrichtungen bei der Quellen-TKÜ sei von vornherein sichergestellt, dass eine ‚über den Überwachungszweck hinausgehende Online-Durchsuchung nicht möglich ist'.

Auch davon ist jedes Wort gelogen. Wenn man das suggestive Bürokraten-Neusprech unkritisch übernimmt, wird die Realität eben nur vernebelt. Deswegen sind diese Wortungetüme wie „Quellen-Telekommunikationsüberwachung" übernommen worden – niemand sollen wissen oder gar begreifen können, um was es sich eigentlich handelt. Das Abhören von Telefonaten ist in der TKÜV geregelt; das ist eine ganz andere gesetzliche Grundlage als, die für den heimlichen behördlichen Zugriff auf fremde Rechner benötigt würde. Wer beides vermischt, hat entweder nichts begriffen oder will bewusst verwirren.

Udo Vetter scheint vergessen zu haben, dass er zum Thema Skype schon am 17.8.2010 gebloggt hat. Er verwies damals auf den Wikipedia-Eintrag zu Skype, wo man lesen kann, worum es eigentlich geht. Natürlich kann man Skype anhören, aber nicht mit Methoden, die der real gar nicht existierenden „Online-Durchsuchung" irgendwie ähneln. Man kann also mitnichten, wie Spiegel offline suggiert, einfach so „heimlich" ein Programm auf fremde Computer „spielen." Nein, das kann man nur, wenn man den physikalischen Zugriff hat und Software installieren darf (der Besitzer des Rechner muss also ein Dau sein.)



Installation der Skype Capture Unit auf dem Zielsystem

Für die Installation der Skype Capture Unit wird eine ausführbare Datei mitgeliefert die zum Beispiel als Anhang an eine E-Mail versendet werden kann oder aber direkt auf dem Zielsystem installiert werden kann.. Weitere Installationsroutinen können jederzeit integriert werden. Diese werden dann nach dem entstandenen Aufwand berechnet.

auf der Website der Piratenpartei Bayern kann man im Detail nachlesen, wie die sich Fall von Skype vorstellen.

Eine ausführbare Datei, die per E-Mail-Anhang verschickt werden kann? Da lachen ja die Hühner!. Und die installiert das Zielobjekt nichtsahnend? Und der Verdächtige hat auch weder einen Mac noch Linux? Ich zitiere mich selbst vom 27.08.2009:

In der Heise-Meldung von gestern heisst es: „Ein Schweizer Software-Entwickler hat auf seinen Seiten den Quelltext zu einem Programm veröffentlicht, das verschlüsselte Kommunikation über Skype heimlich belauschen kann. Das Programm ist dazu vorgesehen, als Trojanisches Pferd auf einem PC eingeschmuggelt zu werden. Dort klinkt es sich nach Angaben des Autors in den laufenden Skype-Prozess ein, schneidet die Audio-Daten der Gespräche heimlich mit und lädt sie dann als MP3-Dateien auf einen externen Server.“

Ds habe ich mir genauer angesehen. Das Trojanische Pferd ist mitnichten ein „Bundestrojaner“, den es bekanntlich nicht gibt, sondern das Programm Minipanzer: „Minipanzer is a trojan horse that disguises as any kind of file type and when executed on a victims system it collects all sensitive data like account information etc. and sends it to an email address owned by the attacker. It is a one-shot-trojan. It doesn’t install on a target system but only executes its payload and removes itself afterwards.“

Im dazugehörigen Blog heisst es: „The code is simple and straightforward. You have know malware development is no rocket science and if you expect big magic you are at the wrong place.“ Am besten hat mir der Kommentar „Giovannis“ gefallen: „Despite what some people say, Skype has never been secure. It is relatively easy to hack skype accounts, skype

does not even check if the same user logs in simultaneusly on different machines and what is worst, the second user can get a copy of all the chats. Skype is good for housewifes that want to chat a bit with their kids, but for confidential conversations the use of strong voice encryption is required. In our company we tested many of them, we now keep with PhoneCrypt from securstar as it proved to be very good, stable, and with an excellent voice quality."

Ich verweise auf mein hiesiges Posting „"Bayerntrojaner" zum Abhören von Internet-Telefonie?" sowie auf meinen Artikel in der Netzeitung: „Wenn der Laptop zweimal klingelt".

Auf law blog gab es einen interessanten Kommentar: „@mark: es geht um einen einfachen Audio-Capture-Client mit Streamingfunktion der sich fernwarten lässt. Der Programmieraufwand dafür beträgt ca. 20-30 h. Dazu kommt dann die Sonderfunktionalität für Skype die man noch mal mit der gleichen Zeit veranschlagen kann. Dazu noch Tests sowie der Server. Alles in allem ein Projekt, dass sich mit nur einem Mann-Monat stemmen lässt. Selbst bei einem Stundenpreis von vollkommen utopischen 500€ für den Entwickler reden wir hier von Entwicklungskosten im sehr niedrigen 5stelligen Bereich. Bei den Preisen muss die Software nur ein einziges Mal zum Einsatz kommen, damit sie sich für die entwickelnde Firma rechnet. Ich bleibe dabei: hier wird über den Tisch gezogen."

Nach mal langsam zum Mitschreiben: Man kann nichts heimlich auf fremde Rechner spielen, wenn der Besitzer das nicht will. Kapiert?

Economic Reasons for Security Failures

Ein sehr interessanter Artikel der New York Times (via Light Blue Touchpaper: „Social network security – an oxymoron?“): „Monopolies Breed Security Breaks“. Thema: Economic Reasons for Security Failures.

„Social networking sites such as Facebook try to capture most of their users‘ online interactions in order to lock in their users and capture any ad revenue. In the process they are not only reinventing mechanisms such as email, chat, groups, Web pages and payments; they are also making the same old mistakes all over again.“

Fazit: „So as people move from the open environment of the Internet to the walled garden of Facebook, we can expect security to get worse“. Das erinnert uns an die „dumb fucks„.

Der Autor Ross Anderson zitiert einen seiner Studenten, und man muss fürchten, dass das ernst gemeint ist: „All the party invitations in Cambridge come through Facebook. If you don’t use Facebook you don’t get to any parties, so you’ll never meet any girls, you won’t have any kids and your genes will die out.“

Dumb Fucks

Spiegel offline („Der Cyber-Cäsar“) ist ja wieder zu blöd und zu faul, uns mit wichtigen Links zu belästigen. Diese Pfeifen-Truppe dort gehörte mal richtig durchgewalkt – sie werden es nie lernen.

„Über den Herrscher kursieren düstere Legenden. Das Techblog ‚Silicon Alley Insider, veröffentlichte Auszüge eines Gesprächs, das der Facebook-Chef vor einigen Jahren per Messenger mit einem Freund geführt hat. Zuckerberg brüstete sich darin, mehr als 4000 E-Mail-Adressen und Fotos von Harvard-Studenten gesammelt zu haben. Der Freund wollte wissen, wie Zuckerberg das geschafft hat. „Ich weiß nicht“, antwortete der Facebook-Chef. ‚Die Leute vertrauen mir. Was für Trottel'“.

Die Trottel sind auch die, die uns das Original vorenthalten wollen, weil sie als gute Deutsche Angst vor dem Internet und dem Link haben. Das Portrait Zuckerbergs im „New Yorker“ ist ebenfalls interessant und wichtig und gehörte erwähnt.

Hier also der Beleg:
ZUCK: i have over 4000 emails, pictures, addresses, sns
FRIEND: what!? how’d you manage that one?
ZUCK: people just submitted it
ZUCK: i don’t know why
ZUCK: they “trust me”
ZUCK: dumb fucks

Quod erat demonstrandum.

Strafverfolgungsfreier Raum

Neue Sprachregelung der Zensur-Lobby: „Das Internet wird zunehmend zum strafverfolgungsfreien Raum“ (sagt natürlich Bosbach, das merkbefreite Sprachrohr der Überwachungsstatt-Fanatiker, laut Heise.) Ich aber sage euch: die Vorratsdatenspeicherung wird erneut kommen, keine Frage.

Demo Freiheit statt Angst


hat einen
KERN-
BEREICH

Truecrypt und der kurze Weg zum Superkriminellen

Jetzt schlägt es doch dem Fass den Boden in’s Gesicht. Via lawblog: “ Was waren die Gründe für den Staatsanwalt, von erhöhter krimineller Energie und konspirativem Vorgehen zu sprechen? Nun, es war festgestellt worden, dass mein Mandant auf seinem Rechner TOR nutzen kann. Außerdem hatte er Truecrypt installiert.“

Wer seine Haustär verschließt, ist kriminell, weil er es den hausdurchsuchenden Beamten schwer macht. Ich habe sogar ein Stangenschloss vor der Tür – ich bin superkriminell. Ich nutze auch Tor und Truecrpyt. Und ich verschlüssele wichtige E-Mails.

Ein hübscher Kommentar dort: „Nicht auszudenken, welches Strafmaß die Staatsanwaltschaft fordern würde, wenn er dann auch noch Linux / BSD / Hurd anstatt Windows/OSX verwendet hätte. Wahrscheinlich wäre laut der Anklage selbst ein Mac genug, um als subversiv zu gelten."

Nur gut, dass dieses Urteil diesem DAU-Gericht in den höheren Instanzen um die Ohren gehauen werden wird.

John F. Kennedy zur Online-Durchsuchung

Das war ja zu erwarten: Die einflussreichste Ente des letzten Jahrzehnts watschelt immer noch. Hinter den sieben Bergen bei den sieben Zwergen (aka Schweiz) ist alles ein weniger langsamer, aber jetzt quakt es auch dort. Wie 20 Minuten Online berichtet, gibt es nur zwei Denkschulen: Die einen wollen im Männer im Kreis um ein Feuer tanzen lassen, damit es bald regnet, und die anderen sagen, das sei grob sittenwidrig und auch Frauen müsse das erlaubt sein.

Halt! So war es gar nicht. Die einen wollen private Computer behördlicherseits heimlich überwachen und die anderen sind dagegen, weil das obrigkeitsstaatlich undsoweiter sei.

Also führen wir schnell eine dritte Denkschule ein, um die schweizer Diskussion aufzulockern. Ganz egal, ob Männer oder Frauen im Kreis tanzen, das hat nichts mit dem Regen zu tun. Ganz egal, ob man einen „Bundestrojaner" blöd findet oder nicht – ihn gab es noch nie, ihn gibt es noch nicht und es wird ihn so, wie DAUs sich das vorstellen, nie geben. Punktum. Es ist ein Hoax, ein Mythos, eine urbane Legende, eine frommes Überwachungsmärchen, aus den feuchten Wunschträumen der

Zensur-Lobby entschlüpft, gar nicht wahr, eine Ente, alles gelogen und noch nicht mal gut erfunden, die Welt als Wille und Vorstellung – muss ich noch deutlicher werden?

John F. Kennedy wird der Satz zugeschrieben: „Der größte Feind der Wahrheit ist nicht die Lüge – absichtsvoll, künstlich, unehrlich -, sondern der Mythos – fortdauernd, verführerisch und unrealistisch."

Besser kann man es nicht beschreiben. Der Mythos von der real gar nicht existierenden „Online-Durchsuchung" wirkt deshalb, weil er fortdauernd wiederholt wird – von dämlichen Journalisten, die von den technischen Hintergründen gar nichts wissen wollen, von eitlen Möchtegern-Hackern, die sich mit ihrem vermeintlichem Allwissen brüsten, von Verschwörungstheoretikern („der Staat/die NSA/der Mossad sind schon drin"), von selbst ernannten Experten, die vor jedes Mikrofon springen, das ihnen hingehalten wird, aber eine Waschmaschine nicht von einem Kühlschrank und einen Algorithmus nicht von einem Oktopus unterscheiden können.

Verführerisch, weil es so schön sexy ist, wie aus einem Hollywood-Movie entsprungen, dort, wo der Hacker als Schamane des 21. Jahrhunderts mit seinen magischen Fähigkeiten in alles Digitale eindringt, was nicht bei drei auf dem nächsten Baum ist. Sexy besonders für die Gegner, weil man mit der Ente schon herumwedeln und vor dem ultrabösen Staat warnen kann.

„Auch bürgerliche Parteien sind skeptisch gegen die Computer-Überwachung: Der SVP etwa sind die Anforderungen für den Einsatz von Trojanern nicht hoch genug, wie sie in einer Stellungnahme schreibt. Die CVP meldet ‚gewisse Vorbehalte' an und die FDP befürchtet 'schwerwiegende Folgen' für die infizierten Computer."

Das ist doch zum Kringeln! Sie gehen schon von „Trojanern" aus, obwohl die vermutlich gar nicht wissen, was das ist. Magie eben. „Die" können das „irgendwie". Haben wir doch im

Fernsehen gesehen. Oder im „Tatort“, wo ein Hacker mit einem Laptop auf einem Hochhaus steht und die Verkehrsampeln ausschaltet.

Unrealistisch sowieso. Aber deswegen ist der Mythos ja einer – im Gegensatz zur Wahrheit. Die Zahnpasta ist aus der Tube und ich könne 77 Büchern über den Hoax „Online-Durchsuchung“ schrieben, es würde nichts nützen.

Was lesen wir über Rheinland-Pfalz? „Mit der gesetzlichen Zulassung von Online-Durchsuchungen dürfen rheinland-pfälzische Ermittler künftig zudem verdeckt auf Computer von Terrorverdächtigen und Schwerkriminellen zugreifen.“ hat auch nur einer der Journalisten, die sich das Gefasel des dortigen Innen-Daus anhörten oder darüber schrieben, gefragt, wie das geschehen, also technisch umgesetzt werden soll? Nein, niemand. Wieso? Sind die Medien gleichgeschaltet? Droht ein Bußgeld, wenn man Fragen stellt als Journalist? Nein, aber bei einem Mythos denkt eben niemand nach. Kopf ab zum Gebet.

Mich ärgert auch die schlampige Formulierung bei Heise. „Die rheinland-pfälzische Polizei erhält damit die Befugnis, Programme auf IT-Systemen zu installieren, die ein Mitschneiden von Kommunikation etwa in Form von Internet-Telefonie noch vor einer Verschlüsselung erlauben (Quellen-TKÜ). Voraussetzung für die Maßnahme ist ein richterlicher Beschluss.“

Natürlich kann man Spionage-Programme auf Rechnern installieren, wenn man den physischen Zugriff hat. Aber ist das bei einem verdächtigen Privatier realistisch? „Heimlich online“ geht es *nicht*.

Das Mitschneiden der Kommunikation hat uns schon Rot-Grün beschwert in Form der (Luftholen vor dem Aussprechen des Wortes nicht vergessen) Telekommunikations-Überwachungsverordnung (TKÜV) und der SINA-Box. Das Abhören hat aber rein gar nichts mit der „Online-Durchsuchung“ zu tun,

es handelt sich auch um zwei völlig verschiedene Rechtsgrundlagen. Wieso muss man das immer total durcheinanderwürfeln? Nur um irgendwann das sexy Wort „Online-Durchsuchung“ unterbringen zu können?

Digitale Selbstverteidigung

Nein, der Chaos Computer Club hat nicht alles erfunden, was man an Begriffen des digitalen und Internet-Zeitalters so kennt. „Der CCC hat vor einiger Zeit den Begriff ‚digitale Selbstverteidigung‘ ins Gespräch gebracht, und meinen damit Dinge wie Verschlüsselung und Tor“, schreibt Fefe. Ach ja? Die German Privacy Foundation wurde unter anderem auch deswegen gegründet, weil der CCC sich um die Tor-Betreiber nicht sehr kümmerte. Natürlich springen sie jetzt auf den Zug auf und sagen, dass alles von ihnen stammte. Al Gore hat ja auch bekanntlich das Internet erfunden.

„Der gemeinnützige Verein German Privacy Foundation e.V. informiert über sichere Kommunikation im Internet und organisiert und unterstützt Weiterbildungs- und Aufklärungmaßnahmen für Erwachsene und Jugendliche. Die GPF steht mit Experten für Anfragen zu den Themen Kryptographie (insbesondere Verschlüsselung von E-Mails) und Anonymität im Internet (zum Beispiel Tor-Server, Java Anon Proxy, anonyme Remailer) zur Verfügung. Darüberhinaus betreibt der Verein im Internet zahlreiche Anonymisierungsdienste zur kostenlosen Nutzung. “

„Derzeit betreibt die GPF e.V. 5 leistungsfähige Tor-Nodes, ein Mixmaster Remailer sowie zwei I2P-Knoten, einen JAP-Mix und unzensierte DNS-Server. Mitglieder des Vereins betreiben weitere Server in eigener Verantwortung mit Unterstützung der

GPF e.V.“

Wir nennen unsere Veranstaltungen übrigens „Digitales Aikido“.

Vorratsdatenspeicherung: Sechs von siebenundzwanzig

„Zum gegenwärtigen Zeitpunkt haben sechs Mitgliedstaaten, Luxemburg eingeschlossen, die Richtlinie noch nicht umgesetzt. Ende 2009 und im Februar 2010 entschied der Europäische Gerichtshof, dass Irland und Griechenland einerseits und Schweden andererseits gegen das EU-Recht verstoßen haben. (…) In Rumänien wurde das einzelstaatliche Gesetz zur Umsetzung der Richtlinie vom Verfassungsgericht für verfassungswidrig erklärt. In Deutschland wurde ein ähnliches Urteil verkündet; gegen Ungarn ist ebenfalls ein Verfahren anhängig.“ (via netzpolitik.org)

Stoppschilder für Raubkopierer

Spiegel Offline schreibt: „Leutheusser-Schnarrenbergers Idee: Internetprovider sollen Nutzer, die eine Urheberrechtsverletzung begehen, frühzeitig warnen. Da würde dann zum Beispiel ein Nutzer den automatischen Hinweis auf seinen Bildschirm bekommen: „Was Du gerade tust, ist illegal und verletzt das Urheberrecht.“ Die Ministerin erhofft sich eine erzieherische Wirkung.“

Nun, hier ist mein Beitrag. Ich hoffe, er erzieht die wohlwollenden Leserinnen und geneigten Leser. Ach ja: wie das gehen soll mit den Stoppschildern? „Sie müssen den Inhalt der Kommunikation mit einer wie auch immer gearteten Datenbank urheberrechtlich geschützter Inhalte abgleichen.“ Ab heute ist Leutheusser-Schnarrenberger für mich Zensursula 2.0.

Polizei bespitzelt sich

selbst

Hier ist die Spitze des Eisbergs und wie es hinter den Kulissen der Polizei wirklich aussieht. Der Tagesspiegel berichtet hier („Neue Merkwürdigkeiten in der Polizeiaffäre in Sachsen-Anhalt“ und hier („Nächster Akt in Dessauer Polizeiaffäre“), Spiegel Offline hier („Polizeidirektion spähte eigene Beamte aus“). Da sieht man, was die tun, wenn keiner hinguckt – was tun die gar mit den Daten anderer?

Hintergrund: Der Leitende Polizeidirektor Hans-Christoph Glombitza wollte seine Staatsschutzabteilung im Kampf gegen Rechtsextremisten ausbremsen. *Spiegel Offline*: „Die hohe Zahl von Ermittlungsverfahren schade dem ‚Ansehen unseres Landes‘. Darüber sei ’niemand glücklich‘.“ Und irgendjemand hatte dennoch mit der Presse geredet.

Der *Tagesspiegel*: „Die Direktionsspitze ließ im Frühjahr 2007 eine Sicherungskopie sämtlicher Daten ziehen, die vom 23. Februar bis zum 11. Mai auf dem Zentralserver gespeichert waren. Damit waren die Daten von 1100 Beamten, auch private E-Mails, ohne Wissen der Betroffenen und des Personalrats auf unabsehbare Zeit in der Hand der Führung der Direktion. Und das, obwohl nur drei Beamte der Abteilung Staatsschutz im Verdacht standen, sie hätten bei der Presse geplaudert.“

Spiegel Offline: „Unter den betroffenen Datensätzen waren dabei nicht nur die Verbindungsdaten dienstlicher E-Mails und Dokumente, die jeder Beamte, für die Hausspitze zugänglich, in der „Ablagemappe“ auf dem Server gespeichert hatte, sondern auch private Speicher, die sogenannten Heimserver. Sie hatten jeweils eine Umfang von 50 Megabyte und dienten passwortgeschützt der Aufbewahrung von privaten Fotos, Schreiben und E-Mails.“

Das schauen wir uns mal genauer an. Was lehrt uns das? Die Polizei verschlüsselt ihre E-Mails nicht, sondern schreibt nur

elektronische Postkarten. Die „Hausspitze“ schnüffelt allen hinterher und kann sogar die privaten Daten überprüfen. Die Polizei ist auch nicht in der Lage, ihre eigene Vorratsdatenspeicherung zu umgehen. Der *Tagesspiegel* kann seinen Informanten auch nicht anbieten, anonym zu kommunizieren, um die interne Schnüffelei zu verhindern – etwa durch eine PrivacyBox. Die leben also alle noch im Zeitalter der Internetausdrucker.

Manchmal geschehen Dinge, die kann man sich gar nicht ausdenken. Wie dämlich muss man eigentlich sein, um sich auch noch bei einer solch schmierigen Affäre erwischen zu lassen?

Linke Dümmste Anzunehmende Soft-und Hardware-Benutzer

Die taz versucht zu berichteten: „Der linken Rechtshilfeorganisation Rote Hilfe ist eine Festplatte mit Mitglieder- und Kontodaten gestohlen worden. (…) In einer Erklärung des Vorstandes heißt es, der Diebstahl sei möglicherweise durch einen „fahrlässigen Umgang einer anderen Gruppe mit Schlüsseln begünstigt worden“. Von einem „gezielten Einbruch“ könne „jedenfalls nicht ausgegangen werden“.

Versucht? Ja, journalistischen Maßstäben wird der Artikel der *taz* nicht gerecht: Er verzichtet darauf, die wesentlichen Fragen zu stellen. Was ist geschehen? Der Verein hat rund 150 Euro verloren. Mehr war die Festplatte vermutlich nicht wert. Daten sind nicht verlorengegangen: Natürlich gab es ein Backup, und die gestohlene Festplatte war mit Truecrypt so gesichert, dass die Hardware für die Diebe wertlos sein wird. Auch wird niemand irgendetwas Internes der Roten Hilfe

erfahren.

Im Ernst: Ich weiß nicht, ob die Truecrypt benutzt haben. Wenn nicht, dann sind sie total bescheuert, und man sollte weder Mitleid haben noch die Veranwortlichen länger als eine Minute an ihrem Vereinspöstchen kleben lassen. Das hätte die *taz* sie fragen sollen. Aber ich wette, dass bei der *taz* auch niemand Truecrypt oder ähnliches Teufelszeug kennt oder gar nutzt.

„Es sei „unwahrscheinlich, aber nicht unmöglich", dass die Diebe mit Hilfe der gestohlenen Daten unberechtigte Abbuchungen von Konten der Rote-Hilfe-Mitglieder vornehmen." Nicht unmöglich. Aha. Dann sitzen dort also linke dümmste anzunehmende Soft-und Hardware-Benutzer. Eine verschlüsselte E-Mail kann man ihnen auch nicht schreiben. Geschieht ihnen ganz recht.

Facebook Privacy: Give him an inch and he'll take an ell

Interessantes Posting Don Dahlmanns: „Wenn Facebook anfängt hinten herum Empfehlungen unter meinem Namen zu versenden, dann ist das ein klarer Grund meine Mitgliedschaft dort zu beenden." Dazu ein zutreffender zynischer User-Kommentar: „Ich nehme an, dass Facebook dich inzwischen besser kennt als du selbst und somit auch in deinem Namen Entscheidungen treffen kann."

Vgl. auch meedia.de: „In den Mitglieder-Postfächern tauchen Freundschaftsempfehlungen auf, die jedoch vom angegeben Absender nie verschickt wurden. Zudem sprechen immer mehr Blogger und Early-Adopter darüber ihr Facebook-Account zu löschen."

Leute, nun mal halblang. Hört auf den Volksmund, der immer Recht hat: „Wenn man dem Teufel den kleinen Finger gibt, so nimmt er die ganze Hand.“ Englisch: „Give him an inch and he’ll take an ell.“

Ihr wusstet doch, worauf ihr euch eingelassen habt? Private Daten der Nutzer an windige Spammer und Commercials zu verscherbeln ist doch das Geschäftmodell der so genannten „sozialen“ Netzwerke! Ein anderes gibt es nicht. Wer das weiß und dennoch Facebook und Konsorten naiv nutzt, ist selbst schuld und sollte im nachhinein nicht jammern.

GPF veröffentlicht den Crypto-Stick