Die Trojaner sind vom Pferd gefallen

Die FAZ schreibt: „Der deutsche Staatstrojaner wurde geknackt“. Auch Heise formuliert „CCC knackt Staatstrojaner“ (von Krempl erwarte ich auch nichts anderes). Der CCC beginnt korrekt „Der Chaos Computer Club (CCC) hat eine eingehende Analyse staatlicher Spionagesoftware vorgenommen“, fährt dann aber leider auch im Medien-Neusprecht fort: „Die untersuchten Trojaner [sic] können nicht nur höchst intime Daten ausleiten, sondern bieten auch eine Fernsteuerungsfunktion zum Nachladen und Ausführen beliebiger weiterer Schadsoftware. Aufgrund von groben Design- und Implementierungsfehlern entstehen außerdem eklatante Sicherheitslücken in den infiltrierten Rechnern, die auch Dritte ausnutzen können.“

Im eigentlichen Bericht (Lesebefehl!) ist es korrekt: „Dem Chaos Computer Club (CCC) wurde Schadsoftware zugespielt, deren Besitzer begründeten Anlaß zu der Vermutung hatten, daß es sich möglicherweise um einen ‚Bundestrojaner‘ handeln könnte.“ (Anführungszeichen! Eben!)

Da fällt mir Wolfgang Fritz Haug ein: „Begriffe sind Abstraktionen, die dann brauchbar sind, wenn sie tatsächliche Bewandtnisse komplexer Gegenstände erfassen. Sie sind analytisch gewonnen Denkbestimmungen, deren Aufgabe es ist, aus dem fürs Denken einzig gangbaren Weg Konkretion zu erreichen.“

„Staatstrojaner“ ist ein Begriff, der ungefähr so seriös ist wie „friedenserzwingende Maßnahme“ für Krieg. Ausserdem wendet sich jeder humanistisch Gebildete mit Grausen ab, weil die sagenhaften Trojaner mitnichten in dem Pferd saßen, sondern die Griechen, und das trojanische Pferd als Computerprogramm dann auch so genannt werden müsste.

Ich habe jetzt das Vergnügen, rational denken zu dürfen, obwohl ich von einer Horde johlender Verschwörungstheoretiker umgeben bin und die wiederum von einer noch größeren Horde von ahnungslosen Dummköpfen, die gar nicht denken wollen.

Die Faz schreibt: *Der Trojaner kann laut der Analyse des Chaos Computer Clubs (CCC) beliebige Überwachungsmodule auf den einmal infiltrierten Computer nachladen – „bis hin zum Großen Lausch- und Spähangriff“, wie CCC-Sprecher Frank Rieger in einem Beitrag für die „Frankfurter Allgemeine Sonntagszeitung“ schreibt.*.

Jetzt mal gaaaanz langsam und genau hinsehen. Die Pointe kommt jetzt:

Die spezielle Überwachungssoftware wird von den Ermittlungsbehörden unter anderem zur sogenannten Quellen-Telekommunikationsüberwachung genutzt. Die Quellen-TKÜ dient dazu, Kommunikation schon auf dem Computer eines Verdächtigen abzufangen, bevor sie verschlüsselt wird. Im Unterschied zur Online-Durchsuchung….

Hier geht es um das Abhören von Internet-Telefonie (Windows! Skype! „Die in den Trojaner eingebauten Funktionen sind das Anfertigen von Screenshots und das Abhören von Skype- und anderen VoIP-Gesprächen, allerdings können auch beliebige Schad-Module nachgeladen und ausgeführt werden.“) und um nicht anderes. Nicht mehr oder weniger. Es geht nicht darum, von fern ein Programm auf einen Rechner zu schleusen (welche IP-Adresse würde diese haben?) und den ohne Wissen des Nutzers fernzusteuern. Das jedoch kann man mit dem vom CCC

analysierten Programm zweifellos („Die Malware bestand aus einer Windows-DLL ohne exportierte Routinen.“ Bekanntlich nutzt *niemand* Linux oder Apple.)

Die Zahnpasta ist leider aus der Tube, auch wenn sogar die FAZ darauf hinweist, dass die real gar nicht existierende „Online-Durchsuchung“ etwas anderes sei als die so genannte „Quellen-TKÜ“. Beide Begriffe stammen ohnehin aus dem Wörterbuch des Unmenschen, sind Propaganda und wurden vom Ministerium für Wahrheit in die Welt gesetzt, was bei der übergroßen Zahl der regimetreuen Medien zu der irrigen Annahme führt, man dürfe auch nur diese Begriffe benutzen.

„Der CCC betonte, die sogenannte Quellen-TKÜ dürfe ausschließlich für das Abhören von Internettelefonie verwendet werden“, schreibt Heise. Richtig, aber die Ermittler handelten offenbar nach der Maxime „legal, illegal, scheißegal“. Ich habe nichts anderes erwartet. Die Schad- und Spionagesoftware macht auch genau das, was man von ihr erwartet: „So kann der Trojaner über das Netz weitere Programme nachladen und ferngesteuert zur Ausführung bringen“. (Gemeint ist: das Trojanische Pferd).

Die ausgeleiteten Bildschirmfotos und Audio-Daten sind auf inkompetente Art und Weise verschlüsselt, die Kommandos von der Steuersoftware an den Trojaner sind gar vollständig unverschlüssselt. Weder die Kommandos an den Trojaner noch dessen Antworten sind durch irgendeine Form der Authentifizierung oder auch nur Integritätssicherung geschützt. So können nicht nur unbefugte Dritte den Trojaner fernsteuern, sondern bereits nur mäßig begabte Angreifer sich den Behörden gegenüber als eine bestimmte Instanz des Trojaners ausgeben und gefälschte Daten abliefern. Es ist sogar ein Angriff auf die behördliche Infrastruktur denkbar.

Avanti Dilettanti. Das ist eigentlich eine gute Nachricht, denn sie straft diejenigen Lügen, die glauben, „die da oben“ hätten von irgendwas eine Ahnung. Wie stellte sich das BKA-

Chef Ziercke das vor mit der „Online-Durchsuchung“:

Dieses Programm, was wir da entwickeln, muss ein Unikat sein, darf keine Schadsoftware sein, darf sich nicht selbst verbreiten können und muss unter der Kontrolle dessen stehen, der es tatsächlich einbringt, wobei die Frage des Einbringens die spannendste Frage für alle überhaupt ist. Ich kann Ihnen hier öffentlich nicht beantworten, wie wir da konkret vorgehen würden. Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht. Wenn man ihnen erzählt hat, was für eine tolle Website das ist oder eine Seite mit ihren Familienangehörigen, die bei einem Unfall verletzt worden sind, sodass sie dann tatsächlich die Seite anklicken.

Sehr hübsch ist das Fazit im CCC-Bericht: „Wir sind hocherfreut, daß sich für die moralisch fragwürdige Tätigkeit der Programmierung der Computerwanze keine fähiger Experte gewinnen ließ und die Aufgabe am Ende bei studentischen Hilfskräften mit noch nicht entwickeltem festen Moralfundament hängenblieb.“

Jetzt aber Butter bei die Fische: „Wir haben keine Erkenntnisse über das Verfahren, wie die Schadsoftware auf dem Zielrechner installiert wurde. Eine naheliegende Vermutung ist, daß die Angreifer dafür physischen Zugriff auf den Rechner hatten.“

Anders geht es nicht. Daher muss ich auch kein Wort meines Buches zurücknehmen. Und nicht nur das: Wie sollen Ermittler die IP-Adresse einen Rechners herausfinden? Was machen sie, wenn Linux zum Einsatz kommt? Egal: Das dumme Volk denkt, „sie“ wären ohnehin schon drin. diesen Einrdruck zu vermitteln, sind die Medien ja da. Das war jetzt *meine* Verschwörungstheorie.

Update: Nein Zeit online, die „Online-Durchsuchung“

funktioniert eben nicht – nur mit physischen Zugriff auf einen Rechner – und das nur bei Windows 32 Bit, und auch nur bei Internet-Telefonie. Es ist zum Haare Ausraufen.

Anonymität ist gut

Oberlandesgericht Hamm – Recht auf anonymisierte Internetnutzung (via law blog):

Die für das Internet typische anonyme Nutzung entspricht zudem auch der grundrechtlichen Interessenlage, da eine Beschränkung der Meinungsfreiheit auf Äußerungen, die einem bestimmten Individuum zugerechnet werden, mit Art. 5 Abs. 1 Satz 1 GG nicht vereinbar ist. Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde allgemein die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung nicht zu äußern. Dieser Gefahr der Selbstzensur soll durch das Grundrecht auf freie Meinungsäußerung entgegen gewirkt werden.

Anonym geht anders

Laut Spiegel Online hat der so genannte Anonymisierungsdienst HideMyAss mit den Behörden kooperiert und die Identität von Nutzern herausgegeben.

Anonym geht anders. „Wir raten von solchen Diensten seit Jahren ab“, sagt Jan-Kaspar Münnich von der German Privacy

Foundation, einem Verein, der sich für das Recht auf Anonymität im Internet einsetzt.

Schon sicherer seien Dienste, bei denen der Internetverkehr über mehrere Server abgewickelt werde, die von verschiedenen Anbietern betrieben würden. „So kann nicht eine Firma den gesamten Verkehr überblicken." Er empfiehlt Dienste wie das Anonymisierungs-Netzwerk Tor oder das aus einem Forschungsprojekt hervorgegangene JonDonym. Diese Dienste setzen auf sogenannte Server-Kaskaden: Ein Netzwerk aus mehreren Servern in verschiedenen Ländern, die gar nicht wissen, was sie da übertragen – und nicht speichern, wer auf sie zugreift. „Daten, die nicht vorliegen, kann man auch nicht herausgeben", sagt Münnich.

Datenkraken, revisited

„Wenn wir in das Netzwerk reingehen, bezahlen wir kein Geld, sondern wir bezahlen eben mit unseren Daten. Und die sind offensichtlich ein einträgliches Geschäft, wenn man sich die geschätzten Börsennotierungen von Facebook anschaut." (Prof. Dr. Johannes Caspar, Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, laut Heise)

Wie kann man eigentlich die

Piratenpartei kontaktieren?

Diese Nachricht wurde automatisch von einem Mailserver erstellt.
This message was created automatically by mail delivery software.
Die Nachricht von Ihnen konnte nicht an alle Empfaenger zugestellt werden.
The message that you sent could not be delivered to all of its recipients.
Es gab Fehler bei folgenden Empfaengern:
The following address(es) failed:

limesurvey@piratenpartei.de
SMTP error from remote mailer after RCPT TO::
host mail.piratenpartei.de [178.19.71.5]: 550 5.1.1 :
Recipient address rejected: User unknown
r.24.14622.06d739bec128b6fb@piratenpartei.de
SMTP error from remote mailer after RCPT TO::
host mail.piratenpartei.de [178.19.71.5]: 550 5.1.1 :
Recipient address rejected: User unknown

—- Es folgt eine Kopie der Nachricht mit allen Kopfzeilen:
—- This is a copy of the message, including all the headers:
_____
_____

Return-path:
(…)
Date: Tue, 20 Sep 2011 16:36:55 +0200
From: Burkhard Schroeder
User-Agent: Thunderbird 2.0.0.6 (Macintosh/20071008)
(…)

Piratenpartei Mitgliederverwaltung schrieb:
Aus diesem Grund kannst du hier
http://limesurvey.piratenpartei.de/index.php?lang=de-informal&

sid=76217&token=[xxxxx]
deine persönlichen Kommunikationspräferenzen eintragen, die wir dann beim Versand weiterer E-Mails beachten.

Nein, kann ich nicht. Wenn ihr nicht zusätzlich mitteilt, dass man Cookies einschalten muss, wird man überrascht und bekommt eine Fehlermeldung. Könnt ihr nicht endlich mal zur Kenntnis nehmen, dass vernünftige Menschen Cookies beim Surfen per default ausstellen?

Grrr

Burks

Popraci, revisited

Gestern fand hier auf dem Richardplatz das „Popraci“ statt, laut „oral history“ (wer’s glaubt…). das „178. Rixdorfer Strohballenrollen“.

Anders formuliert: Ich bekenne, dass ich keine Lust auf die „Freiheit statt Angst„-Demo hatte. Nina Hagen und Renate Kühnast – eine Kampffront? Das fehlte noch…

Die Grünen haben uns die TKÜV beschert, die sie noch nicht einmal bereuen, und marschieren da jetzt mit? Verlogenes Pack!

Wenn der Button zwei Mal klickt

Ein Artikel von mir in der *taz*: „Der Computerverlag Heise unterwandert die Versuche von Facebook, an Daten von Nutzern zu kommen. Er tut es sehr geschickt – und Facebook ist machtlos.“

Pakistanis lernen jetzt Steganografie

Die Abbildung stammt von Jan Feindt, der die israelische Comix-Anthologie Dimona gegründet hat. Damit habe ich schon vor acht Jahren hier Steganografie demonstriert.

Guardian: „Pakistan to ban encryption software“ – „Millions of internet users in Pakistan will be unable to send emails and messages without fear of government snooping after authorities banned the use of encryption software.“

Das ärgert mich immer an den ahnungslosen Berichten in den Medien: Das Wichtigste fehlt meistens. Verschlüsselung verbieten? Das hatten wir doch schon mal. Guckst du bei Kristian Köhntopp: „Das Recht auf Kryptographie ist ein Menschenrecht“. Darauf sind wir Deutschen natürlich zuerst gekommen.

Kanther fordert in seiner Rede, den Risiken, die sich aus der Technik ergeben auch mit den Mitteln der Technik zu begegnen und führt dabei unter anderem auch elektronische Wegfahrsperren als Mittel zur Verhinderung von Kraftfahrzeugdiebstählen an. Dieser Vergleich mutet seltsam

unpassend an, handelt es sich dabei doch genau wie der Einsatz von kryptographischen Mitteln um ein klassisches Mittel zu Verbrechensprävention, nicht um ein staatliches Instrument zur Strafverfolgung. Eine Umsetzung von Kanthers Vorschlägen würde den Anwender von Datennetzen seiner legitimen Verteidigungsmöglichkeiten gegen Computerkriminelle berauben.

Kanther führt weiter aus, wie er sich die Kontrolle des Staates vorstellt: „Dies kann dadurch geschehen, daß die verwendeten Schlüssel sicher hinterlegt werden. Durch eine Kombination von organisatorischen, personellen, technischen und juristischen Maßnahmen kann jedem Verdacht einer Mißbrauchsmöglichkeit begegnet werden."

Das war am 28 April 1997!

Es ist keine Forderung abstrus und blöd genug, als dass sie nicht irgendeinem merkbefreitem Politiker einfallen würde, wenn es um das Internet geht.

Die Pakistanis werden also jetzt die Tatsache, dass sie verschüsseln, verbergen. Das geht mit Steganografie.

Ich habe hier schon mehrfach zum Thema was geschrieben: Am 10.02.2007: „Geheimes Schreiben gegen Schäuble", oder gar am 16.09.2003: „Für Rätselfreunde: Steganografie für Dummies".

Kampagnero Ziercke

Daten-Speicherung.de beweist, dass der Chef des Bundeskriminalamts ein Lügner ist. Und ein Dummschwätzer obendrein. (via law blog)

„Vor einigen Tagen forderte der Präsident des Bundeskriminalamts (BKA), Jörg Ziercke, von der

Bundesregierung wieder einmal eine flächendeckende Speicherung aller Verbindungsdaten in Deutschland zum „Kampf gegen Kinderschänder'“. Für seinen Lobbyismus pro Totalüberwachung ist Ziercke fast jedes Mittel recht – die Lüge allemal.

Gefällt mir gefällt mir nicht

Stephan Weichert in der BZZ Online (komplett linkfrei): „#Journalist 2.0 – Was die mobilen und interaktiven Medientechniken für die Zukunft des Journalismus bedeuten“.

Der Journalismus befindet sich seit geraumer Zeit in einer betörenden Begriffswolke aus Neologismen: Web2.0, Social Media, Crowdsourcing, Open Source oder User Generated Content sind nur einige der Schlagworte, die den Beruf und seine Kernbestimmung zu vernebeln drohen. Einst zu Kennziffern eines zeitgemässen Neo-Journalismus erhoben, taugen die Worte inzwischen nur noch als abgewetzte Marketingfloskeln. (…) Neue Studien belegen zumindest, dass soziale Medien bisher überschätzt wurden. (…) Von vereinzelten Vorreitern guten Community-Reportings wie der Wochenzeitung «Freitag» einmal abgesehen, atmet das, was in Deutschland heute journalistisch umgesetzt wird, noch zu wenig den Geist eines New Digital Journalism, wie er zum Beispiel an der Aufbruchsstimmung bei

einigen Internetangeboten in den USA erkennbar ist.

Natürlich lobt Weichert den Freitag, er ist dort auch Autor. Und was zum Teufel ist „Community-Reporting“?

Der Besinnungsaufsatz enthält aber einige Ideen zum weiterdenken.

Zum Thema passt Heise: „Facebooks ‚Like‘-Button im Visier deutscher Datenschützer“.

Das ULD hat offenbar die „Like“-Funktion schon länger im Visier. Heute veröffentlichte es eine ausführliche technische Analyse der Usertracking-Möglichkeiten, die Facebook ohne ausdrückliche Genehmigung der Nutzer ermöglicht, darunter eben die auf fremden Webseiten platzierten Social-Plug-ins wie der Like-Button. Binden Site-Betreiber den Button ein, kann Facebook anhand der Cookies die Nutzer erkennen.

I disagree. Wer so bescheuert ist, mit eingeschalteten Cookies zu surfen, der ist doch selbst schuld, und Mitleid ist nicht angebracht: „Datenschützer warnen vor den überall auftauchenden Gefällt-Mir-Buttons von Facebook. Tatsächlich übermittelt er persönliche Daten, auch ohne dass man ihn angeklickt hat“, heisst es bei Heise.

Journalisten, die per Smartphone ihren Standort allen möglichen Datenkraken verraten, weil ein Smartphone geil und chic und cool ist, die haben ihr Gehirn eh an der Gardeobe abgegeben.

How do websites block Tor

nodes?

Der Friederich, der Friederich, das war ein arger Wüterich! Jetzt fordert er „das Ende der Anonymität im Internet“. Bruhahaha.

Wie will er denn das durchsetzen? Wieso hat ihn das beim ehemaligen Nachrichtenmagazin niemand gefragt? Waren sie in Ehrfurcht erstarrt? Oder hat man bei der Ausbildung der Redakteure vergessen zu lehren, dass es nicht die Aufgabe von Journalisten ist, die Propaganda von Behörden zu verbreiten? (Die Leute, die dafür zuständig sind, nennt man „Pressestellen“.)

Übrigens muss ich hier das mir bisher unbekannte Blog Rentner-News lobend erwähnen. „Innenminister Friedrich fordert Zensur“ liest man da. Das ist zwar technisch gesehen nicht ganz richtig, aber inhaltlich ein Schritt in die richtige Richtung.

Friedrich kann sich darauf verlassen, dass die Mainstream-Medien seine Agitprop kritiklos wiederkäuen, ohne dass irgendjemand das Publikum darüber aufklärt, wie dämlich und technisch unsinnig die Forderung des Innenministers ist. Ihm geht es ja nur darum, einen Stein ins Wasser zu werfen und die medialen Wellen zu beobachten, die entstehen.

By the way: Sogar in der Mailingliste des Tor-Projekts kann man nachlesen, wie Websites den Anonymisierungdienst blocken können (Wikipedia macht das schon lange):

You can generate a list of Tor IPs that allow exiting to your IP(s) at https://check.torproject.org/cgi-bin/TorBulkExitList.py, or use the TorDNSEL service https://www.torproject.org/projects/tordnsel.html.en Services should never block Tor users altogether, but instead implement rate limiting, read-only access, etc, and unblock

Tor after a few days or weeks.

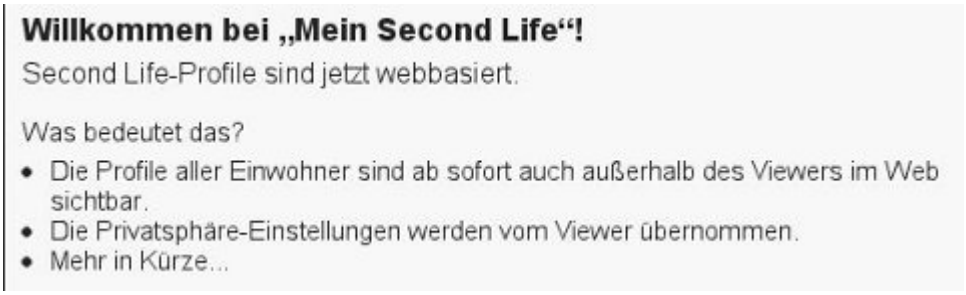
Letzteres werden die Chinesen natürlich nicht beherzigen.

Second Life Facebook Style

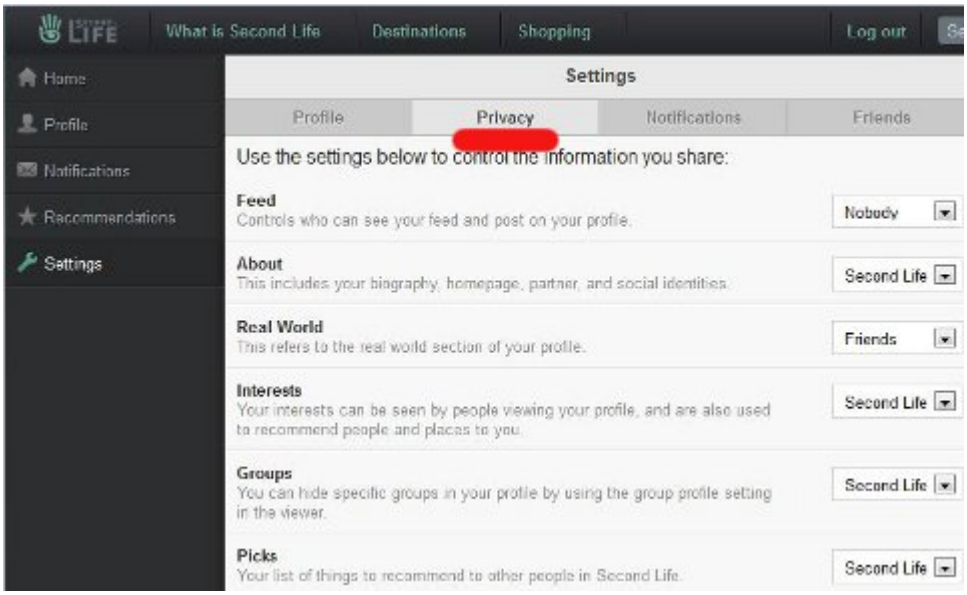
Die größte 3D-Welt Second Life geht einen Schritt in Richtung Facebook. Die Profile, die man im Avatar über sich selbst anlegen kann, sind jetzt im World Wide Web einsehbar; man muss also nicht mehr einen speziellen Viewer benutzen.

Krypton Radio schreibt: *San Francisco based Linden Lab (LL), creators of the virtual world Second Life (SL), have taken the next step in what appears to be their overall plans to merge SL with the social media craze that has been sweeping the internet for many years now. The public profiles of SL users*

have now been changed to work more like the well known Facebook wall, allowing other users to post comments on the profiles of anyone who has it turned on, and it's turned on by default. Originally a users profile could only be seen by another user while logged-in and in-world, but as Linden Lab pushed its next-gen Viewer project, it moved the profiles to website based.



Die Geschäftsidee von von LindenLab unterscheidet sich überhaupt nicht von der anderer sogenannter „sozialer Netzwerke". Es geht immer und ausschließlich darum, die Daten und das Nutzerverhalten zu loggen und zu verkaufen. Das ist bei Google Mail ja auch nicht anders. Diese Unternehmen vertrauen darauf, dass 95 Prozent alles Nutzer dämlich sind und sich das gefallen lassen. Damit liegen sie richtig.



Man kann das Schlimmste verhüten (vgl. Screenshot):

To adjust your privacy settings, log into your profile via

https://my.secondlife.com/ Go to Settings, then Privacy, and you can set your Feed setting to Nobody. This will prevent anyone from using your Feed/Wall, and your other settings can only be set to a minimum of friends if you want to hide it from the general public. Also, the web-profiles work independently of your client, no matter what version you use. Using an older client will not disable this, you will still need to log into your web-profile in order to change your settings.

Mexiko-Deutschland: Folter in Kauf genommen

Informationsstelle Militarisierung (IMI) e. V.: „Nicht nur in Afrika erweitert die Bundesregierung ihr Engagement in Bezug auf Waffenexporte und Sicherheitszusammenarbeit. Der Export von Rüstungsgütern nach Mexiko explodierte seit der Amtsübernahme des mexikanischen Präsidenten Felipe Calderón. Laut den Rüstungsexportberichten der Bundesregierung pendelt das Volumen, das sich zuvor nur im unteren sechsstelligen Euro-Bereich bewegte, seit 2007 zwischen 2,5 und 4,1 Millionen Euro. Dabei ist die vereinbarte Lieferung von zwölf Militärhubschraubern durch den Rüstungsexportbericht nicht einmal erfasst. Ferner geht es um eine verstärkte Zusammenarbeit im Hinblick auf organisierte Kriminalität und Terrorismus. In diesem Rahmen stehen auch Ausbildungs- und Ausstattungshilfen für die Polizei zur Debatte, mit denen bewusst Folter in Kauf genommen, ja unterstützt wird…“ (via Womblog)

Aktive Wanzen

Netzpolitik.org: „Es war ja davon auszugehen, dass die offengelegten Wanzen der Polizei nicht mehr in Betrieb, bzw. nicht mehr erreichbar sein würden (…) Nur um uns zu vergewissern haben wir mal ein paar der Nummern angerufen. (…) Die Wanzen sind allem Anschein nach nicht nur noch aktiv, sondern auch in keiner Form gegen unauthorisierten Zugriff geschützt.“

Ganz großes Kino.

HackerLeaks

PC Magazin: „Auf der Website gibt es bereits seit dem 24.6. diverse Einreichungen. Will ein Hacker Material an Hackerleaks übergeben, kann er für kleine, rein textliche Übermittlungen bis 2 MB einen Account bei PrivacyBox , einem Dienst des German Privacy Foundation e.V. nutzen.“

Medientrojaner

Der dümmste anzunehmende Historiker nennt das Pferd, mit dem sich laut Homer die Griechen in die Stadt Troja schmuggelten, „Trojaner“ bzw. er nennt die Griechen Trojaner, obwohl die Trojaner draussen waren und die Griechen drinnen. Man kann ja

auch die Deutschen Franzosen nennen oder die Russen Amerikaner, ist irgendwie sowieso egal.

So falsch, schräg und unpassend die Metapher „Trojaner“ für eine Software ist, die – so stellt sich das Klein Fritzchen vor – irgendwie auf einen fremden Rechner geschmuggelt wird, etwa mit Hilfe von Zauberformeln, die ein Beamter in Wiesbaden beim BKA vor sich hin murmelt, während er eine ausführbare Datei an einen verdächtigen Menschen schickt, in der Hoffnung, der benutze das Betriebssystem Windows und würde alles per Mausklick und per Admin-Account installieren, was nicht bei drei auf dem nächsten Baum ist – es hindert die Holzmedien dennoch nicht, diesen Quatsch wieder und wieder zu verbreiten.

Aktueller Fall, Zitat Spiegel ~~online~~: Das Münchener Justizministerium habe eingeräumt, „dass die [*welche? B.S.*] umstrittene [!] Spionage-Software zwischen 2009 und 2010 insgesamt fünfmal [sic] in Augsburg, Nürnberg, München und Landshut zur Anwendung kam.“

Man merkt schon bei diesem Deutsch des Grauens, dass hier irgendjemand irgendwelche Behörden-Agitprop abgekupfert hat – so redet kein Mensch: „zur Anwendung kam“? Das Gehirn des Schreibers kam offenbar nicht zur Anwendung. Wer wendete was an – und vor allem wie?

Und nur ganz nebenbei: „banden- und gewerbsmäßiger Betrug“ und „Handel mit Betäubungs-und Arzneimittel“ sind keine Straftatsbestände, bei denen das Bundesverfassungsgericht den Einsatz von Spionage-Software auf Computern erlaubt hätte. Den Bayern scheint das legal, illegal, scheissegal zu sein. Wundert mich nicht.

Jetzt aber die Pointe:
„Die Fahnder fanden trickreiche Wege, zum Aufspielen der Trojaner: einmal half der Zoll am Münchener Flughafen, einmal wurde der Spion per Remote-Installation aufgespielt, dreimal nutzen die Ermittler das Durcheinander einer

Hausdurchsuchung.“

Das muss man sich auf der Zunge zergehen lassen. Zum ersten, liebe Spiegel-Redakteure, gibt es hier sowieso nicht mindestens zwei unabhängige Quellen, sondern nur das, was die Behörde von sich zu geben beliebt. Ihr hättet das überprüfen oder anmerken müssen: „Die Behörde behauptet das.“

Zum zweiten und mal ganz langsam von vorn: Hier handelt es sich um Software zum Mithören von Skype. **Das ist etwas ganz anderes als die real nicht existierende Online-Durchsuchung. Und mehr als Internet-Telefonie zu belauschen kann die Software nicht. Wann kapiert ihr das endlich?**

Lauschen wir Gulli.com: „Die Installation des so genannten Bayerntrojaners soll wahlweise durch einen Einsatz der Polizei vor Ort oder remote per E-Mail geschehen. (…) Die Schadsoftware kann Daten an und über einen Rechner außerhalb des deutschen Hoheitsgebietes versenden. Dabei kann Zugriff auf interne Merkmale des Skypeclients und auf SSL-verschlüsselte Websites genommen werden.“

O ja. Per Mail? Wie soll das gehen? Wenn der Verdächtige so bescheuert ist wie die Leute, die diesen Unfug wiederholen, ohne auch nur ein Milligramm Gehirnschmalz zu aktivieren, dann wird er auch zu dämlich sein, um ein Programm zu installieren (und das müsste er).

Bei der so genannten Online-Durchsuchung geht es mitnichten um das Belauschen von Internet-Telefonie, und Skype ist sowieso nicht sicher! Wie ich schon am 04.01.2008 in der Netzeitung schrieb:

Skype hat aber nicht nur ein Problem. In vielen Unternehmen ist es verboten, weil das Sicherheitsrisiko zu groß erscheint. Die Software verhält sich zu Firewalls und Routern wie ein Nashorn, wenn es in Wut gerät: Sie bohrt Löcher hinein, damit auch der dümmste anzunehmende Nutzer bequem plaudern kann und nicht erst in den digitalen Eingeweiden fummeln muss.

Wer sich um die Konfiguration der Privatsphäre nicht kümmert, könnte sich versehentlich von fremden Menschen abhören lassen. Eine Firma, die Skype einsetzte, verlöre auch die Kontrolle über den Datenverkehr. Deshalb raten Wirtschaftsverbände davon ab.

Der größte Nachteil von Skype ist prinzipieller Natur: Das Programm ist proprietär – also nicht kompatibel mit freier Software -, und der Gesprächspartner darf keine andere VoIP-Software nutzen. Die Innereien von Skype – der Quellcode – sind ohnehin ein Betriebsgeheimnis. «Security by obscurity» nennt man das System im Hacker-Milieu. Im Internet kursieren detaillierte Analysen wie «Silver Needle in the Skype», die die Schwachstellen der Software aufzeigen.

Für politisch denkende Zeitgenossen ist Skype ähnlich igitt wie Googles E-Mail-Dienst: Nutzer von Skype aus China bekommen einen Textfilter vorgesetzt, der bestimmte Worte nicht durchlässt. «Falun Gong» und «Dalai Lama» sind als verboten gesetzt. Diese Zensur kann nur funktionieren, weil die Betreiberfirma die Möglichkeit ab Werk eingebaut hat, die Gespräche mitzuprotokollieren und zu belauschen.

Das alles wird den normalen Nutzer nicht abschrecken. Der installiert manchmal sogar eine Webcam im Schlafzimmer, weil er nichts zu verbergen hat und nutzt das bekannte Betriebssystem eines rothaarigen Multimilliardärs, bei dem alle relevanten Sicherheitsfeatures ab Werk ausgestellt sind.

Welche „trickreichen Wege“ nutzten also die Beamten ganz legal, illegal, scheissegal? „Per Remote-Installation aufgespielt“ – könntet ihr hier mal ins Detail gehen? Welche IP-Adresse attackieren sie denn, oder wurde dem Verdächtigen eine per Einschreiben mit Rückschein vorher aufgezwungen?

„Nutzen die Ermittler das Durcheinander einer Hausdurchsuchung“ – ach ja? So geht das also in Bayern zu, das überrascht mich nicht. Da kann ich ja froh sein, dass die

Beamten, die meine Wohnung durchsuchten, nicht alle Buchregale umgeworfen, das Geschirr auf den Boden und die Monitore mal eben so umgestoßen haben? Wie kann man so etwas als Journalist einfach kritiklos „vermelden“, wie es in grauenhaften Journalisten-Neusprech heutzutage heißt? Wenn das in China passierte – „die Ermittler nutzen das Durcheinander einer Hausdurchsuchung“ -, dann würdet ihr alle heuchlerisch jammern und klagen.

Verlogenes unkritisches obrigkeitshöriges Pack! Das kotzt mich wirklich an. Und ihr habt keinen Schimmer von dem, wovon ihr schreibt.

Nur ganz nebenbei: Wie hätte denn bei mir jemand während der Hausdurchsuchung etwas auf meine Rechner „spielen“ können? Die waren ausgeschaltet, und ich hätte notfalls einfach die Stecker rausgezogen, wenn dem nicht so gewesen wäre.

Unstrittig ist, dass, wenn man den physischen Zugriff auf einen Rechner hat und wenn der eingeschaltet ist und/oder von Fremdmedien bootet, recht viel möglich ist. Aber das geht bei Leuten nicht, die einen Rechner von einem Videorecorder unterscheiden können. Aber vielleicht irre ich mich ja, und meine Mitmenschen sind noch dämlicher als ich eh schon annehme.

Grün-Rot für Vorratsdatenspeicherung

Das grün-rot regierte Baden-Württemberg will sich auf der Innenministerkonferenz am Mittwoch in Frankfurt am Main dafür einsetzen, dass die Vorratsdatenspeicherung wieder eingeführt wird. (Heise)

Wer hat uns verraten? Grüne und Sozialdemokraten!

Phishing-Angriff auf den Internationalen Währungsfonds

Ein Leserkommentar im Heise-Forum: „Wenn eine Firma oder Institution, erst recht, wenn diese mit sensiblen Daten zu tun hat, ihre Mitarbeiter nicht halbwegs zu schulen in der Lage ist, wie man mit solchen Mails umzugehen und dass man eben nicht wahllos auf Links zu klicken hat … sorry, dann hat sie es einfach nicht anders verdient als ausspioniert zu werden. Vermutlich findet man in den Papiermüll-Containern hinterm Haus auch massenhaft Akten in einwandfreiem Zustand inkl. Stempel ‚Streng geheim!'“

Ich finde, dass man eine Firma, die keine vernünftige E-Mail-Policy hat, deren Mitarbeiter noch nicht einmal mit Javascript umgehen können und die so doof sind, dass sie auf Phishing hereinfallen, sogar noch Strafe zahlen müsste.

Bericht der EU-Kommission zur Evaluation der Vorratdatenspeicherung

Die EU-Kommission hat heute einen Bericht zur Evaluierung der Vorratsdatenspeicherung vorgelegt.

Der Arbeitskreis Vorratsdatenspeicherung schreibt in seiner Bilanz dazu:

„Die verdachtsunabhängige und wahllose Vorratsdatenspeicherung ist die am tiefsten in die Privatsphäre eingreifende und unpopulärste Überwachungsmaßnahme, die die EU bis heute hervorgebracht hat. Die EU-Richtlinie zur Vorratsdatenspeicherung verpflichtet alle EU-Staaten zur wahllosen Erfassung und Sammlung sensibler Informationen über soziale Kontakte (einschließlich Geschäftsbeziehungen), Bewegungen und das Privatleben (z.B. Kontakte zu Ärzten, Rechtsanwälten und Strafverteidigern, Betriebsräten, Psychotherapeuten, Beratungsstellen usw.) von 500 Millionen

Europäern, die sich keines Fehlverhaltens verdächtig gemacht haben. Einer Umfrage zufolge lehnen 69,3% der Bürger eine Vorratsspeicherung aller Verbindungsdaten ab – kein anderes ‚Überwachungsgesetz' einschließlich biometrischer Pässe, Zugang zu Bankdaten, Online-Durchsuchung und Fluggastdatenspeicherung stößt auf so starke Ablehnung."

In einer Stellungnahme des AK Vorrat heisst es:

„Mit ihrem jetzt vorgelegten Bericht gesteht die EU-Kommissarin in vielerlei Hinsicht Fehler und Risiken einer Vorratsdatenspeicherung ein. Allerdings vermeidet Frau Malmström die einzig richtige Konsequenz daraus, nämlich die Abkehr vor einer flächendeckenden Erfassung aller Verbindungsdaten. Der Bericht der EU-Kommission ist ein politisches Dokument und nicht das Ergebnis einer unabhängigen und wissenschaftlichen Standards genügenden Wirksamkeitsanalyse, die den Namen Evaluierung verdient hätte. Die von der EU-Kommission angeführten Statistiken und Einzelfälle belegen die Notwendigkeit einer Erfassung aller Verbindungsdaten nicht. Die EU muss zur Kenntnis nehmen, dass eine Vorratsdatenspeicherung weder die Quote der aufgeklärten Straftaten erhöht noch die Zahl der begangenen Straftaten vermindert hat."

Bei Heise gibt es mehr dazu: „Die Nachweise, die EU-Länder für die Erforderlichkeit der tief in die Grundrechte einschneidenden Maßnahme erbracht hätten, seien zwar „begrenzt" gewesen, räumt die Brüsseler Regierungseinrichtung ein. Trotzdem verwiesen sie auf die wichtige Rolle, welche die Aufbewahrung von Telekommunikationsdaten für Ermittlungen spiele. (…) … eine Studie des Wissenschaftlichen Dienstes des Bundestags hat aber bereits herausgefunden, dass die Vorratsdatenspeicherung in der EU die Aufklärungsquote in Ländern mit entsprechenden Auflagen nicht entscheidend verbessert hat. (…)

Für Alvaro zeigt die ‚mit siebenmonatiger Verspätung'

vorgelegte Evaluierung, dass ‚wir einem Wildwuchs an nationaler Willkür gegenüberstehen'“.

„In manchen Ländern greift die Küstenwache auf die Vorratsdaten zu, in anderen reicht für Sicherheitsbeamte ein schriftlicher Beleg, damit sie die privaten Daten der Bürger einsehen dürfen. Auch bei den Zugriffszahlen gibt es eklatante Abweichungen. So sind die polnischen Behörden alleine für die Hälfte der jährlich circa zwei Millionen europäischen Zugriffe auf Vorratsdaten verantwortlich. Einen statistischen Nachweis für den Nutzen der Richtlinie kann die Kommission jedoch wie erwartet nicht vorlegen.“

Quod erat demonstrandum.

Datenschutzgründe

Ich verstehe diese „Datenschutzgründe“ nicht. Ein DAU loggt sich bei Facebook ein und bleibt eingeloggt, auch wenn er ganz

woanders hin surft (wieso sollte man sich so bescheuert verhalten?) – und Spiegel Online loggt dann die IP-Adresse, aus „Datenschutzgründen“? Seid ihr denn völlig irre? Oder habe ich jetzt etwas missverstanden?