German Internet Angst

Diese Artikel steht – leicht verändert – in der aktuellen Ausgabe des Medienmagazins Nitro.

Kann der Staat private Rechner kontrollieren und durchsuchen? Fachleute des Chaos Computer Club haben Spionage-Software auf Festplatten gefunden, die das beweisen. Aber was ist wirklich geschehen und was machten die Medien daraus?

Dem deutschen Journalismus kann vieles vorgeworfen werden: Die Journaille sei duckmäuserisch und feige, lasse sogar Interviews „autorisieren“, Recherchen fänden im Tagesgeschäft kaum noch statt, und der technische Sachverstand, das Netz aller Netze betreffend, entspräche dem Niveau von Grundschülern. Das ist alles richtig und kann mit dem kulturellen Tradition des Obrigkeitsstaats und der „German Internet Angst“ erklärt werden, ein Begriff, den die US-amerikanische Zeitschrift Wired schon im Juni 1998 prägte.

The reunified nation still shows symptoms of schizophrenia, and nowhere are the symptoms wreaking more havoc than on the Internet. (Wired 1998)

Drei von vier Deutschen haben laut einer repräsentativen Untersuchung Angst vor Computern und dem Internet; die Mehrheit nutzt das Netz nur selten.(Süddeutsche,18.03.2010). Journalisten denken und verhalten sich nicht signifikant anders als der Rest der Bevölkerung. Des Diskurs über staatliche Spionage-Software beweist das immer wieder: Die Berichte und Kommentare in den Medien über die sogenannte „Online-Durchsuchung“ sind seit fünf Jahren fast ausnahmslos eine Mischung aus techischem Voodoo, grobem Unfug und heißer Luft.

Die schlimmste Berufskrankheit des deutschen Journalismus ist aber die rational nicht zu erklärende Unart, suggestive Begriffe unkritisch zu übernehmen und wiederzukäuen, die von Behörden und Firmen erfunden wurden, um bestimmte Sachverhalte

zu verschleiern und euphemistisch umzudeuten. In der guten alten Zeit nannte man das unter Journalisten Propaganda oder „Agitprop“. Das gilt insbesondere für die vom bürokratischen Neusprech vergifteten Worthülsen „Staats-Trojaner“, „Online-Durchsuchung“ und „Quellen-Telekommunikationsüberwachung“. Ein Schelm, wer an „Rettungsschirme“ und „friedenserzwingende Maßnahmen“ oder gar an das Wahrheitsministerium von George Orwell denkt.

Eine Mischung aus techischem Voodoo, grobem Unfug und heißer Luft.

Kein Wunder, dass auch viele Journalisten glauben, „die Hacker“ könnten zaubern und mit magischen Methoden in Rechner eindringen und die manipulieren, entweder in staatlichem Auftrag oder aus quasi-kriminellen Motiven. Eine gute Nachricht also vorweg: Die Idee, man könne ohne vorherigen physischen Zugriff (und das auch nur unter ganz bestimmten Voraussetzungen) gezielt auf einen privaten Rechner zugreifen und ohne Zustimmung des Verdächtigen eine Spionage-Software „aus dem Internet” implementieren, ist eine Verschwörungstheorie und technisch gesehen Blödsinn.

Nun rufen alle im Chor: „Ja, aber?“ Richtig: Es ist den Behörden gelungen, auf einigen Rechnern Programme zu installieren, die nicht nur die Kommunikation belauschten, sondern Screenshots anfertigten und unbemerkt versandten, also digitale Fotos dessen, was jeweils auf dem Monitor zu sehen war. Noch mehr: Die Spionage-Software konnte sogar zusätzliche Programme und Features nachladen. Letztlich kann das natürlich dazu führen, dass die befallenen Rechner hätten von fern gewartet, also übernommen („remote access“) werden können. Das streitet niemand ab.

Was macht DPA (10.10.2011) daraus? „Eigentlich Trojanisches Pferd genannt, schleust sich eine solche Schadsoftware unbemerkt in fremde Rechner ein…“ Nein, ganz falsch. Eine Software kann sich nicht selbst einschleusen. Das ist – auch

auf die Gefahr hin, etwas zu wiederholen – eine Verschwörungstheorie.

Auch die Tagesschau machte mit: „Dabei sollen Computer einmal (Online-Durchsicht) oder während eines gewissen Zeitraums (Online-Überwachung) überprüft bzw. überwacht werden, ohne dass der Nutzer das bemerkt. Das Innenministerium sprach 2008 nicht von Bundestrojanern, sondern von „Remote Forensic Software".“ Sollen? Was jemand will, sollte von der jeweiligen Pressestelle verbreitet werden. Journalisten sollten herausfinden, was war und ist, nicht mehr und nicht weniger.

Die Frankfurter allgemeine Zeitung (03.11.2011) schrieb etwas von einer „ferngesteuerten Informationstechnik“. Das ist einfach nur Quatsch. Man braucht sich gar nicht zu streiten, ob es einen Unterschied gebe zwischen einer „Durchsicht“ und einer „Überwachung“. Wer seinen Rechner schützt, etwa nach den im Internet abrufbaren Maßgaben des Bundesamtes für Sicherheit in der Informationstechnik, der braucht sich keine Sorgen zu machen, „online durchsucht“ zu werden. Es hat sich auch noch niemand, noch nicht einmal der Chaos Computer Club, erkühnt, einen Weg zu beschreiben, wie das „von fern“, online und gezielt möglich sei. Wieso ist das eigentlich so schwer zu verstehen?

Im aktuellen Fall geht es um die Überwachung von Internet-Telefonie.

Im aktuellen Fall geht es um die Überwachung von Internet-Telefonie, deren „Nebeneffekt" jedoch war und ist, dass der Rechner komplett überwacht werden kann. Man muss also Programme installiert haben, etwa Skype, die Telefongespräche via Internet ermöglichen.

Apropos Internet-Telefonie: In vielen Unternehmen ist Skype 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. 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.

Das ist alles seit Jahren bekannt; Software, die Telefonieren per Internet belauscht, wird sogar kommerziell angeboten. Um die aber installieren zu könnten, braucht man den physischen Zugriff auf einen Rechner. Und wenn dessen Besitzer davon nichts merken soll, muss dieser seinen Computer völlig ungesichert herumstehen lassen oder herausgegeben haben.

Die Tageszeitung (11.10.2011) schildert, wie man das so macht: „Bayerns LKA bricht auch mal heimlich in ein Firmenbüro ein, um Schnüffelsoftware zu installieren.” Das erinnert an die zentrale Losung der Hausbesetzer-Bewegung in den 80-er Jahren: legal. illegal, scheißegal.

Kann man sich vorstellen, dass von den zahlreichen deutschen Medien und mehreren tausend Journalisten niemand fragte, wie man denn eine Software zum Spionieren und „Online-Durchsuchen“ gezielt auf einen bestimmten Rechner bekäme? Nein, niemand fragte. Man faselte nur vage herum. Da gab es doch einen Geschäftsmann, der auf einem Flughafen in Bayern seinen Laptop abgeben musste und dem irgendwelche Beamten irgendetwas implementierten? So mag es gewesen sein. Nichts Genaues weiß man nicht, und es interessiert auch niemanden.

Wie dumm muss man aber sein, seinen Computer so einzustellen, dass ein Fremder Software installieren darf? Keine Passworte? Booten von Fremdmedien, etwa USB-Sticks, erlaubt? Keine verschlüsselte Partitionen der Festplatte vorhanden, zum Beispiel mit Truecrpyt? Wie jetzt? E-Mails – also digitale Postkarten – im Klarterxt und unverschlüsselt – so etwas gibt es noch im 21. Jahrhundert? Ja, es handelt sich um Deutschland

einig Entwicklungsland, das Internet betreffend.

Bei staatlicher Datenspionage greifen mittlerweile mediale Beißreflexe, die dem Diskurs über Drogen gleichen.

Bei staatlicher Datenspionage greifen mittlerweile mediale Beißreflexe, die dem Diskurs über Drogen gleichen: Seit vier Jahrzehnten sind bei diesem alle Textbausteine und Argumente bekannt, sie werden in konjunkturellen Schüben aus moraltheologischen Gründen ständig wiederholt. So auch hier: Die Überwachungslobby möchte ihrem feuchten Traum, in der digitale Unterwäsche aller Untertanen ständig herumschnüffeln zu dürfen, nicht abschwören, weil es ums Prinzip geht. Die Datenschützer und ihre Verbündeten müssen den Popanz, das sei einfach so möglich, beschwörend vor sich her tragen, um die Gefahr des totalitären Staates 2.0 allen permanent vor Augen führen zu können.

Der Berliner Richter und Verfassungsrechtler Ulf Buermeyer hat in einem Interview mit netzpolitik.org (10.10.2011) lapidar kommentiert: „…solche Software darf es niemals geben, und zwar weil sie auch das Einspielen von Daten auf dem Zielsystem erlaubt. Das ist unter Geltung des Grundgesetzes stets unzulässig“.

Damit ist das Thema eigentlich erledigt. Buermeyer, der während seines Studiums auch als IT-Techniker gearbeitet hat und im Gegensatz zu vieler seiner heutigen Kollegen weiß, wovon er redet, wenn es um Computer geht, kennt jedoch die Mentalität der Behörden: „Richtig ist aber auch, dass sich Teile der Justiz die fehlende Rechtsgrundlage einfach selbst schaffen, indem sie die Regeln für „normale” Telefonüberwachungen für anwendbar erklären.“

Die Überwachungslobby möchte ihrem feuchten Traum, in der digitale Unterwäsche aller Untertanen ständig herumschnüffeln zu dürfen, nicht abschwören.

Im Urteil des Bundesverfassungsgerichts vom 27. Februar 2008

(1 BvR 370/07, 1 BvR 595/07) heißt es: „Das allgemeine Persönlichkeitsrecht umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen."

Die Zeitschrift „Das Parlament" titelte am 31.10.2011 über eine Abstimmung zum Thema im Bundestag: „Mehrheit für Online-Durchsuchung". Die SPD-Parlamentarierin Gabriele Fograscher meinte, neue Kommunikationstechniken ermöglichten es Straftätern, „sich im Netz zusammen zu finden, zu radikalisieren, zusammen zu arbeiten". Daher müsste die „Online-Durchsuchung" den „Sicherheitsbehörden" erlaubt sein. Also nichts dazu gelernt. Quod erat demonstrandum.

Gesetze? Urteile des höchsten deutschen Gerichts? Hermann Höcherl (NSDAP, später CSU) prägte schon 1963 den bezeichnenden Satz: „Verfassungsschützer können nicht ständig das Grundgesetz unter dem Arm tragen". In einem Bundesland, in dem man mit dem Auto Menschen totfahren kann und trotzdem später Verkehrsminister werden darf, sollte einen also gar nichts mehr wundern. Die Demokratie ist oft nur ein dünner Firnis, unter dem Dinge zum Vorschein kommen, wenn man nur ein wenig kratzt, die man am liebsten gar nicht anschauen möchte.

Die Anti-Terror-Lüge

Richard Gutjahr hat einen äußerst lesenswerten Artikel auf seinem Blog verfasst (via Fefe ua.):

Vorratsdatenspeicherung, Bundestrojaner, Anti-Terror-Gesetze. Noch nie in der Geschichte der Bundesrepublik gab es einen solchen Raubbau an Bürgerrechten. Ein Blick in die Statistik bringt Erstaunliches zutage: Die sog. „Anti-Terror-Gesetze“ werden für alles Mögliche benutzt, selten aber zur Bekämpfung von Terroristen. (…)“„Der Gesetzgeber schafft praktisch rechtsfreie Räume“, sagt Thomas Stadler. Selbst das Bundesverfassungsgericht stemme sich nur noch bedingt gegen diese Entwicklung,..

Nicht zu vergessen den Link zu den den Abhörstatistiken der letzten Jahre. Lesebefehl, obwohl es zum Gruseln ist!

Anti-Viren-Programme sind Malware

Computerbild: „Ein bekannter Virenschutz-Hersteller hat beim Ausspähen eines Nutzers geholfen.“

„Eine Strafverfolgungsbehörde hat sich an uns gewendet und unsere Mitarbeit angefragt. Ein User wurde anhand eines gezielten Angriffs ausgespäht“, heißt es in der vertraulichen Nachricht des hochrangigen Mitarbeiters. Dem Hersteller wurde eine Kopie des Bundestrojaners überlassen. Das Virenschutz-Unternehmen hat den Trojaner daraufhin so angepasst, dass die eigene Schutz-Software den Verdächtigen nicht warnte – und so die Bespitzelung ermöglichte.

By the way, Computerbild: Wie kam die eigentliche Software zum Ausspähen auf den/die Rechner des Verdächtigen? Nur mal so ganz nebenbei gefragt.

Die Pointe steht aber hier: *Fakt ist aber, dass der modifizierte Trojaner zumindest im Ermittlungszeitraum eine Gefahr für alle Kunden der kooperierenden Anti-Viren-Schmiede war.*

Noch mal zum Mitschreiben: Das Unternehmen, was rechtlich nicht verpflichtet war, Hilfspolizei zu spielen, hat sene „Virenschutz“-Software so modifiziert, dass diese die Spionage-Software zum Ausspähen von Internet-Telefonie Mit den bekannten Risiken und Nebenwirkungen) nicht erkennen konnte.

Das ist deutsche Leitkultur. Noch Fragen?

Verfassungskonforme Überwachung von Computern ist technisch nicht möglich

Christopher Lauer sagt klar und angenehm, was erstens, zweitens, drittens käm (via Fefe):

Der Einsatz des "Bundestrojaners", der unter anderem auch Bildschirminhalte überwacht, stellt also einen klaren Verfassungsbruch dar, wird aber trotzdem von Spitzenpolitikern wie Uhl oder Friedrich verteidigt. (…) Eine verfassungskonforme Überwachung von Computern ist schon technisch nicht möglich. Der Innenminister täte gut daran seinen aussichtslosen Kampf gegen die Realität zu beenden.

Solchen Dumpfbacken wie dem Innenminister würde ich auch einen Putschversuch trauen.

Sperrt sie ein!

Christopher Lauer (Piraten): „Ich bin es leid, ich bin es echt leid. Der Staat gibt einer Firma, deren Geschäftsführer wegen Bestechlichkeit verurteilt wurde Geld, damit sie Schadsoftware herstellt, um die Bevölkerung zu überwachen. Würde ich ‚Der Staat' im vorherigen Satz durch ‚Eine kriminelle Vereinigung' austauschen würde jeder sagen: Sperrt sie ein!"

Wieso ist das eigentlich so schwer zu verstehen?

FALSCH, Wirtschaftswoche: „Eigentlich Trojanisches Pferd genannt, schleust sich eine solche Schadsoftware unbemerkt in fremde Rechner ein…“

Das eben nicht. Eine Software kann sich nicht selbst einschleusen. Das ist eine Verschwörungstheorie.

FALSCH, Tagesschau: „Der Begriff steht für eine Online-Durchsuchung seitens der Bundesregierung. Dabei sollen Computer einmal (Online-Durchsicht) oder während eines gewissen Zeitraums (Online-Überwachung) überprüft bzw. überwacht werden, ohne dass der Nutzer das bemerkt. Das Innenministerium sprach 2008 nicht von Bundestrojanern, sondern von „Remote Forensic Software“.

Hier geht es um die Überwachung von Internet-Telefonie, deren „Nebeneffekt“ ist, dass der Rechner komplett überwacht werden kann. Und dazu braucht man den physischen Zugriff, und der Nutzer muss seinen Rechner UNGESICHERT herumstehen lassen oder herausgegeben haben.

Wieso ist das eigentlich so schwer zu verstehen?

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.

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.

Nicht ich bin’s gewesen, die Hacker sind es gewesen

Spiegel ~~online~~ im Interview mit Kasperksy („ein russisches Softwareunternehmen (…) hat sich auf die Entwicklung von Sicherheitssoftware spezialisiert“):

„So hält auch der Russe es für die wahrscheinlichste Erklärung, dass der Computerwurm Stuxnet, der im vergangenen Jahr viel Aufmerksamkeit auf sich zog, eine amerikanisch-israelische Erfindung sein könnte“. Könnte? Hätte? Würde? Fakten? Fehlanzeige.

„Mutmaßlich über verseuchte USB-Sticks gelangte er in iranische Atomanlagen.“ Mutmaßlich? Seit wann verbeiten Journalisten Mutmaßungen und verschweigen sogar die Quelle der Gerüchte? Stand es in der Bild-Zeitung?

„Aber selbst für den großen Stromausfall, der Teile Nordamerikas im August 2003 lahmlegte, macht Kasperski mittlerweile PC-Schädlinge verantwortlich“. Wer hätte das gedacht. Die Firma verkauft Software gegen „PC-Schädlinge“.

„Ich bin mir heute ziemlich sicher, dass diese Katastrophe von einem Virus ausgelöst wurde.“ Ich bin mir ziemlich sicher, dass Kaspersky das Interview benutzen will, um seine eigenen Produkte loszuwerden. Und ich bin mir ziemlich sicher, dass Kasperky wusste, dass deutsche Journalisten keinen kritischen Fragen stellen, wenn es um Computer und Internet geht, und auch an Fakten nicht besonders interessiert sind, nur an vagen Bedrohungsszenarien.

„Er will überdies nicht ausschließen, dass hinter vielen der aktuellen Hackerattacken heute Regierungen stecken.“ Ich will

nicht ausschließen, dass ich mich bewerbe, Vorsitzender der Piratenpartei zu werden. Ich will auch nicht ausschließen, dass der Kaiser nackt ist und er gar keine neuen Kleider trägt.

„In Zukunft allerdings müssen wir mit Cyber-Attacken auf Fabriken, Flugzeuge und Kraftwerke rechnen.“ Nicht nur das: Auch mit Attacken auf harmlose kleine Privatrechner, die mit gaaaaanz vielen „Bundestrojanern“ nur so gespickt werden. Wie die Kollegin Annette Ramelsberger schon vor vielen Jahren schrieb: „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.“

„Kasperski zum SPIEGEL: ‚Alles, was wir erreichen können ist, zu verhindern, dass da draußen alles außer Kontrolle gerät.'“ Ja, genau! Kauft mehr „Anti-Viren-Programme“ von Kapersky! Das Ende ist nahe!

Polizei beschlagnahmt Server der Piratenpartei Deutschland

Bundesvorstand der Piratenpartei: „Am Morgen des 20.Mai 2011 hat die Polizei in Folge eines französichen Ermittlungsersuchens eine Vielzahl an Servern der Piratenpartei Deutschland, die bei der Firma AixIT in Offenbach gemietet sind, beschlagnahmt."

Truecrypt? SpOn: „Die Polizei nahm die Webserver der Partei am Freitagvormittag vom Netz. Es liegt ein Durchsuchungsbeschluss vor." Was denn nun? Die Server wurden nicht „durchsucht" (man hätte auch ein Image ziehen können), sondern „beschlagnahmt", also weggenommen.

„Die Abschaltung aller Server ist ein massiver Eingriff in die Kommunikations- und Informationsstruktur der sechstgrößten Partei Deutschlands", protestieren die Mitglieder des Bundesvorstands der Piratenpartei Deutschland Sebastian Nerz, Bernd Schlömer, Marina Weisband, Rene Brosig, Wilm Schumacher, Matthias Schrade und Gefion Thürmer. „Angesichts der in zwei Tagen anstehenden Landtagswahlen in Bremen wird hier politisch ein massiver Schaden angerichtet, den der Bundesvorstand der Piratenpartei Deutschland aufs Entschiedenste verurteilt. Im Zusammenhang mit den laufenden Ermittlungsarbeiten wird daher zu klären sein, ob die erfolgte Durchsuchungs- und Beschlagnahmeanordnung rechtlichen Vorgaben entsprochen hat, insbesondere ob die Grundsätze der Verhältnismäßigkeit gewahrt wurden."

Verhältnismäßig? Natürlich nicht, aber das Wort kennt man bei einer Staatsanwaltschaft nicht, wenn man schon einmal die

Gelegenheit bekommt, Rechern zu beschlagnahmen (das Verfahren als Strafe, wie bei mir).

Saarländische Online-Zeitung: „Hausdurchsuchung bei Piratenpartei Deutschland“ (völliger Blödsinn). „Spekulationen zufolge sucht man nach einer bestimmten Datei, die der Piratenpartei zugespielt und veröffentlicht wurde. Es soll sich um ein Dokument betreffend Bundestrojaner und dem Abhören von Skype-Telefongesprächen handeln, das offensichtlich zu einem Ermittlungsverfahren gegen Unbekannt wegen Verletzung des Amtsgeheimnisses gehört. Dies hätte dann zur Hausdurchsuchung bei der Piraten- IT geführt.“

Es soll sich. So etwas nennen die nun „Berichterstattung“.

Bei Telepolis liest man: „Polizei kopiert Inhalte von deutschem Piratenpartei-Server“.

Mannomann. Man wird noch nicht einmal korrekt informiert, ob die Rechner nun weg sind oder nicht. Kann mir das jemand sagen? Pappnasen.

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)

Skype abhören oder wie sich deutsche Richter das E-Mail-Schreiben vorstellen

Der Beschluss wurde im Auftrag der Staatsanwaltschaft Landshut von den Polizeibehörden vollzogen. Hierzu hat das Bayerische Landeskriminalamt zum Zwecke der Ausleitung der verschlüsselten Telekommunikation auf dem Computer des Beschuldigten [redacted] eine Software aufgebracht, welche über zwei Überwachungsfunktionen verfügt: Die Überwachung und Ausleitung der verschlüsselten Skype-Kommunikation (Voice-over-IP sowie Chat) vor der Ver- bzw. nach der Entschlüsselung sowie das Erstellen von Screenshots der Skype-Software sowie des Internet-Browsers Firefox im Intervall von 30 Sekunden zur Überwachung der über https geführten Telekommunikation. Diese Maßnahmen wurden sodann auch umgesetzt.

Der Beschuldigte wurde von den durchgeführten Telekommunikationsmaßnahmen nicht unterrichtet.

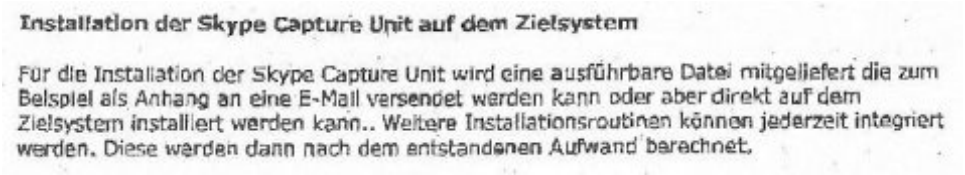
Beschluss des Landgerichts Landshut: „Zwar muss der Beschuldigte um eine E-Mail verfassen zu können, eine Verbindung zu einem Server aufbauen, der ihm die erforderliche Maske zur Verfügung stellt. Der Vorgang des Schreibens der E-Mail findet dann aber ohne Datenaustausch statt, da die einzelnen Buchstaben nicht sofort an den Server weiter übertragen werden. Die E-Mail wird erst dann zum Server und damit in die Außenwelt transportiert, wenn der Beschuldigte den IIVersenden-Button“ betätigt. Hält man sich diese technischen Vorgänge vor Augen, kann nach Auffassung der Kammer – auch im Lichte der Entscheidung des Bundesverfassungsgerichts zur Unzulässigkeit der Online-Durchsuchung (NJW 2008, 822) – beim Schreiben einer E-Mail noch nicht von einern Vorgang der Telekommunikation gesprochen werden.“ (via law blog, mehr dazu bei ijure.org)

Bruhahahah. Das ist ja wieder ein gefundenes Fressen für unsere Verschwörungstheoretiker zum Thema „Online-Durchsuchung“. Hier geht es aber um Skype (vgl. auch den Beschluss des LG Landshut dazu.) Der Beschuldigte kommunizierte via Skype und benachrichtigte die Gesprächspartner vorher durch eine SMS.

Frage: Wie kam der so genannte „Trojaner“ (der keiner ist) auf den Rechner des beschuldigten? (Es ging übrigens um die pöhsen Drogen.) Was wäre gewesen, wenn der Beschuldigte *nicht* den Internet-Explorer für Windows, sondern Galeon für Linux benutzt hätte?

Zum Thema habe ich am 09.20.2010 ausführlich gebloggt – „Skype: Heimlich auf den Rechner spielen“:

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



Installation der Skype Capture Unit auf dem Zielsystem

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

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

In der Heise-Meldung von gestern heisst es: „Ein Schweizer

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

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

Im dazugehörigen Blog heisst es: „The code is simple and straightforward. You have know malware development is no rocket science and if you expect big magic you are at the wrong place.“ Am besten hat mir der Kommentar „Giovannis“ gefallen: „Despite what some people say, Skype has never been secure. It is relatively easy to hack skype accounts, skype does not even check if the same user logs in simultaneusly on different machines and what is worst, the second user can get a copy of all the chats. Skype is good for housewifes that want to chat a bit with their kids, but for confidential conversations the use of strong voice encryption is required. In our company we tested many of them, we now keep with PhoneCrypt from securstar as it proved to be very good, stable, and with an excellent voice quality.“

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

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

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

Skype: Heimlich auf den Rechner spielen

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

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

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

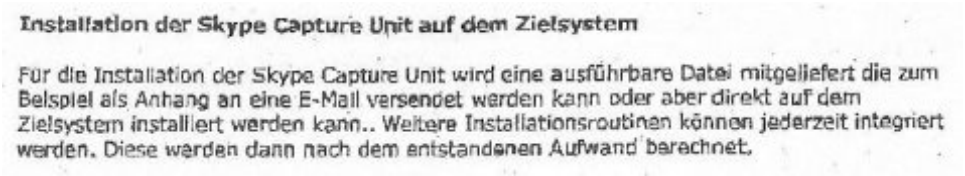
Dieser Quatsch ist gleich mehrfach zu beanstanden. Zum einen ist es kein Journalismus, wenn man zu bestimmten Themen ausschließlich „innenpolitische Sprecher“ und andere Lobbyisten zu Wort kommen lässt. Es geht nicht darum, wie politische Parteien die Welt sehen wollen, sondern darum, wie sie ist. Ein Journalist sollte den Ehrgeiz haben, die Leserinnen und Leser aufzuklären. Wenn das nicht geschieht, handelt es sich um Propaganda oder um das Verbreiten von Gerüchten.

Bei Compliance-Magazin.de lesen wir zum Beispiel: „Auf die Frage der Liberalen, wodurch sich die Quellen-TKÜ von der Online-Durchsuchung unterscheide, verweist die Regierung darauf, dass bei diesen beiden Maßnahmen ‚lediglich die

Technik der Vorgehensweise ähnlich‘ sei. Durch programmtechnische Vorrichtungen bei der Quellen-TKÜ sei von vornherein sichergestellt, dass eine ‚über den Überwachungszweck hinausgehende Online-Durchsuchung nicht möglich ist‘.

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

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



Installation der Skype Capture Unit auf dem Zielsystem

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

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

Eine ausführbare Datei, die per E-Mail-Anhang verschickt werden kann? Da lachen ja die Hühner!. Und die installiert das Zielobjekt nichtsahnend? Und der Verdächtige hat auch weder

einen Mac noch Linux? Ich zitiere mich selbst vom 27.08.2009:

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

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

Im dazugehörigen Blog heisst es: „The code is simple and straightforward. You have know malware development is no rocket science and if you expect big magic you are at the wrong place.“ Am besten hat mir der Kommentar „Giovannis“ gefallen: „Despite what some people say, Skype has never been secure. It is relatively easy to hack skype accounts, skype does not even check if the same user logs in simultaneusly on different machines and what is worst, the second user can get a copy of all the chats. Skype is good for housewifes that want to chat a bit with their kids, but for confidential conversations the use of strong voice encryption is required. In our company we tested many of them, we now keep with PhoneCrypt from securstar as it proved to be very good, stable, and with an excellent voice quality.“

Ich verweise auf mein hiesiges Posting „“Bayerntrojaner” zum

Abhören von Internet-Telefonie?“ sowie auf meinen Artikel in der Netzeitung: „Wenn der Laptop zweimal klingelt“.

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

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

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'!

John F. Kennedy zur Online-Durchsuchung

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

Halt! So war es gar nicht. Die einen wollen private Computer

behördlicherseits heimlich überwachen und die anderen sind dagegen, weil das obrigkeitsstaatlich undsoweiter sei.

Also führen wir schnell eine dritte Denkschule ein, um die schweizer Diskussion aufzulockern. Ganz egal, ob Männer oder Frauen im Kreis tanzen, das hat nichts mit dem Regen zu tun. Ganz egal, ob man einen „Bundestrojaner“ blöd findet oder nicht – ihn gab es noch nie, ihn gibt es noch nicht und es wird ihn so, wie DAUs sich das vorstellen, nie geben. Punktum. Es ist ein Hoax, ein Mythos, eine urbane Legende, eine frommes Überwachungsmärchen, aus den feuchten Wunschträumen der Zensur-Lobby entschlüpft, gar nicht wahr, eine Ente, alles gelogen und noch nicht mal gut erfunden, die Welt als Wille und Vorstellung – muss ich noch deutlicher werden?

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

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

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

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

Das ist doch zum Kringeln! Sie gehen schon von „Trojanern" aus, obwohl die vermutlich gar nicht wissen, was das ist. Magie eben. „Die" können das „irgendwie". Haben wir doch im Fernsehen gesehen. Oder im „Tatort", wo ein Hacker mit einem Laptop auf einem Hochhaus steht und die Verkehrsampeln ausschaltet.

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

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

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

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

Das Mitschneiden der Kommunikation hat uns schon Rot-Grün beschwert in Form der (Luftholen vor dem Aussprechen des Wortes nicht vergessen) Telekommunikations-Überwachungsverordnung (TKÜV) und der SINA-Box. Das Abhören hat aber rein gar nichts mit der „Online-Durchsuchung“ zu tun, es handelt sich auch um zwei völlig verschiedene Rechtsgrundlagen. Wieso muss man das immer total durcheinanderwürfeln? Nur um irgendwann das sexy Wort „Online-Durchsuchung“ unterbringen zu können?

Meidet die dunklen Ecken des Internet (burks.de)!

Immer wenn man glaubt, dümmer ginge es nimmer, kommt der Bund deutscher Kriminalbeamter daher und legt noch einen drauf. Bei Heise las ich: „Wer zukünftig im Internet einkauft, Geld

überweist, Behördengänge erledigt oder andere Geschäft abwickelt, soll sich nach dem Willen des Bundes Deutscher Kriminalbeamter zuvor bei einer staatlichen Stelle registrieren lassen, sagte der BDK-Vorsitzende Klaus Jansen in einem Interview der Neuen Osnabrücker Zeitung. (…) Zudem solle die Polizei das Recht bekommen, ‚Trojaner, Viren und Schadprogramme von privaten Rechnern entfernen zu dürfen'."

Das Märchen von der real gar nicht existierenden Online-Durchsuchung also. Anscheinend hat dieser Kerl gar nicht gemerkt, dass das Bundesverfassungsgericht den Wunschtraum des behördlichen Zugriffs in Echtzeit auf alle „Internet-Festplatten" schon längst verboten hat, obwohl das Anliegen ohnehin technisch nicht umsetzbar ist. Nach dem Motto „steter Tropfen höhlt den Stein" wird der Unfug einfach immer und immer wieder wiederholt. Politischer Flankenschutz kommt von Leuten wie Uhl (um mal jemand anderen als den unvermeidlichen Bosbach zu nennen), der die chinesische Zensur gern in Deutschland einführen möchte: „Was die Chinesen können, sollten wir auch können. Da bin ich gern obrigkeitsstaatlich".

Die Agitprop der obrigkeitsstaatlichen Internet-Ausdrucker steht ähnlich auch bei RP Online (Rheinische Post). Zeit Online wie auch andere verzichten auf jedwedes kritisches Wort – deutscher „Qualitätsjournalismus" eben.

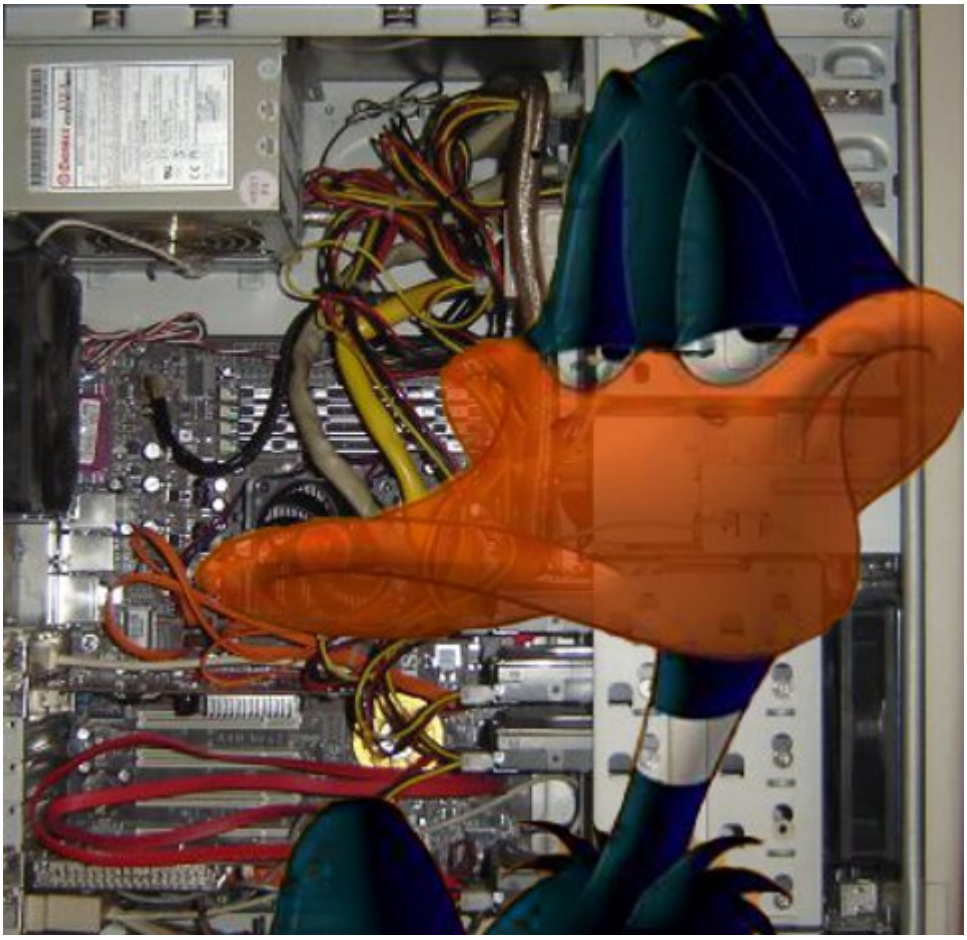
Die Neue Osnabrücker Zeitung titelt: „Kriminalbeamte wollen in sozialen Netzwerken verdeckt ermitteln." Das ist natürlich eine tolle Idee: Wenn jeder, der sich in Partnerbörsen, bei Facebook, StudiVZ oder sonstwo im so genannten Web 2.0 herumtreibt, damit rechnen muss, dass der Gesprächspartner ein verdeckter Ermittler ist, würden vielleicht einige DAUs mit ihren Daten vorsichtiger umgehen.

Im Heise-forum steht schon ein Entwurf der „Internet-Verkehrsordnung", der mir gefallen hat:
§1: Ins Internet darf nur, wer einen Internetführerschein hat.
§2: Für P2P-Protokolle gelten Geschwindigkeitsbegrenzungen.

§3: Staatlichen Paketen, bei denen das Blaue-Blinklicht-Flag im Header gesetzt ist, ist Vorrang zu gewähren. Zuwiderhandlungen werden mit Internetführerscheinentzug von sechs Monaten bestraft; sollten die Pakete den Bundestrojaner enthalten, kann die Strafe auf ein Jahr erhöht werden.
§4: Teile des Webs dürfen durch Aufstellen entsprechender Verkehrszeichen gesperrt werden.

„Weniger als ein Prozent der 260000 Polizisten in Deutschland“ seien „fit fürs Netz“. Das merkt man. Jansen ist ein schlagendes Beispiel dafür.

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'!

Sicherheit: Dau, Dauer, am Dausten

Das hier fand ich in einem Heise-Forum:

„Man stelle sich vor, potenzielle Autokäufer würden sich darüber aufregen, dass sie erst einen Führerschein machen müssen, um zu beweisen, dass sie ihr Fahrzeug im Straßenverkehr beherrschen. Würde man einen PC- und

Internetführerschein durchsetzen, hätte sich das Mal- und Scareware-Problem komplett erledigt.

Komischerweise verlangt jeder Mensch mit gesundem Verstand, dass alle Verkehrsteilnehmer ihr Fahrzeug und die Regeln des Straßenverkehrs beherrschen. Beim Gebrauch von Computern jedoch lehnen scheinbar gesunde Menschen nicht nur konsequent jegliche Verantwortung ab. Sie fordern auch noch für sich das Recht ein, von dem technischen Kram überhaupt keine Ahnung haben zu müssen.

Es sind vermutlich dieselben Menschen, die Denunziations-Buttons in Webbrowsern, KiPo-Sperren und Bundestrojaner für eine gute Idee halten."

Jedes Wort wahr, auch und insbesondere bei Journalisten.

Die Ente nach Schweizer Rezept

Wie sich die Textbausteine der DAUs doch gleichen. „Staat will Zugriff auf Schweizer Festplatten", formuliert die Basler Zeitung unkritisch und ahnunglos. Natürlich kommt im gesamten Artikel kein Wort darüber vor, ob das überhaupt machbar sei, was das Bundesamt für Justiz dort will. Danach fragt niemand mehr. Es ist wie bei Schopenhauer – die digitale Alpenwelt als Wille und Vorstellung.

„Der Staat will künftig auf die Festplatten verdächtiger Personen zugreifen können. Mithilfe von Trojanern sollen Strafverfolgungsbehörden sich auf den Harddisks umsehen dürfen." Mit „Trojanern„? Halt. Bitte jetzt zunächst das Gehirn einschalten. So dämlich ist ja noch nicht einmal

Ziercke. („Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht.“) Der möchte mittlerweile schon gern vorher in die Wohnung des Verdächtigen einbrechen lassen, um zu versuchen, ob man physisch auf den Rechner zugreifen kann.

Wie will man erstens die IP-Adresse der Zielperson herausfinden? Wie will man zweitens einen „Trojaner“ genau auf deren Rechner schleusen, wenn die auch nur einmal die Ratschläge des Bundesamtes für Sicherheit in der Informationstechik beherzigt hat? Das geht nicht.

„Im Falle eines Verdachts sollen dank den Überwachungsprogrammen alle Mails, Fotos und Filme für die Untersuchungsbehörden zugänglich sein.“ Was soll dieser Unfug: Was ist, wenn die Person ihre E-Mail verschlüsselt? Das „Abhören“ digitaler Postkarten ist ja ohnehin leicht möglich. Was also noch? Wie will man von außen einen Keylogger installieren? Und wie will man unbemerkt und beweissicher abgefangene Informationen verschicken?

Basler Zeitung, es interessiert mich nicht die Bohne, was jemand „will“ und was sein „soll“, sondern nur, *wie* das geschehen könnte. Das wisst ihr nicht? Ihr habt noch nicht einmal diese doch nicht unwesentliche Frage gestellt? Dann solltet ihr euer journalistisches Selbstverständnis mal updaten.

„Das Bundesamt für Justiz rechtfertigt diesen Schritt damit, dass im Internet vermehrt über Verschlüsselung kommuniziert werde. Gerade Straffällige würden sich dies zunutze machen. Trojaner, die, einmal installiert, jede Tastatureingabe mitverfolgen können und die Informationen an den Urheber des Überwachungsprogramms schicken, sollen diese Lücke schliessen.“ Also doch Keylogger. Noch mal zum Mitschreiben: Wie wollt ihr den auf die (!) Rechner der Zielperson bekommen? Und gerade „Straffällige“ verschlüsseln? Beweise dafür?

„Oder des Vertriebs von verbotener Pornografie.“ Nun, das ist kein deutscher Satz. Wir versuchen ihn dennoch zu verstehen. Diese suggestive Wortwohl suggeriert uns, dass das Böse (auf dem die menschliche Fortpflanzung beruhgt) in bildlicher Form auf den berüchtigen „Internet-Festplatten“ lauert. Darf ich mich mal kurz selbst zitieren (06.02.2007)? Danke.

„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.“

Was mich am meisten aufregt, sind die merkbefreiten „Kritiker“. Sie kritisieren die Verschwörungstheoretiker des Bundesamtes für Justiz nur, anstatt laut zu rufen: „Der Kaiser ist nackt! Es gibt keine ‚Bundestrojaner'“!

Der Kaiser ist auch in Rheinland-Pfalz nackt

Das Innenministerium in Rheinland-Pfalz ist nicht für besonders ausgeprägte Internet-Affinität bekannt. Deshalb darf man denen auch nicht übelnehmen, dass sie die wohl bekannte Ente aka Hoax „Online-Durchsuchung“ über ihre Website watscheln lassen. Man möchte übrigens auch „verschlüsselte Internet-Telefonie“ überwachen. Wie, das weiß kein Mensch. Aber so ist das eben bei Enten: Die Welt als Wille und Vorstellung. Wehe, es erinnert jemand an die Realität.

„‚Für eine erfolgreiche Gefahrenabwehr ist es unerlässlich, dass die Methoden der Sicherheitsbehörden mit den technischen Möglichkeiten der Terroristen und Kriminellen Schritt halten‘, erklärte Bruch. Allerdings betont Bruch auch, dass das Recht der Bürger auf Privatsphäre auf jeden Fall geschützt werde. Die gesetzlichen Voraussetzungen für die Online-Durchsuchung berücksichtigten selbstverständlich die Rechtsprechung des Bundesverfassungsgerichts. ‚Wegen ihrer besonderen Schwere unterliegen solche Eingriffe daher engen Grenzen und sind auf

die Abwehr erheblicher Gefahren und schwerster Straftaten beschränkt.‘, unterstrich der Minister weiter. Denn nicht nur die gesetzlichen Voraussetzungen seien hoch angesetzt, auch die für eine solche Maßnahme zu treffenden Vorbereitungen seien außerordentlich zeitintensiv und komplex, so dass die Online-Durchsuchung voraussichtlich nur höchst selten zur Anwendung kommen werde.“

Das ist natürlich Kokolores und kompletter Blödsinn. Wie dem Stammpublikum bekannt und wie auch in meinem Buch zum Thema hinreichend erörtert, hat es noch nie eine Online-Durchsuchung gegeben, wie sie der Volksmund versteht, und noch niemand hat sich erkühnt, eine Erfolg versprechende Methode vorzuschlagen, den Rechner eines Vedächtigen zielgenau ohne dessen Wissen zu durchsuchen. Das geht gar nicht. (Meine Artikel in Telepolis zum Thema hat Wikipedia weggelassen – was die Ente stört, lässt man weg. By the way: Der Kaiser ist nackt!)

Hier kann man es zum Beispiel nachlesen: „Eine Online-Durchsuchung wurde – soweit sie dem Projektteam bekannt wurde – lediglich in drei Fällen angedacht und in zwei Verfahren beantragt, aber abgelehnt. In zwei weiteren Fällen wurde die Maßnahme genehmigt, aber nicht durchgeführt.“ Quod erat demonstrandum. Alles andere ist Verschwörungstheorie, und dafür sind die Medien und der Chaos Computer Club zuständig.

Sogar die taz rezensierte – weil es so nett geschrieben ist, hier eine Langfassung:

„Die sogenannte Onlinedurchsuchung ist nicht viel mehr als ein aufgeblasener Medienhype und ein zahnloser Papiertiger obendrein. Mit diesem Instrument lässt sich zwar jede Menge rechtspolitischer Flurschaden an-, aber wenig Effektives gegen den internationalen Terrorismus ausrichten. Dabei liegt der Skandal für die beiden Autoren weniger in der zweifelhaften Technik, als in den Fehlinformationen, die darüber verbreitet werden.

Denn, so die überraschende Ausgangsthese des Buchs: So etwas wie eine ‚Onlinedurchsuchung' gibt es überhaupt nicht, jedenfalls nicht als funktionierendes Instrument in Händen der Ermittlungsbehörden. Die Vorstellung, Polizei und Geheimdienste könnten sich heimlich in jeden PC hacken, und zwar ohne dafür die Wohnung des Betroffenen betreten zu müssen, kann demnach getrost ins Reich der Märchen verwiesen werden – zu hoch sind die technischen Hürden, die dafür überwunden werden müssten. Selbst Laien könnten sich mit einfachsten Mitteln erfolgreich gegen Spitzelprogramme dieser Art wehren; einmal abgesehen davon, dass bislang noch keine Behörde überzeugend dargestellt habe, wie ein solcher staatlich sanktionierter Hackerangriff in der Praxis überhaupt aussehen könnte.

Was den Glauben an den „Bundestrojaner" am Leben erhalte, sei nichts anderes als Ignoranz in Sachen Computertechnik und der Mythos von der Allmacht des ‚Hackers'. Die etablierten Medien hätten allesamt in der Berichterstattung über die Onlinedurchsuchung regelmäßig versagt, so die Kritik der Autoren. Praktisch durchgehend sei nach dem System ‚Stille Post' verfahren worden: Einer schreibt vom anderen ab, und am Ende bestätigen sich Halb- oder Unwahrheiten von selbst. (…) Schröder weist überzeugend nach, dass es entgegen anderslautenden Berichten bis jetzt keinen einzigen erfolgreichen Einsatz eines ‚Bundestrojaners' gegeben hat."

Und was machen die Medien im aktuellen Fall daraus? Kein kritisches Wort, weder bei Heise noch beim SWR. Es wird einfach so getan, als sei so etwas möglich. Recherche? Fehlanzeige.

So perpetuuiert sich die Ente. Oder, wie Albert Einstein 1922 richtig sagte: „Jeder Blödsinn kann dadurch zu Bedeutung gelangen, dass er von Millionen Menschen geglaubt wird."

Screenshot: SWR zum Thema – man kann muss die Sicherheitseinstellungen des Browsers herunterfahren, um einen

Beitrag rezipieren zu können – so werden Surfer zur Dummheit erzogen.