Unter Propagandisten

Jemand fragte bei Heise: „Wie genau schafft es Russland verschlüsselte Kommunikation aufzubrechen? Ich bin bisher davon ausgegangen, dass man das nur mit dem Einsatz von Trojanern auf dem Gerät des Nutzers hin bekommt. Welchen Beitrag die Kompromittierung der Netze dazu hat, ist mir nicht klar.“

Ich hatte geantwortet, dass der Autor des Artikels, Stefan Krempl, nur die „Propaganda der Sicherheitsbehörden“ wiedergebe. So war das auch beim Thema „Online-Durchsuchung“.

Mein Beitrag würde von Heise ~~wegen Hassrede~~ gesperrt. Die sind ganz schön dünnhäutig. Also habe ich offenbar einen Nerv getroffen.

Ich erinnere an Annette Ramelsberger in der „Süddeutschen“: „Den meisten Computernutzern ist es nicht klar: Aber wenn sie im Internet surfen, können Verfassungsschützer oder Polizei online bei ihnen zu Hause auf die Festplatte zugreifen und nachschauen, ob sie strafbare Inhalte dort lagern – zum Beispiel Kinderpornographie oder auch Anleitungen zum Bombenbau.“

Auch das nenne ich „die Propaganda der Sicherheitsbehörden

wiedergeben“. Journalismus ist das nicht.

Trojaner auf externen Internet-Festplatten

Darstellung einer Online-Durchsuchung mit „Staatstrojaner“ aus Zachiku, Mittani-Reich, ca. 1550 – 1350 v. Chr., Fundort Mosul-Stausee im Irak

Krempl liefert bei Heise wieder den gewohnten Bullshit ab: „Strafverfolger haben Staatstrojaner 2021 häufiger eingesetzt. Die Gerichte genehmigten 2021 55-mal das Hacken von IT-Geräten, während es 2020 48 Anordnungen gab.“

Ach ja? Wie machten die das? „Mithilfe von Staatstrojanern“ natürlich. „Dabei dürfen die Fahnder etwa auch Festplatten inspizieren und nicht nur die laufende Kommunikation mitschneiden.“ Die Internet-Festplatten sind schon seit 2006 als Textbaustein in Mode.

Ich halte das für ein fettes Lügenmärchen aus der Propaganda-Maschine der Strafverfolger, das Krempl wie gewohnt kritiklos wiederkäut. Natürlich können die üblichen Verdächtigen

„Kommunikation“ in Echtzeit verfolgen, etwa bei der Telefonie. Aber sie können nicht einfach so auf externe „Festplatten“ zugreifen, schon gar nicht „von weitem“, außer der Verdächtige ist so bekloppt, dass er vermutlich gar keinen Computer bedienen könnte.

Außerdem gab es da mal ein Urteil des Bundesverfassungsgerichts. Jemand kommentierte ganz richtig: „Zunächst mal heißt es eben nicht, daß das Instrument auch eingesetzt wurde, nur weil ein Richter die Erlaubnis erteilt hat. Und weiterführend sagt das auch nichts darüber aus, ob es erfolgreich eingesetzt wurde, ob verwertbare Informationen erlangt wurden, die sonst nicht erlangt worden wären, usw..“

Darstellung einer Online-Durchsuchung mit „Staatstrojaner“ aus Zachiku, Mittani-Reich, ca. 1550 – 1350 v. Chr., Fundort Mosul-Stausee im Irak

---

Surveillance, allüberall und nirgends [Update]

Midjourney/©Burks

Heise veröffentlicht Bullshit-Bingo für Klein-Fritzchen, natürlich von Stefan Krempl. Ich weiß nicht, was den treibt. „Polizei soll Staatstrojaner nicht mehr bei Alltagskriminalität einsetzen.“

– Erstens heißt es nicht „Staatstrojaner“. Die Trojaner waren draußen, die Griechen saßen im Pferd.

– Zweitens darf die Polizei das nicht (was sie natürlich nicht daran hinderte). Es gibt ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Oder ist die Entscheidung des Bndesverfassungsgerichts mittlerweile revidiert worden, Heise? Nein, ist sie nicht.

Midjourney/©Burks

– Drittens ist es technisch grober Unfug, auch wenn tausend juristische Pappnasen das immer wieder anders behaupten. Man sollte auch nicht die Transportverschlüsselung mit der Verschlüsselung von Inhalten auf einem Rechner verwechseln. Nur noch einmal, Krempl, zum langsamen Mitschreiben: **niemand** (in Worten: niemand) kann auf meine Rechner von „draußen“ zugreifen, selbst wenn ich einen Angriffskrieg vorbereitete. **Niemand** hat auch bisher erklärt, wie das gehen sollte. Die raunen nur alle geheimnisvoll herum und tun sich wichtig damit.

Ohne weiteres kann der Staat jedoch nicht erfassen, was auf einem Computer geschieht. Der einzige Weg ist über Sicherheitslücken in den betroffenen Systemen. Und hier muss man sich schon wundern: Statt, dass der Staat hilft, bekannte Lücken zu schließen oder zumindest auf sie aufmerksam zu machen, die letztlich alle Nutzer von Computern gefährden und

von Kriminellen ausgenutzt werden können, nutzt er sie selbst aus, um das Gerät zu hacken und „mitlesen“ zu können. (Das „schreiben Mitarbeiter der intersoft consulting, die als Experten für Datenschutz, IT-Sicherheit und IT-Forensik international Unternehmen beraten.“)

Der Staat nutzt also Lücken aus? Wie denn? Beispiele?! Das Bundesinnenministerium kauft also Zero-Day-Exploits, womöglich für Linux? Ihr spinnt doch.

Midjourney/©Burks

– Viertens gibt es die „Online-Durchsuchung“ weder bei „Alltagskriminalität“ noch bei schweren Straftaten, nur im nachhinein, wenn die Rechner des Verdächtigen beschlagnahmt wurden und dieser auch noch ein IT-Vollidiot ist.

Was will mir dieser Artikel suggerieren? „Bei der Quellen-TKÜ geht es darum, die laufende Kommunikation per Staatstrojaner direkt auf dem Gerät eines Verdächtigen abzugreifen, bevor sie

ver- oder nachdem sie entschlüsselt wurde.“ Ach ja? Und wie soll das gehen? Krempl, du bist ein Verschwörungstheoretiker.

Dazu passt noch ein ganz ähnlicher Artikel: „Autos, Navis & Co.: Polizei will Zugriff auf alles – unverschlüsselt und sofort“. Schon klar. Ich will auch Diktator von Deutschland werden. Das ist ähnlich realistisch, selbst wenn diejenigen, die das fordern, Nachhilfeunterricht beim Chinesen nähmen.

Midjourney/©Burks

[Update] Links repariert.

Praktisch unbemerkt

surveillance blacklight::1 grayscale color::1 –v 4 –chaos 100 –s 750

Netzpolitik.org und Heise berichten synchron: EU-Länder wollen Blankoscheck zum Ausspionieren von Journalisten.

Das finde ich super. Dann lernt die Journaille endlich auf die harte Tour, sich mit Überwachung zu beschäftigen und sich davor zu schützen. Oder glaubt jemand ernsthaft, die herrschende Klasse hielte sich an die eigenen Gesetze? Warum dieses Gejammer und Apellieren an den Staat, das Gute zu tun und das Böse zu lassen? Seriously?

So sollen solche Überwachungsprogramme „im Einzelfall aus Gründen der nationalen Sicherheit“ verwendet werden dürfen oder „im Rahmen von Ermittlungen zu schweren Straftaten“. Was haben wir gelacht. Was genau ist die „nationale Sicherheit“ und wer bestimmt das? Und sind wir nicht alle irgendwie

Einzelfälle?

Jeder kann sich übrigens Journalist nennen. Das ist keine geschützte Berufsbezeichnung. Um wen geht es dann? Auch um Blogger oder „Influencer“?

Stefan Krempl, der schon zur so genannten Online-Durchsuchung viel Unsinn von sich gab, schreibt auch hier wieder vom „Staatstrojaner“. Netzpolitik.org macht mit dem Bullshit-Bingo weiter: *Das Mittel der Wahl bei den Überwachungsaktionen: Staatstrojaner. Berüchtigt ist insbesondere Pegasus, ein Trojaner der israelischen Firma NSO Group, der Handys praktisch unbemerkt infiltrieren kann. Dadurch kann selbst verschlüsselte Kommunikation über Dienste wie WhatsApp oder Signal ausgelesen werden. Journalisten, die mit Pegasus oder anderen Trojanern gehackt wurden, müssen die Preisgabe ihrer Quellen fürchten.*

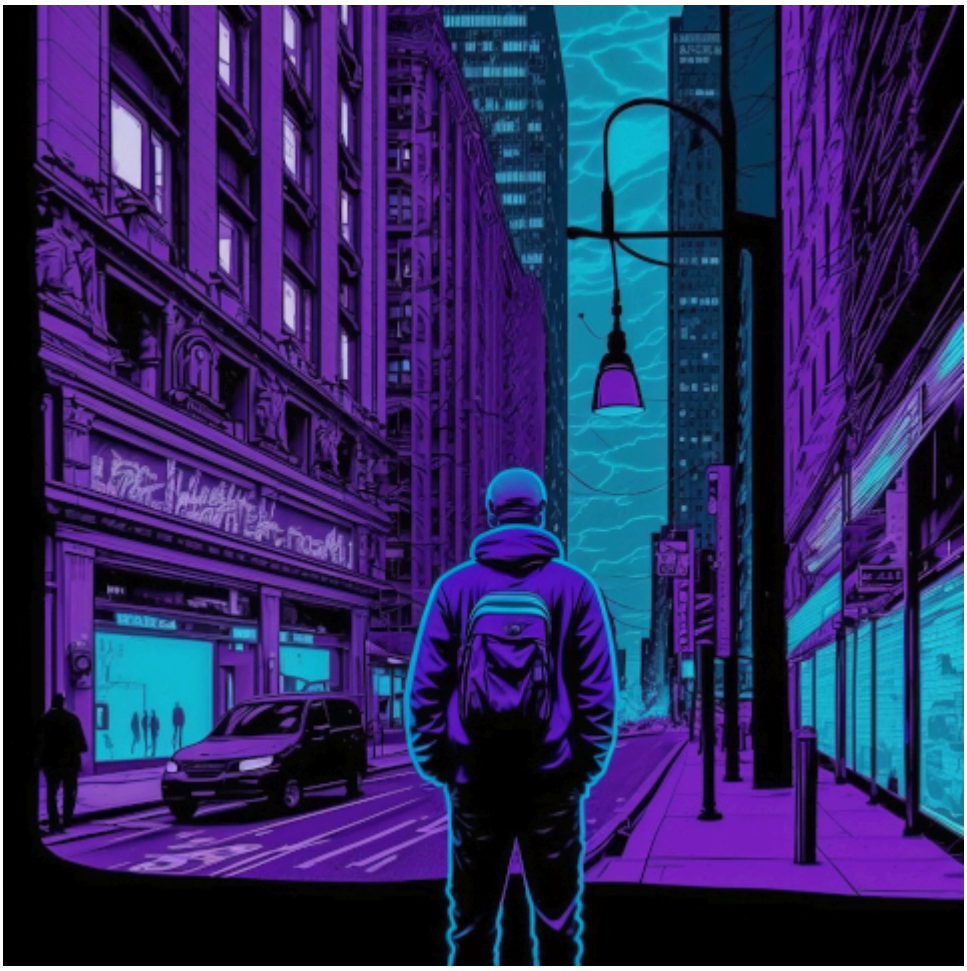
Falsch. Auf meine Rechner kommt nichts, was ich nicht erlaubt habe. Pegasus kommt auch nicht auf mein Android-Smartphone, weil ich alle „Infektionswege“ kenne und vermeide. *Der Angriff erfolgt grundsätzlich über iMessage in Form einer Nachricht mit einem Link zum Anklicken.* Warum zum Teufel sollte ich in einer „iMessage“ (was soll den das sein?) auf einen Link klicken, wenn ich nicht weiß, wohin der führt, zumal der Absender ohnehin unter Spam-Verdacht steht, wenn ich ihn nicht kenne? Wenn ich lese „der Handys praktisch unbemerkt infiltrieren kann“, schwillt mir der Kamm. Und theoretisch unbemerkt? Das ist genau dieses vage Gefasel wie bei der „Online-Durchsuchung“, das die Fakten haarscharf umgeht oder nicht erwähnt.

„Das Hacken von Geräten ist somit nur in Ausnahmefällen erlaubt, nämlich wenn eine konkrete Gefahr besteht, schreibt Wikipedia. Und wie wollen die mich hacken? Nur zu! Ich brauche keine Gesetze, „solchen Übergriffen einen Riegel vorzuschieben“.

Vielleicht sollt ich die NSO Group mal interviewen und sie fragen, ob sie ein Staatstrojaner-Konzern sind oder nicht vielmehr ein Staatsgriechen-Konzern? Die würden sich totlachen. Und wie die sich das mit Linux, PGP, Veracrypt usw. vorstellen? Und vor allem mit Gar-Nicht-Irgendwo-Draufklicken? Und was ist mit Mutt und Clawsmail, die das Klicken bei Strafe des In-einen-virtuellen-See-geworfen-Werdens sowieso nicht wollen?

Diese hyperventilierende Berichte verschweigen die beiden wichtigsten Fakten: 1. Überwacht wird nur der, der es fahrlässig erlaubt. 2. Wer glaubt, der Ausschuss, der die Geschäfte der Bourgeoisie organisiert, hielte sich, wenn es darauf ankommt, an Gesetze, ist naiv und entsetzlich dumm.

Schön, dass wir darüber geredet haben.



User: Warum nennen manche Leute eine Überwachungssoftware „Staatstrojaner“, obwohl die Griechen im Trojanischen Pferd

saßen und die Trojaner draußen waren?

ChatGPT: Es ist wichtig, metaphorische Ausdrücke nicht wörtlich zu nehmen, sondern ihre symbolische Bedeutung zu verstehen. Der Begriff „Staatstrojaner“ soll verdeutlichen, dass die Überwachungssoftware heimlich in die Geräte eindringt, ähnlich wie die versteckten Krieger im Trojanischen Pferd. Es ist nicht beabsichtigt, dass die Überwachungssoftware tatsächlich „Staatsgriechen“ genannt wird.

User: Die versteckten Krieger waren aber Griechen. Ist die Metapher von einem „Staatstrojaner“ nicht irreführend, weil die Trojaner gar nicht versteckt waren?

ChatGPT: Du hast recht, die Metapher des „Staatstrojaners“ kann in Bezug auf die Geschichte des Trojanischen Krieges etwas irreführend sein. Im Mythos des Trojanischen Pferdes waren es tatsächlich die Griechen, die sich im Inneren des hölzernen Pferdes versteckten, während die Trojaner unwissentlich das Pferd in ihre Stadt brachten.

Cyberdings oder: Unter Staatsgriechen et al

Mykonos Vase, 675 v.u.Z., Archäologisches Museum Mykonos, älteste bekannte Darstellung des Trojanischen Pferdes

Ich muss noch die Cybernachrichten der letzten Tage aufarbeiten. Ich habe das vor mir hergeschoben, weil ich wusste, das ich mich ärgern würde. So war es auch.

Die Zwangsfilter, die in Betriebssysteme eingebaut werden wollten, sind zugleich das Allerletzte und das Allerlustigste. Ich möchte gerne mal die Gesichter der Leute sehen, die sich so etwas ausdenken: Eine Mischung aus Claudia Roth, Saskia Esken und Philipp Amthor?

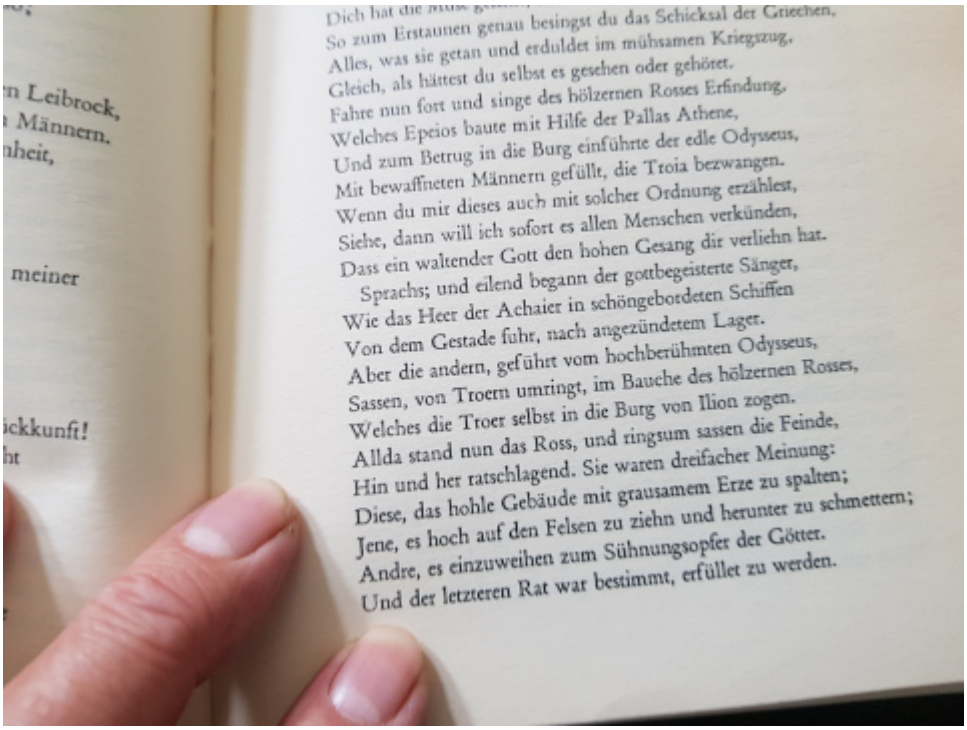
Dazu ein Kommentar bei Heise: *Ach, die drehen das so, dass freie Betriebssysteme ohne diesen Jugendschutzblödsinn plötzlich zu „terroristischem Werkzeug" umdeklariert werden. Der Bezug, Besitz und die Weitergabe werden dann pauschal als „Unterstützung einer Terrororganisation" eingetütet. +seufz+ … und Krieg ist Frieden.*

Dann haben wir noch die x-te Version vom Staatstrojaner. Manchmal möchte ich den Kollegen Krempl einfach nur ohrfeigen, wenn er zm 1000-sten Mal mit seinen schlampigen Begriffen Schlampiges daherschreibt. Und warum müssten Journalisten bürokratisches Neusprech wie „Quellen-TKÜ plus" übernehmen?

Das ist doch sowieso alles Unfug. Seit dem Erscheinen meines Buches hat mir immer noch niemand die Frage beantwortet, *wie* mir jemand ein Programm unterjubeln könnte, ohne dass ich mich vorher total bekloppt verhalten hätte? (FinSpy hatten wir hier schon.) Oder geht es gar nicht um meine Computer?

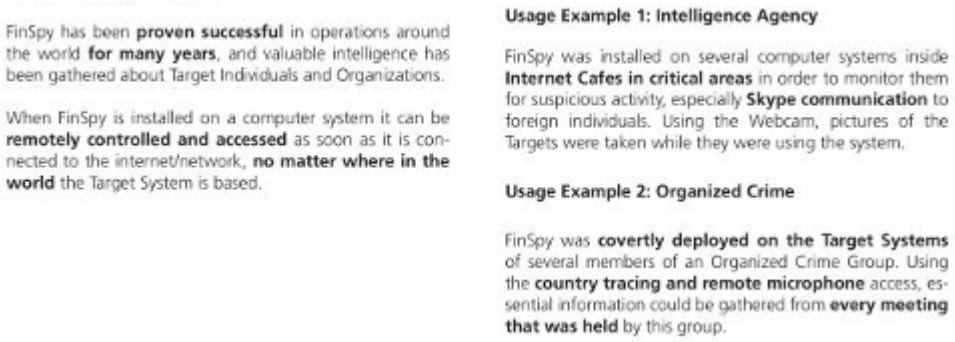
….sollte die Bundespolizei mithilfe des Bundestrojaners Messenger-Kommunikation etwa via WhatsApp, Signal oder Threema sowie Internet-Telefonate und Video-Calls… Gefasel und Bullshit-Bingo. Geht es nicht genauer? Mich regt noch mehr auf, dass die Journaille einfach nicht genauer nachfragt, sondern alles nachplappert. Netzsperren reloaded halt.

By the way: Ich hoffe nur, dass es keine Serienmörder oder andere Kriminelle gibt, die so wie ich heißen. Sonst müsste ich Google verklagen. Und ASCII ist jünger als ich. Ich weiß nicht, ob das gut oder schlecht ist.



Odyssee von Homer, übersetzt von Johann Heinrich Voss – obwohl das Pferd in den Gesängen der Osyssee gar nicht vorkommt, sondern in den Iliu persis.

Cyberdurchsuchung, die 894ste



FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

Usage Example 1: Intelligence Agency

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

Usage Example 2: Organized Crime

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Manchmal habe ich bei den offenbar hingeschlampten Meldungen von Heise, insbesondere von Stefan Krempl, den Eindruck, hier werde haarscharf an einer Verschwörungstheorie vorbeigeschrieben.

Es ist eindeutig eine urbane Legende, wenn man suggeriert, irgendein Cyberpolizist säße irgendwo vor dem Monitor und „hackte“ sich irgendwo in einen privaten Rechner. So etwas zu können behauptet noch nicht einmal FinSpy.

Auch Wikipedia faselt sinnfrei herum: „handelt es sich um einen Trojaner, da die Spionagefunktionen in einer harmlos aussehenden Hülle eingeschmuggelt werden.“ (Die Diskussionsseite ist gesperrt – vermutlich nicht zufällig.)

„Harmlos aussehende Hülle“? Geht es ein bisschen konkreter? Nein, weil das Blödsinn ist! Man kann trojanische Pferde (so heißt das und nicht „Trojaner“) nur auf einem „fremden“ Rechner implementieren, wenn man entweder den physischen Zugriff hat und der Rechner ungesichert ist oder wenn man per USB-Stick Software installieren kann, und das alles nur unter ganz bestimmten Bedingungen. Alles andere ist Voodoo und ein Hoax der allerfeinsten Sorte.

Wenn man sich die Passagen bei Wikipedia zur Quellen-Telekommunikationsüberwachung (was für ein Wort!) genauer anschaut, wird auch sofort klar, dass es sich weitgehend um heiße Luft handelt.

„Die Malware bestand aus einer Windows-DLL ohne exportierte Routinen“, schreibt der CCC in seiner Analyse. „Wir haben keine Erkenntnisse über das Verfahren, wie die Schadsoftware auf dem Zielrechner installiert wurde.“ Quod erat demonstrandum. Nur wie ich oben schrieb.

In einem Internet-Cafe ginge das natürlich, falls ein Richter das anordnete. Übrigens habe ich Linux. Und man müsste schon an meinem Stangenschloss hinter der Wohnungstür vorbei und einbrechen, um an meine Rechner zu kommen. Per USB geht bei mir auch nichts, meine BIOSSE (heißt das so?) verbieten das. Keylogger funktionieren bei Ubuntu oder XFCE auch nicht oder ich würde es merken.

Aber noch mal für Krempl zum Mitschreiben: Gefährder sitzen ausschließlich und immer an demselben Platz in immer demselben Internetcafe und nutzen ausschließlich Windows.

Hart zu Gericht

Heise (Krempl): „Hart zu Gericht mit dem Kurs der Urheberrechtsgesetzgebung auf deutscher und europäischer Ebene in den vergangenen Jahren gingen am Mittwoch Juristen und Wirtschaftsvertreter bei einem Fachgespräch im Ausschuss Digitale Agenda des Bundestags.“

Preisfrage: Wann tritt das handelnde Subjekt des Satzes auf, und ab wann bekommen Simultanübersetzer suizidale Gedanken?

Hart zu Gericht mit der dämlichen Unsitte, die gefühlt wichtigsten Wörter in einem Satz krampfhaft nach vorn zu beamen eingedenk der empirisch gar nicht verifizierbaren Tatsache, dass die Rezipienten nur den Anfang läsen und dann gleich wegzappten, ging Burks während des Kaffeetrinkens beim

Frühstück.

No backdoors, never ever

Heise berichtet ausführlich über den Vortrag Roger Dingledines (obwohl von Krempl geschrieben: lesenswert wegen vieler interessanter Details): „Eine Vertreterin des Justizministeriums sei auf die Kernentwickler zugekommen und habe davon gesprochen, dass der US-Kongress Washington das Recht gegeben habe, ‚alles mit Hintertüren zu versehen'. (…) Der nach Berlin ausgewanderte US-Netzaktivist freute sich besonders, dass Tor insgesamt den ‚Snowden-Sommer' überlebt habe. Er spielte damit auf Enthüllungen des NSA-Whistleblowers an, wonach sich der technische US-Geheimdienst an dem Anonymisierungsnetz bislang mehr oder weniger die Zähne ausgebissen habe."

Staatstrojanisches Pferd, revisited

Meine Schwester teilte mir mit, sie erwäge mir ein T-Shirt mit der Aufschrift zu schenken: „Ich bin kein Klugscheißer. Ich weiß es wirklich besser."

Heise (Stefan „Staatstrojaner" Krempl) formuliert immerhin nicht ganz verkehrt, es geht bei dem „Staatstrojaner" um eine Software, die Internet-Telefonie abhöre:

Die längere Zeit zum Abhören der Internet-Telefonie eingesetzten Staatstrojaner waren zuvor durch Veröffentlichungen des Chaos Computer Clubs (CCC) in Misskredit geraten und sollen vorläufig nicht mehr verwendet werden.

Nein, die staatliche Malware war schon vorher „in Misskredit" geraten, weil ich darüber ein ganzes Buch geschrieben habe, das Krempl tunlichst verschweigt.

Außerdem gibt es einen „Staatstrojaner" *so* gar nicht, wie es sich unbedarfte Verschwörungstheoretikerinnen denken – im Sinne einer Software, die heimlich „von außen" und ohne Wissen des Computer-Nutzers und *ohne physischen Zugriff* auf dessen Recher „aufgespielt" werden kann.

Der Heise-Artikel zeigt aber eines: Bisher waren die Behörden offenbar nicht in der Lage, selbst diese Software, von der sie träumen, zu bauen. Das heisst: Alle Medienberichte, die seit 2006 etwas anderes behauptet haben, sind gelogen oder frei erfunden oder – wie in den meisten Fällen – wüstes ahnungsloses Herumspekulieren.

Schauen wir doch mal in die Berliner Zeitung vom 07.12.2006 (sechs Jahre her):
Das Bundeskriminalamt soll künftig online in die Personalcomputer von Verdächtigen eindringen und sie nach „verfahrensrelevanten Inhalten" durchsuchen können. Bundesinnenminister Wolfgang Schäuble (CDU) habe jetzt den Haushaltsausschuss des Bundestages darüber in Kenntnis gesetzt, dass die entsprechenden Computerprogramme, mit denen über die vorhandenen Kommunikationsnetze auf die Festplatten mutmaßlicher Krimineller und Terroristen zugegriffen werden kann, derzeit entwickelt werden, meldete jetzt die Bild-Zeitung..

Ach?!

Was richtig ist: Der CCC, der zum Glück nicht nur aus Bogk und

Maguhn besteht, hat eine kommerzielle Software der Firma Digitask untersucht, die die staatlichen Behörden einsetzten, um Internet-Telefonie abzuhören, und die mehr konnte, als nur das. Dazu muss der Computer-Nutzer aber die Software für Internet-Telefonie aber vorher eigenhändig installiert haben.

Da aber die Zahnpasta schon aus der Tube ist, sind vernünftige Leute wie Jürgen Kuri von der c't fast allein auf weiter Flur (um mich selbst nicht zu nennen).

Bundesregierung und Spionage-Software: Dämlich oder zynisch

Krempl wirft bei Heise wieder Rauchbomben: „BKA hat in sieben Fällen Online-Durchsuchungen durchgeführt".

Dann schauen wir uns mal das Original an (Antwort der Bundesregierung auf eine Anfrage der Bundestagsfraktion der Linken): Es handelt sich um die schon vom CCC analysierte Spionagesoftware zum Abhören von Internet-Telefonie, die aber als Feature ermöglichte, andere Software zu laden und zu installieren (also alles).

Vgl. Spiegel Online: „Experten werfen Bundesregierung Vertuschung vor".

Vgl. auch Fefe.

Die Antworten der Bundesregierung sind einfach haarsträubend – entweder sind die dort total dämlich oder so zynisch, dass ihnen die Rechtsprechung des höchsten deutschen Gerichts total scheißegal ist. Vermutlich sogar beides.

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.

Lena in Gefahr – Terror-Alarm in Deutschland [2. Update]

Es fällt mir immer schwerer, *nicht* von gleichgeschalteten Medien in Deutschland zu sprechen. Der Vergleich hinkt natürlich, weil die Vorzensur aus der Schere in den Köpfen besteht, kombiniert mit Dummheit und Faulheit. Niemand zwingt Journalisten dazu, gequirlten Unsinn zu schreiben. (Ich dürfte gar nicht meckern, hätte ich doch einen guten Artikel selbst schreiben zu können, aber ich bin gestern zu spät ins Bett gegangen.)

Ich habe mir also zum Frühstück das angeschaut, was mir als „Nachrichten“ und „Fakten“ zum Thema „Terrorgefahr in Deutschland“ angeboten wird. Dass Stefan Krempl bei Heise das Märchen von den „heimlichen Online-Durchsuchungen“ wieder aufwärmt, wundert mich jedoch nicht.

Mit „gleichgeschaltet“ meine ich: Das, was eine Behörde verlautbart, wird unkritisch übernommen (inklusive der

suggestiven Sprachregelungen), ohne zu überprüfen, ob die Fakten stimmen. Im Sozialismus hieß eine derartige „Quelle“ schlicht „Agitprop“. Wenn viele Medien voneinander abschreiben, gilt eine These offenbar als verifiziert. Das war auch schon beim Thema Online-Durchsuchung so. Die Rheinische Post schießt den Vogel ab und gibt es auch noch zu: „Übereinstimmenden Medienberichten zufolge sollen die Festgenommenen einen größeren Anschlag in Deutschland geplant haben“. Dann *muss* es ja wahr sein, wenn alle anderen des Kaisers neue Kleider bewundern!

„Den Angaben zufolge wurde die Kommunikation der Männer überwacht. (…) Amid C. sei dafür verantwortlich gewesen, die ‚verschlüsselte und konspirative Kommunikation‘ untereinander sicherzustellen. Laut Ziercke war es den Behörden jedoch mit umfangreichen, monatelangen Überwachungsmaßnahmen gelungen, den mutmaßlichen Terroristen auf die Spur zukommen.“ (Focus) „Im Zuge der Ermittlungen hatte das BKA einen Trojaner für eine Online-Durchsuchung sowie eine Software für eine Telekommunikationsüberwachung auf seinem Rechner installiert.“ (Spiegel) „Das Bundeskriminalamt (BKA) ist den mutmaßlichen Terroristen durch Überwachung ihrer Handys und Computer auf die Spur gekommen.“ Süddeutsche) „Bei den Ermittlungen hatte das BKA dem „Spiegel“ zufolge einen Trojaner für eine Online-Durchsuchung sowie eine Software für eine Telekommunikationsüberwachung auf dem Rechner des Verdächtigen installiert.“ (FTD) „Den Angaben zufolge wurde die Kommunikation der Männer überwacht.“ Mitteldeutsche Zeitung)

Die FTD redet also von einem „Bundestrojaner“. Was aber soll das sein? Man kann einen Computer nur fernsteuern und überwachen, wenn man a) einen physikalischen Zugriff auf ihn hatte, b) wenn der Besitzer des Computers denselben nicht geschützt hatte und c) haben die Ergebnisse, die durch Spionage-Software auf einem Rechner gewonnen wurden, vor Gericht keinerlei Beweiswert, weil diese den Computer verändert. Man kann das vergleichen mit einem V-Mann, der eine

Neonazi-Kameradschaft gründet und diese dann auffliegen lässt. (Darüber habe ich ein ganzes Buch geschrieben.)

Die Taz gibt sich wenigstens Mühe: „Permanent waren 50 Leute in Observationstrupps und weitere 76 Beamten für sonstige Überwachungsmaßnahmen im Einsatz. Dabei wurden Wohnungen und Telefone abgehört, Emails mitgelesen. Auf Computern wurden Spähsoftware installiert und verschlüsselte Internet-Telefonate wurden schon im Computer, also vor der Verschlüsselung (mittels Quellen-TKÜ) erfasst.“

Aha. Bei der angeblichen „Online-Durchsuchung“ wird es sich um das Abhören von Skype gehandelt haben. Verschlüsselte E-Mails kann man nicht lesen, es sei denn, man hätte einen Keylogger installiert und protokollierte die Tastatur-Anschläge a priori mit. (By the way, taz: „Quellen-TKÜ“ ist Neusprech des Wahrheitsministeriums.)

Und was lehrt uns das alles? Schauen wir doch ein wenig genauer hin, um hinter den Nebelkerzen ein paar winzige Fakten erkennen zu können.

„Dort habe er von einem ‚hochrangigen Al Qaida-Mitglied‘ den Auftrag bekommen, einen Anschlag in Deutschland auszuführen. Wer der Auftraggeber konkret war, wollten weder Ziercke noch Bundesanwalt Rainer Griesbaum sagen. “ (taz) Ich weiß, wer es war – Adil Hadi al Jazairi Bin Hamlili!

Regimetreue Medien geben der Totalüberwachungs-Lobby jetzt breiten Raum: „‚In Deutschland besteht weiterhin eine konkrete Terrorgefahr‘, sagte Uhl der ‚Welt am Sonntag‘. Gleichzeitig zeige der Fall, dass die Nachrichtendienste zu wenig Eingriffsrechte besäßen. Denn die entscheidenden Hinweise erhielten die deutschen Ermittler von der amerikanischen CIA. (…) ‚Wir müssen wissen, mit wem die Terroristen kommunizieren, um ihre Netzwerke ausfindig machen zu können‘, sagte er. ‚Dafür brauchen wir die Vorratsdatenspeicherung.'“

Passt schon. Wir haben verstanden.

Vermutlich wird bei der Gerichtsverhandlungen, die vielleicht noch in diesem Jahr stattfinden, von den Vorwürfen nicht viel übrig bleiben. Aber das wird dann im Kleingedruckten stehen, das niemand mehr liest: „Bei der Hausdurchsuchung wurde kein Sprengstoff gefunden. Außerdem stellte das BKA fest, dass der Plan zur Herstellung eines Zünders gar nicht hätte gelingen können, weil die Terrorbastler die falschen Grillanzünder gekauft hatten."

Wie das? Stehen im Internet denn *falsche* Bombenbauanleitungen? Gehört es denn nicht verboten, *falsche* Bombenbauanleitungen zu verbreiten? (Akte aka Ulrich Meyer, übernehmen sie: „Es war unser Thema am vergangenen Donnerstag: Bombenbauanleitungen im Internet. Das Netz ist voll davon, Spezialisten haben über eine eigene Filtersoftware 680.000 Seiten weltweit aufgestöbert".)

„Dennoch erließ die BGH-Ermittlungsrichterin gegen alle drei Beschuldigte Haftbefehle." Quod erat demonstrandum.

Mich wundert, dass alle Medien, sogar die Krawallblätter, sich die einmalige Chance entgehen ließen, das Volk auf die anlass- und verdachtsunabhängige Totalüberwachung aka Vorratsdatenspeicherung mental einzustimmen. „Unterdessen verlautete aus Sicherheitskreisen, dass die drei Terrorverdächtigen einen Anschlag auf den Eurovision Song Contest geplant haben könnten. Allerdings hätten die Verdächtigen nicht konkret darüber gesprochen, hieß es." (Welt)

Burks.de hat daher die dazu passenden Schlagzeile gewählt.

„Sicherheitskreise": Das sind die Geheimdienstler, die Journalisten auf ihrer Gehaltsliste haben oder wissen, dass diese geschmeichelt sind, wenn man ihnen angebliche „vertrauliche Vorab-Informationen" zukommen lässt und die daher gern bereit sind, Agitprop, die man gern verbreitet hätte, Wort für Wort ohne Kritik zu publizieren.

„Die Terroristen wollen Lena umbringen. Das haben sie zwar nicht so gesagt, aber es könnte ja sein. Würden Sie das bitte so bei Welt Online veröffentlichen? Danke."

Update: EFF: „New FBI Documents Provide Details on Government's Surveillance Spyware". „The documents discuss technology that, when installed on a target's computer, allows the FBI to collect the following information"..blabla..und wie bekommt man das auf den Computer des Zielobjekts?

Guckst du hier (burks.de, 31. Juli 2007):

„… es geht um CIPAV: „FBI-CIPAV.exe Is an Unknown Application. Install Anyway?" Jetzt aber im Ernst: „Die Abkürzung steht für „Computer and Internet Protocol Address Verifier", zu Deutsch: Computer- und Internet-Protokoll-Adressen-Verifizierer. Dieses Programm ist in der Lage, auf dem Rechner des Verdächtigen die Internet-Verbindungen und angesteuerten Homepage-Adressen samt Datum und Uhrzeit aufzuzeichnen. Die in Fachkreisen Trojaner genannte Software erfasst auch weitere Daten wie das Betriebssystem des ausgehorchten Computers, den Namen des bei der Windows-Registrierung angegebenen Nutzers, Teile der Windows-Registrierungsdatenbank oder eine Aufzählung aller laufenden Programme. Im vorliegenden Fall übermittelte CIPAV einige dieser Informationen per Internet an die FBI-Rechner." Das ist aber ein ultraböhzes Programm, fast so böse wie das Betriebssystsem, auf dem es nur läuft.

Wired dazu: „[1] the FBI sent its program specifically to Glazebrook's then-anonymous MySpace profile … [2] „The CIPAV will be deployed through an electronic messaging program from an account controlled by the FBI. The computers sending and receiving the CIPAV data will be machines controlled by the FBI." … [3] More likely the FBI used a *software vulnerability*, either a published one that Glazebrook hadn't patched against, or one that only the FBI knows." Genau, Software-Lücken, von denen nur das FBI etwa weiß. (…)

Die *Welt* betont sehr deutlich, dass der Schüler offenbar „arglos“ etwas abrief, vermutlich so, wie das *Welt*-Redakteure machen mit ihrem Outlook und dem unverschlüsselten und mit Javascript-gespickten Spam, den sie das immer bekommen. Der Artikel ist also ein Schmarrn. Ich darf auf mein Blog vom 19.07.2007 hinweisen („Heise Hoax-verseucht“), in dem die Details zu CIPAV abgehandelt werden.“

2. Update: New York times: „Bild, Germany’s most widely read and generally reliable (sic!) newspaper, reported that the terrorist cell might have planned to hit the popular Eurovision Song Contest on May 14, though that event’s organizers said they had not been alerted to any such threat. „>. Qood erat demonstrandum. (via Überschaubare Relevanz)

Einen Trojaner von der Leine lassen

Der Heise-Kollege Stefan Krempl ist, wenn es um die real gar nicht existierenden „Online-Durchsuchung“ geht, für suggestive und unseriöse Formulierungen bekannt. Die aktuelle Überschrift seines Artikels „Rheinland-Pfalz lässt den Landestrojaner von der Leine“ ist nicht nur eine saudämlich schräge Metapher (das trojanische Pferd war nie an der Leine, soweit ich meinen Homer kenne), sondern unterschlägt auch alle Fragen, die ein seriöser Journalist stellen müsste, zum Beispiel diese: Wie wollen sie den Verdächtigen online finden? Und wie wollen sie in seinen Rechner heimlich einbrechen? Noch niemand hat mir eine Antwort gegeben. Es ist eine Schande, Krempl!

Ceterum censeo: Der Kaiser ist nackt! Es gibt keine „Online-

Durchsuchungen“!

[Bitte selbst ausfüllen] fordert [bitte selbst ausfüllen]

„Für kommendes Jahr wird ein Gesetzentwurf der US-Regierung erwartet, durch das Internet-Telefonate einfacher abgehört und verschlüsselte E-Mails sowie Chat-Nachrichten besser überwacht werden sollen“, berichten Heise und netzpolitik.org.

Wie will man verschlüsselte Nachrichten „überwachen“? Von einem journalistischem Text erwarte ich, dass derartige sinnfreie Textbausteine zerhauen und der Unfug, der sich in ihnen verborgt, dem Publikum deutlich gemacht werden. Auch IRC-Nachrichten kann man nicht „überwachen“; ja, man kann sogar verschlüsselt chatten.

„Das wirklich fürchterliche bei derart dummen Vorschlägen ist daher leider, dass helle Köpfe kostbare Zeit dafür opfern müssen, sich zu diesem Unsinn zu äußern“, steht bei netzpolitik.org. Full ack. Aber was das heisst, wissen die DAUs auch wieder nicht.

Verschwörungstherorien leben davon, dass sie immer und immer wiederholt werden. Wie heute leider auch bei Heise anlässlich eines dummdreisten Rülpsers des sattsamm bekannten Schünemann, der aus irgendwelchen Gründen „Innenminister“ in Niedersachsen ist. (Für die Nachgeborenen: wir hatten diesen Herrn hier schon vor fünf Jahren durchgenommen.)

„Weiter drängt der Innenminister auf neue Befugnisse für die

Länderpolizeien wie Online-Durchsuchungen von IT-Systemen oder ‚präventive Überwachungen von Telefonaten und E-Mails‘. Bisher ist die Einsatzmöglichkeit entsprechender Spionagesoftware dem Bundeskriminalamt (BKA) vorbehalten, das davon bis zum Frühjahr nach eigenen Angaben aber noch keinen Gebrauch gemacht hatte“, schreibt Krempl und erwähnt mit keinem Wort, dass es eine derartige Software weder jemals gegeben hat noch dass es sie geben könnte. Ohne Beweise glaube ich sowieso kein Wort. Krempls suggestive Formulierungen nenne ich unseriös. Ich warte darauf, dass jemand „präsentiv“ meine E-Mails überwacht. Probiert es doch!

„If crypto is outlawed, only outlaws will have crypto.“ Yeah.

Telekommunikationsüberwachungsverordnungsmaßnamen

Ich musste mich regelrecht prügeln, zum Entenbraten, auch bekannt als der einflussreichste Hoax des Jahrzehnts, auch bekannt als das Märchen von der real gar nicht existierenden und technisch nicht umsetzbaren so genannten „Online-Durchsuchung“ etwas zu verfassen. Wie gewohnt ist die Berichterstattung der ahnungslosen Medien interessanter als das Faktum selbst. Natürlich fordert ein Innenminister immer schärfere Gesetze, ungeachtet seiner Parteizugehörigkeit und seines Charakters, falls vorhanden, hieße er Schily, Schäuble oder de Maiziere. Das Sein bestimmt das Bewusstsein, und ein Innenminister, der sich ausschließlich von opportunistischen Karrieristen, Zensur-Propagandisten, ahnungslosen Dampfplauderern (ja, ich denke an Bosbach) und Lobbyistne des Überwachungsstaats umgibt und qua Amt umgeben muss, der trägt immer den unvermeindlichen Komparativ auf den Lippen: Der

Staat muss härter melden, durchführen und verbieten.

Bei Heise las ich die irreführende Überschrift: „De Maizière will heimliche Online-Durchsuchungen auch zur Strafverfolgung“. Der Kollege Krempl ist für merkwürdige und suggestive Formulierungen schon einschlägig bekannt: „Zudem macht sich de Maizière für den Einsatz heimlicher Online-Durchsuchungen zur Strafverfolgung stark. Bisher darf allein das Bundeskriminalamt (BKA) zur Abwehr terroristischer Gefahren verdeckt auf IT-Systeme Verdächtiger zugreifen. Der Innenminister drängt nun auf eine Verwertungsbefugnis für Daten, die mit dem Bundestrojaner gewonnen werden, in der Strafprozessordnung (StPO).“

Kein Wort darüber, dass der „verdeckte Zugriff“, der hier suggeriert wird, weder bisher ein einziges Mal stattgefunden hat noch jemals so stattfinden wird. Auch ist die Bezeichnung „Bundestrojaner“ Schaumschlägerei, weil es diesen „Trojaner“ (es müsste eigentlich Trojanisches Pferd heissen, die Trojaner standen aussen um den antiken hölzernen Gaul herum) gar nicht gibt. Aber Krempl drückt eben wie der mediale Mainstream die Zahnpaste weiter aus der Tube. Man muss Unfug nur lange genug wiederholen, irgendwann glaubt jeder daran. Aber der Begriff ist eben so sexy, da kann niemand widerstehen.

Welt Offline hat etwas genauer formuliert: „Im Einzelnen will de Maizière dem Verfassungsschutz die Erlaubnis zur sogenannten ‚Quellen-Telekommunikationsüberwachung‘ (Quellen-TKÜ) geben.“ Diese Wort-Ungetüm wird immer dann ins Spiel gebracht, wenn niemand mehr nachfragen soll, was eigentlich gemeint ist. Die fromme Legendenbildung der Überwachungslobby hat bekanntlich zur Sprachregelung geführt: Man muss die Daten der Kriminellen überwachen, bevor sie auf den Knopf zum Verschlüsseln drücken. So stellen die sich das vor. Das Neusprech hat seinen Weg in die Medien auch deshalb gefunden, weil die brav jedwedes Deutsch des Grauens nachplappern, ohne ihrer verdammten Pflicht nachzukommen, dieses gespreizte Bläd- und Furzbürokratendeutsch in kleine und verständliche Teile zu

zerhacken. Man geriert sich als Durchblicker, wenn man den Quatsch und jeden Jargon übernimmt. Ich sage nur: Telekommunikationsüberwachungsverordnungsdurchführungsmaßnahmen.

Die so genannten „Quellen-TKÜ“ hat auch mit dem, was bei DAUs und im Volksmund als „Online-Durchsuchung“ bezeichnet wird, gar nichts zu tun, sondern handelt davon, wie man Telefonie und E-Mails belauschen soll.

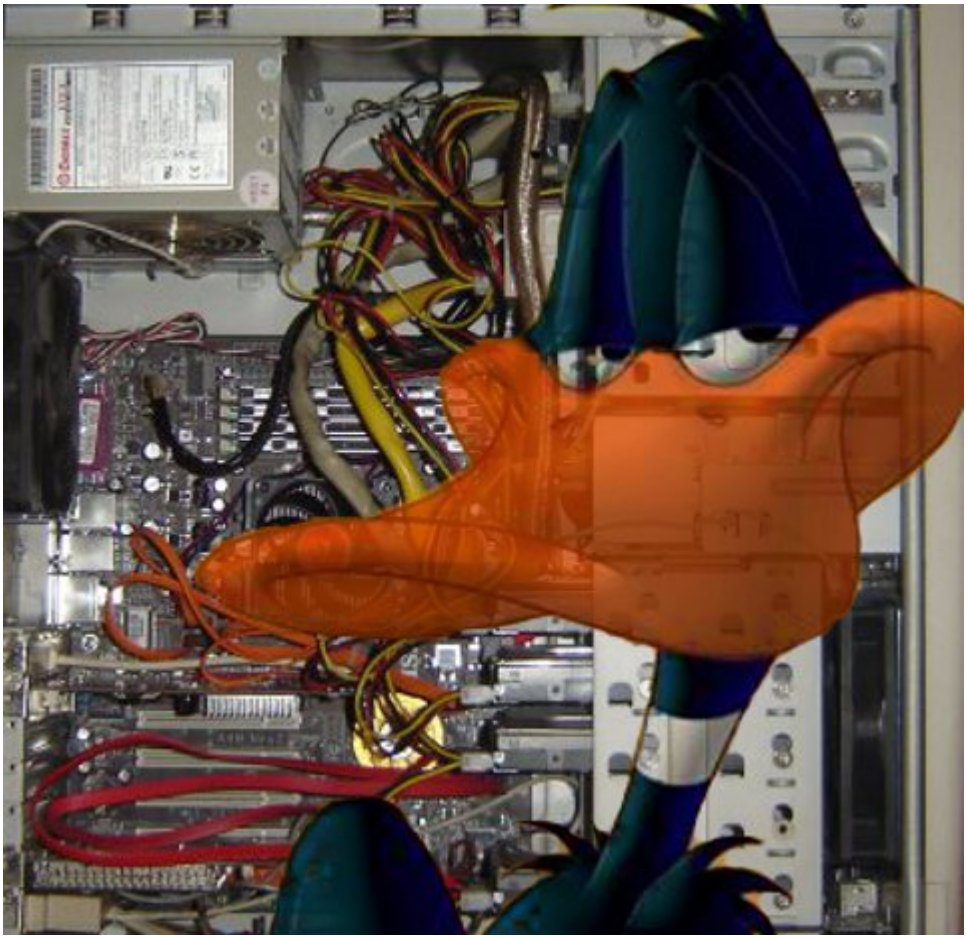
Ich habe keine Lust, alles immer zu wiederholen. Also zitiere ich mich selbst: *Krempl (..:), hier diese Rezension weiterlesen: „Als nächstes zeigen die Autoren, dass es sich bei der Online-Durchsuchung um ein sich selbst verstärkendes Phänomen handelt, das aus unklaren Definitionen darüber herrührte, was mit der Online-Durchsuchung eigentlich gemeint sein soll. Gepaart mit dem Mythos des allmächtigen Hackers schaukelte sich die Darstellung der Online-Durchsuchung in den Medien zu immer größeren Horrorszenarien auf, die man letztlich als nahezu faktenfrei bezeichnen kann. Die einzig gesicherten Fakten waren nur die Berichte in den Medien, nicht deren Inhalt. Aus der vielleicht noch anfangs verwendeten konjunktiven Form ‚könnte‘ wurden dann konkrete Forderungen von Politikern. Journalisten stellten suggestive Fragen, ob es denn solche Fälle nicht schon längst gegeben habe, und weil man nicht genau wusste, was mit ‚Online-Durchsuchung‘ gemeint ist (oder was man selbst darunter versteht) und man es mit anderen Verfahren vermischte/verwechselte, ergab sich das Bild, dass schon seit langem dieses Verfahren ohne Rechtsgrundlage abgelaufen ist. Dies Alles, gepaart mit dem fehlenden Sachverstand, führte zu dem schon genannten ‚Medien-Hype‘. Beim Lesen dieses Teils des Buches kommt man aus dem Staunen über diese Vorgänge nicht heraus. Steht es so schlecht um den Journalismus in Deutschland?“*

Zitat im Zitat: *Ich zitiere mich selbst: „In Wahrheit hat es eine „Online-Durchsuchung“ oder gar den „Bundestrojaner“, der seit geraumer Zeit durch die Medien geistert und sogar einen*

eigenen Eintrag bei Wikipedia bekommen hat, nie gegeben – und es wird ihn auch nie geben. Er ist ein Hoax und beruht auf dem mangelnden Sachverstand eines Oberstaatsanwaltes, jeweils einer Falschmeldung der taz und der Süddeutschen und der Tatsache, dass alle deutschen Medien, ohne die Fakten zu recherchieren, voneinander abgeschrieben haben. Nach dem Prinzip ‚Stille Post' steht am Ende der Berichterstattung dann der ‚behördliche' Hacker, vom dem am Anfang nie die Rede war."

Ceterum censeo: Der Kaiser ist nackt! Es gibt keine ‚Bundestrojaner'!

Die sich selbst verstärkende faktenfreie Ente, lau aufgewärmt



„700.000 Euro für eine Ente“ schrieb ich am 25.05.2010 in diesem kleinen onlinedurchsuchungshoaxfeindlichen Blog. Gestern wärmten der Heise-Newsticker („CDU/CSU und SPD halten an heimlichen Online-Durchsuchungen fest“) und die taz („BKA hält sich zurück“) [*was für ein dämlicher Titel!*] die wohl bekannte Ente wieder auf.

Die beiden Artikel enthalten keine Informationen – sie geben nur das sinnfreie Gefasel einiger Politiker zum Thema der real gar nicht existierenden „Online-Durchsuchung“ wieder. „Gerade beim internationalen Terrorismus beobachten wir zunehmend, dass sich Personen modernster Technologien bedienen, um nicht entdeckt zu werden.“ Modernste Technologien – was könnte damit gemeint sein? Terroristen nutzen das Internet? Der Satz wäre ja sinnvoll, weil für unsere Sprechblasen-Absonderer das Internet ultramodern ist (weil ihnen erst gestern ein persönlicher Referent davon erzählt hat).

„Die Rechtsextremen haben die moderne Technik entdeckt“,

raunte Focus 1993. Das ist der Stand der Diskussion: Man häufe ein paar Komparative um ein vermeintliches Bedrohungsszenario, drapiere es mit kulturpessimistischer Attitude („es wird alles immer schlimmer“) und deutschtypischer Hysterie („die Bösen werden immer öfter immer böser“) und tröpfele noch ein wenig Eigenwerbung drauf („der Verfassungsschutz mahn, warnt und ist besorgt“).

Aber ich schweife ab. Mich regen die „Kritiker“ genau so auf: „Der verdeckte Zugriff auf Festplatten sei ‚überflüssig‘ und richte ‚bürgerrechtlichen Flurschaden‘ an, da er nicht einmal an einen festen Tatverdacht geknüpft sei.“ Bevor ich auch nur ein Wort weiterlese, möchte ich wissen: Wie soll der so genannte „verdeckte“ Zugriff auf „Festplatten“ bewerkstelligt werden? Warum, verdammt noch mal, taucht diese doch nicht ganz unwesentliche Frage weder bei Stefan Krempl noch bei dem einschlägig bekannten Dampfplauderer und Nebelkerzenwerfer Christian Rath von der taz auf? Weil die Zahnpasta schon aus der Tube ist und nicht wieder hinein könnte, selbst wenn sie wollte? Wozu habe ich eigentlich das Buch geschrieben? Liest der Rath seine eigene Zeitung nicht?

Krempl und Rath, hier diese Rezension weiterlesen: „Als nächstes zeigen die Autoren, dass es sich bei der Online-Durchsuchung um ein sich selbst verstärkendes Phänomen handelt, das aus unklaren Definitionen darüber herrührte, was mit der Online-Durchsuchung eigentlich gemeint sein soll. Gepaart mit dem Mythos des allmächtigen Hackers schaukelte sich die Darstellung der Online-Durchsuchung in den Medien zu immer größeren Horrorszenarien auf, die man letztlich als nahezu faktenfrei bezeichnen kann. Die einzig gesicherten Fakten waren nur die Berichte in den Medien, nicht deren Inhalt. Aus der vielleicht noch anfangs verwendeten konjunktiven Form ‚könnte‘ wurden dann konkrete Forderungen von Politikern. Journalisten stellten suggestive Fragen, ob es denn solche Fälle nicht schon längst gegeben habe, und weil man nicht genau wusste, was mit ‚Online-Durchsuchung‘ gemeint

ist (oder was man selbst darunter versteht) und man es mit anderen Verfahren vermischte/verwechselte, ergab sich das Bild, dass schon seit langem dieses Verfahren ohne Rechtsgrundlage abgelaufen ist. Dies Alles, gepaart mit dem fehlenden Sachverstand, führte zu dem schon genannten ‚Medien-Hype'. Beim Lesen dieses Teils des Buches kommt man aus dem Staunen über diese Vorgänge nicht heraus. Steht es so schlecht um den Journalismus in Deutschland?"

Ich zitiere mich selbst: „In Wahrheit hat es eine „Online-Durchsuchung" oder gar den „Bundestrojaner", der seit geraumer Zeit durch die Medien geistert und sogar einen eigenen Eintrag bei Wikipedia bekommen hat, nie gegeben – und es wird ihn auch nie geben. Er ist ein Hoax und beruht auf dem mangelnden Sachverstand eines Oberstaatsanwaltes, jeweils einer Falschmeldung der taz und der Süddeutschen und der Tatsache, dass alle deutschen Medien, ohne die Fakten zu recherchieren, voneinander abgeschrieben haben. Nach dem Prinzip ‚Stille Post' steht am Ende der Berichterstattung dann der ‚behördliche' Hacker, vom dem am Anfang nie die Rede war."

Ceterum censeo: Der Kaiser ist nackt! Es gibt keine ‚Bundestrojaner'!

Noch mehr „Online-Durchsuchungen"

Ich kann mir nicht helfen: Beim Lesen mancher Artikel, in denen das Reizwort „Online-Durchsuchungen" auftaucht, muss ich an Horst Ehmke denken: „Der sozialdemokratische Kanzleramtsminister Horst Ehmke hatte damals den BND aufgefordert, eine Übersicht der Journalisten anzufertigen,

die mit dem Dienst kooperieren. Ausgenommen bleiben sollten operativ eingesetzte Medienvertreter, also an Geheimdienstoperationen beteiligte Agenten.“ So eine Liste hätte ich heute auch gern, aber natürlich aktualisiert.

Nehmen wir einen Bericht aus Focus, der sich vom Heise auf den ersten Blick untgerscheidet, weil Fcous den fragwürdigen und vor allem irreführenden Begriff „Online-Durchsuchungen“*nicht* in Anführungszeichen schreibt. Bei Heise heißt es: „Über die konkrete technische Durchführung dieser „Online-Durchsuchung“ ist noch nichts Weiteres bekannt, allerdings sollen auch „private Laufwerke“ überprüft worden sein.“ Sollen. Es ist also ein Gerücht oder man weiß es vom Hörensagen. Deutscher Journalismus at it’s best. Und was ist mit den öffentlichen Laufwerken? Bei Focus Online: „Zudem durchsuchte der Bundesnachrichtendienst nach FOCUS-Informationen in einer heimlichen Online-Durchsuchung die Computer von 49 Mitarbeitern des Fachreferats zur Aufklärung der Organisierten Kriminalität.“

Frage: Wer hat Focus die „Internen Protokolle“ gesteckt – und mit welchem Motiv? Focus Online publizierte schon April 2007 die faktenfreie Falschmeldung: „Deutsche Geheimdienste spähen schon seit 2005 heimlich über das Internet Computer von Verdächtigen aus.“ Und Focus ist das einzige großere Medium Deutschlands, das den Bundesnachrichtendienst vehement und permanent in diesem Zusammenhang lobhudelt und ihm magische Fähigkeiten zuspricht: „Technische Unterstützung holte sich der Inlandsgeheimdienst bei den Kollegen des Bundesnachrichtendienstes (BND) – Spezialisten auf dem Gebiet der Hacker-Angriffe.“ Honi soit qui mal y pense. Wer wollte Focus instrumentalisieren – offensichtlich mit Erfolg?

Im aktuellen Fall ist die Sache ausgesprochen banal: Entweder hatten die EDV-Verantwortlichen beim BND einen Remote-Zugriff auf die Rechner alle Angestellten, wovon auszugehen ist (wäre komisch und unprofessionell, wenn nicht) oder sie hatten Usernamen und Passworte für die E-Mail-Accounts (bei beim

afghanischen Handelsminister – oder beides. BND-Angestellte schreiben nur elektronischen Postkarten und kümmern sich nicht um die Sicherheit ihrer Rechner. Das ist klar wie Kloßbrühe. Wie wollen die nur im Ausland so spionieren? Beides wäre aber nicht das, was der Sprachgebrauch unter „Online-Durchschung" meint – dass staatliche Hacker von außen auf private Rechner zugreifen könnten. Aber Focus tut alles daran, wiederholt den Eindruck zu erwecken, der BND sei dazu in der Lage. Das stimmt mich nachdenklich. Ich denke schon wieder an Horst Ehmke.

Christian Rath, der „Rechtsexperte" der taz (Computerexperten haben die gar nicht), macht sich ebenfalls zum PR-Sprachrohr der Schlapphüte. Zur Erinnerung aus der Journalistenschule; Journalisten sind *nicht* dazu da, die Sprechblasen irgendwelcher Politiker und Apparatschiks zu publizieren. Dafür gibt es Pressesprecher und ganze Abteilungen in den jeweiligen Behörden. (Nicht viel besser ist Stefan Krempl bei Heise.) Auch zur Erinnerung: sogar Schäuble hat zugegeben, dass Heinz Fromm, der Chef des Verfassungsschutzes, von Technik und Computern keine Ahnung hat. Und wenn der laut taz fordert, auch die Dauer-Skandalbehörde Verfassungsschutz müsse immer öfter „Online-Durchsuchungen" vornehmen dürfen, darf man das nicht einfach unkritisch verbreiten – zumal der Verfassungsschutz bisher bei offiziellen Anfragen immer geleugnet hat, dass er das jemals hingekriegt bzw. praktiziert hätte. Die „Online-Durchsuchung" bleibt ein frommer Wunsch ahnungloser Politiker.

Übrigens, Kollege Rath: „Einzelne Online-Durchsuchungen hat der Bundesverfassungschutz früher schon durchgeführt, unter anderem gegen den Islamisten Reda S." Welche Quellen? Welche Fakten? Ja, es gibt eine Quelle – und nur eine: Focus. Mit der Quellenlage des besagten Artikels habe ich mich in unserem Buch ausführlich beschäftigt. „Einzelne"? Nein, Auch das ist gelogen. Wenn man schon woanders abschreibt, Kollege Rath, ohne zu prüfen, ob es mehrere unabhängige Quellen gegeben hat, dann bitte richtig. Focus schrieb in Ausgabe 2/2008: „Mit

einem einzigen Klick hatte der von Terrorfahndern als Gefährder eingestufte Islamist Seyam die Schleuse geöffnet für die erste und bislang einzige Online-Razzia in Deutschland.“ In dem Fall waren die Ermittler schon beim Computerkauf indirekt dabei. Und gefunden hat man auch nichts.

Ein irrer Haufen Online-Durchsucher

So so. Die „Experten“ faseln wieder über die real gar nicht existierenden „Online-Durchsuchungen“. „Im Streit um das BKA-Gesetz scheint ein tragbarer Kompromiss gefunden.“ Da das hier ein Blog und kein journalistischer Mainstream-Artikel ist, kann ich offen reden: Es handelt sich um einen Haufen Irrer.

Schauen wir genauer hin. Die Financial Times lässt Friederike von Tiesenhausen etwas zum Thema berichten, eine Politik-Redakteurin. Wird gefragt, wie eine „Online-Überwachung“ technisch umgesetzt werden könnte? Nein. Der Kaiser ist aber nackt.

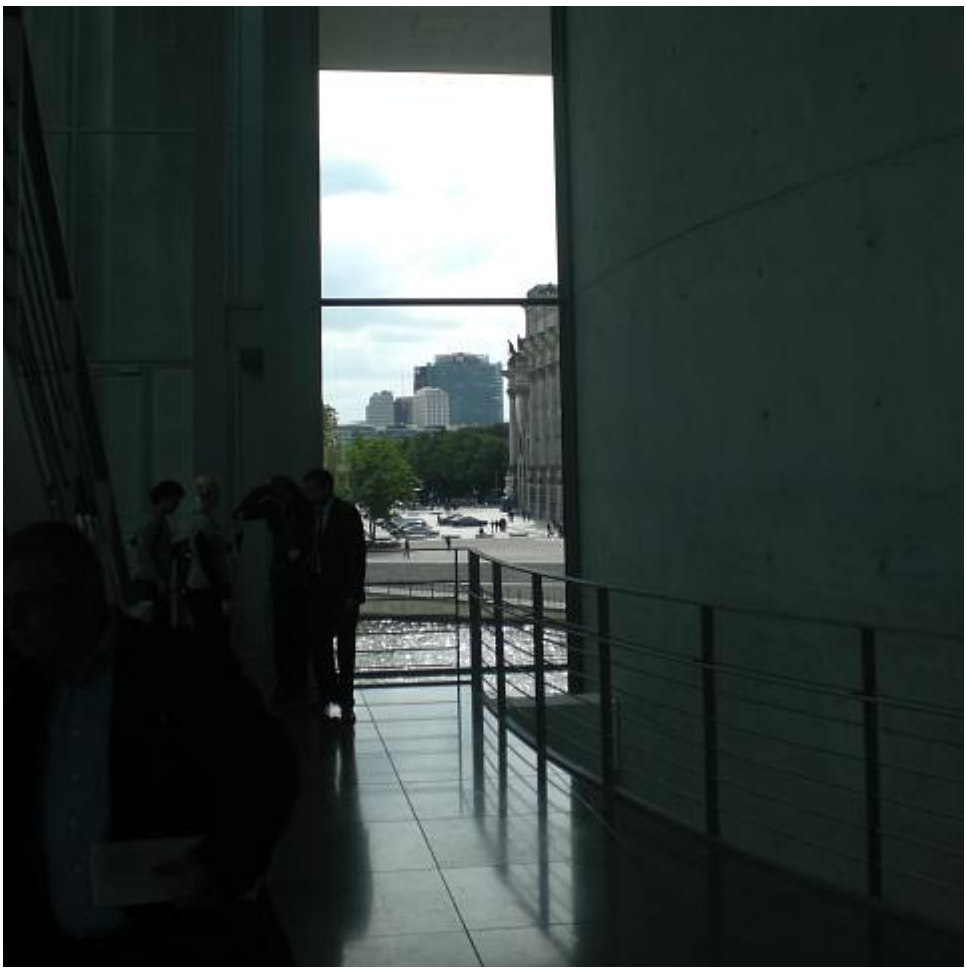
Im Tagesspiegel schreibt der Politik-Redakteur Albert Funk zum Thema. Wird gefragt, wie eine „Online-Überwachung“ technisch umgesetzt werden könnte? Nein. Der Kaiser ist aber nackt.

In der Süddeutschen kommt Susanne Höll zu Wort, die „neugierig und kritisch sein“ will. Ist sie das? Wird gefragt, wie eine „Online-Überwachung“ technisch umgesetzt werden könnte? Nein. Der Kaiser ist aber nackt

Allgemeiner Trend: Die Medien wiederholen nur, was alle möglichen Verdächtigen gesagt haben, ganz gleich, ob das grober Unfug, Agitprop oder sonstwas ist. So auch bei Heise

Stefan Krempl. Ich kann das seichte Gefasel einfach nicht mehr hören und wiederhole mich: Ein Haufen Irrer, allesamt, nicht nur die Politiker, die über das Thema beschließen, sondern auch die Journaille, die darüber berichtet. Zeige mir jemand die Ausnahme, die die Regel bestätigt – und ich wäre für ein paar Minuten glücklich.

BKAG-E vor dem Innenausschuss



Zugegeben: Ich habe mich gestern während der Anhörung im Innenausschuss des Bundestages ziemlich aufgeregt. Das ist unprofessionell. Man merkt das unserem Telepolis-Artikel an.

Ich bin ausnahmsweise vollständig Fefes Meinung: „Der aktuelle

Kriegsschauplatz ist nicht, ob wir den Bundestrojaner kriegen, sondern ob sie heimlich in die Wohnung einbrechen dürfen, um ihn zu installieren.“ Auch, dass der Kollege Krempl offenbar auf einer anderen Veranstaltung war ich Leitner und ich. Die Meldung in der Tagesschau überrascht mich mittlerweile gar nicht – beim Thema „Online-Durchsuchung“ haben sie ohnehin groben Unfug verbreitet. Kai Raven hat alles mitgeschrieben, deshalb muss ich meine Notizen hier nicht noch einmal bloggen.

Im Gegensatz zu Fefe war mein Favorit Roggan. Ich habe in der Pause mit ihm ein paar Worte gewechselt. Meinem Eindruck nach war er deshalb so zurückhaltend, weil er genau wusste, dass es kaum jemanden interessierte, was er zu sagen hatte, und dass die Angelegenheit eine bloße Farce war. Leider fragten die Vertreter der Parteien nur diejenigen Experten, die sie selbst eingeladen hatten. Ich habe mich auch darüber geärgert, dass Petra Pau und Ulla Jelpke Fragen an Jörg Ziercke vom BKA stellten. Ich hätte diesen erbärmlichen Schwätzer nicht so zu Wort kommen lassen. Ziercke muss man live erlebt haben: Ich frage mich, wie jemand, der so dumm und zum Teil primitiv argumentiert, eine solch große Behörde überhaupt leiten kann, ohne dass alles drüber und drunter geht. Roggan hat, wenn er gefragt wurde, scharf argumentiert und subtil verdeutlicht, wo er den Hebel ansetzen wird. Er wird, wie auch Gerhart Baum, das Gesetz juristisch angreifen. Und ich wette, dass das Bundesverfassungsgericht auch das BKA-Gesetz in die Tonne treten wird. Diejenigen Herrschaften, die das verabschieden wollen, sind schlicht belehrungsresistent.

Sehr gut gefallen hat mir „Paulus“ Hansjörg Geiger, der jede Menge Dreck am Stecken hat, aber sich offenbar auf die Seite der Guten schlagen will. Seine Empörung über das Ansinnen von heimlichen Durchsuchungen wirkte sehr echt.

Aber doch noch ein paar Stichpunkte, die ich im Artikel nicht erwähnt habe: Kutscha kritiserte, dass nicht geregelt sei, welche Daten wann an ausländische Geheimdienste übermittelt würden. Einige der neuen Befugnisse des BKA hätten keinen

Terrorismus-Bezug – wie zum Beispiel das Recht, Platzverweise zu erteilen. Das sei doch eine „James-Bond-Persiflage“.

Möllers meinte, dem BKA würden jetzt alle Befugnisse und Kompetenzen gegeben, die bisher schon die Geheimdienste hätten. Die Gesetzgeber betreibe offenbar nur noch „Verfassungsgerichtsexegese“, anstatt selbst Gesetze zu gestalten. Es könne nicht sein, dass die gesetzlichen Normen immer nur „so gerade an der Verfassungsgemäßheit entlangschrappen.“

Poscher sah die vom Grundgesetz vorgeschriebene Trennung von Poliezi und Geheimdiensten relativiert.

Roggan: Bis jetzt gebe es keinen Nachweis, dass die Befugnisse der Online-Durchsuchung unverzichbar seien. Die Prävention habe Einzug in das Strafrecht gehalten. Der Personenkreis der „Gefährder“ werden unverhältnismäßig ausgeweitet. („Wir sind alle Gefährder“ war mein erster Arbeitstitel für den Telepolis-Artikel) Wenn man das durchsetzen wolle, was geplant sei, müssten sie das Grundgesetz ändern.

Kabarettreif war Wolfgang Wieland, der nicht nur so laut redete, dass man ihn gut verstand, sondern auch witzig argumentierte. Es gebe im Übrigen keine Definition des „Internationalen Terrorismus“, auch die Autonomen in Heiligendamm könnte man in Zukunft als terroristische Vereinigung ansehen. Es sei im Gesetzentwurf von „ideologischen Strömungen“ die Rede. Reiche es aus, dass ein Terrorist fernsehe und sich „deshalb“ als „international“ einschätze, dass er zu einer terroristischen Vereinigung werde? Poscher hielt diese fehlende Definition gleich für verfassungswidrig.

Fazit: Es kommt noch einiges auf uns zu. Von der CDU und der SPD ist rein gar nichts zu erwarten. Die würden alles abnicken, selbst ein Ermächtigungsgesetz. Sie würden es noch nicht einmal merken. Man kann nur hoffen, dass die niemals

eine Zweidrittelmehrheit im Bundestag kriegen. Dann könnte selbst das Bundesverfassungsgericht gegen die zahlreichen Verfassungsfeinde im Bundestag nichts ausrichten.

Auf meinem Foto ist der Ausschuss-Vorsitzende Edathy zu sehen, der ein Interview gibt. Ich hatte aber keine Gelegenheit, ihn zu begrüßen.

Hansetrojaner

Mit Schmunzeln habe ich bei Heise „Hamburgs Innensenator plant den Hansetrojaner“ gelesen. Die hübsche Story geht auf die taz zurück. „Online-Razzien seien heute ein ‚unverzichtbares Instrument‘ der Strafverfolger“, sagt Hamburgs Innensenator Christoph Ahlhaus. Ahlhaus ist ein Lügner, denn ein Instrument ist dann nicht „unverzichtbar“, wenn es gar nicht funktioniert und wenn es noch nie erfolgreich angewendet wurde. Der gute Mann ist gelernter Bankkaufmann und Jurist und hat vom Internet und von Computern so viel Ahnung wie ein Zeuge Jehovas vom Atheismus. Ich überlege, ob wir ihm Ende des Monats mal ein Büchlein schicken. Aber solche Leute sind meist so eingebildet, dass sie aufs Lesen und Erwägen rationaler Argumente gern verzichten. „Weitere Einzelheiten zu dem Vorhaben sind bislang nicht bekannt“, schreibt Krempl bei heise.de. Quod erat demonstrandum. Wie auch. Es gibt keine.