Ozapftis exekutiert

Ein Artikel von mir auf Telepolis: „Ozapftis exekutiert – Nach der Aufdeckung des Schnüffelprogramms gibt es die üblichen Argumente, eine wirkliche Online-Durchsuchung gibt es aber immer noch nicht.“

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.

Mescalero, reloaded

Die Nachgeborenen werden nicht wissen, wer in die 70-er Jahren Mescalero war. Um er kurz zu machen: Der freute sich heimlich über etwas, worüber „man“ sich nicht freuen durfte, weil das pöhse gewesen wäre. „Unzulässige Schadenfreude“ oder so.

Unsd jetzt zu etwas vermeintlich ganz anderem. Was lesen wir in der Washington Post? „Anonymous hackers claim to have stolen encrypted military passwords from major US contractor“.

Ich mag das eigentlich nicht, weil derartige Schlagzeilen den Mythos beflügeln, „Hacker“ besäßen irgendwelche magischen Fähigkeiten und es könnte sogar eine „Online-Durchsuchung“ stattfinden, wenn man nur Beamte in diesen Fertigkeiten schulen könnte. Mitnichten.

Es ist alles ganz einfach. Ein Satz erklärt es – „Anonymous“ antwortet der betroffenen Militär-Firma:

„You have a security policy?” they said. „We never noticed.“

Quod erat demonstrandum. Bruhahaha.

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?

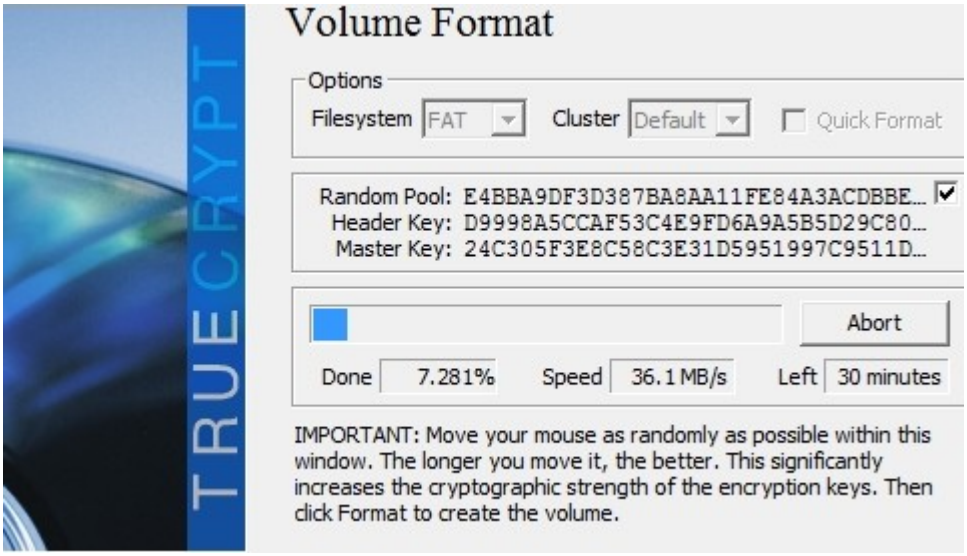
„Nutzen die Ermittler das Durcheinander einer Hausdurchsuchung“ – ach ja? So geht das also in Bayern zu, das überrascht mich nicht. Da kann ich ja froh sein, dass die Beamten, die meine Wohnung durchsuchten, nicht alle Buchregale umgeworfen, das Geschirr auf den Boden und die Monitore mal eben so umgestoßen 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.

Meine Rechner sind besenrein!



Wer meine Computer beschlagnahmt oder klaut, wird gar keine Dateien auf denselben finden, weder Texte noch Bilder. (Der Linux-Rechner ist eh komplett verschlüsselt.) Das gilt für alle drei Rechner (oder waren es vier?). Natürlich denkt der Mensch, der etwas zu verbergen hat (deutsche Journalisten, bitte wegzappen! Das ist nichts für euch!), an Truecrypt. Ja, bei mir ist alles digital verrammelt und verriegelt.

Mir fiel eben unangenehm auf, dass die ältere Festplatte, auf der die Daten meines auch schon sehr alten Laptops (Windows XP, igitt!) gesichert sind, gar nicht abgedichtet war. Also habe ich sie komplett formatiert und mit Truecrypt verschlüsselt.

Jetzt warte ich auf eine „Online-Durchsuchung." Mein Lieblingszitat: „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."

Nur zu! Die Kollegin Annette Ramelsberger hat weder widerrufen noch bezweifelt sie den Unfug, den sie dort 2006 verzapft hat.

Sternstunden des Journalismus

Der Schauspieler in "Inception": Er gilt als Womanizer.

Spiegel ~~online~~ gilt als Leitmedium. Burks.de gilt als Nörgel-Internet-Webpräsenz-Portal. Die „Online-Durchsuchung“ gilt als einflussreichster Hoax des Jahrzehnts. Deutsche Journalisten gelten als verschnarcht und obrigkeits-treu. Sex gilt als verkaufsfördernd. Wolfsburg gilt als Stadt.

Chinesen greifen das Pentagon an, revisited

Diesen Artikel schrieb ich hier am 04.09.2007. Untertitel: „Offenbarung statt Recherche.“ Das Niveau der

Berichterstattung hat sich nicht geändert: Einer schreibt vom Anderen ab, ohne die Fakten zu überprüfen. Irgendwann ist die Zahnpasta aus der Tube und keiner will es gewesen sein. Die pöhsen Chinesen waren es so lange nicht, bis mir jemand Beweise zeigt, die ***nicht*** *von Geheimdiensten oder anderen Pressure Groups mit einschlägigen Motiven stammen.*

Die Financial Times hat es behauptet und alle plappern es natürlich nach: „Chinese military hacked into Pentagon“. Jetzt stelle mer uns ganz dumm. Ist das wahr? Gibt es Beweise? Ist das möglich? Kann man das überprüfen?

Die Zeit ersetzt die Recherche durch Offenbarung: „Hacker des chinesischen Militärs sind offenbar ins EDV-Netzwerk des Pentagon vorgedrungen.“ Anschließend beruft man sich auf die *FTD*. „Wie die britische Zeitung am Dienstag unter Berufung auf amerikanische Regierungsstellen berichtete, wurden bei dem Hacker-Angriff auch Teile des EDV-Systems im Büro von US-Verteidigungsminister Robert Gates zum Absturz gebracht. Falls das so stimmt, bedeutet es, dass die Computerexperten Chinas inzwischen in der Lage sind, zentrale Systeme andere Länder stillzulegen.“

„Falls das so stimmt“ – ein journalistisches Armutszeugnis. Wenn man etwas nicht weiß, muss man es eben nachprüfen und nicht irgendwelche Gerüchte in die Welt hinausposaunen, nur weil es andere auch tun. Und was ist, wenn es nicht stimmt? Nimmt die *Zeit* dann alles zurück und behauptet, es sei in Wahrheit Osama bin Laden gewesen? Und der Heise-Newsticker? „Chinesische Angreifer stecken offenbar hinter Cyber-Attacke auf das Pentagon“ Offenbar. Oder auch nicht.

Nach der Attacke Mitte Juni hatte das Pentagon 1500 Rechner für mehr als eine Woche offline genommen. Nun heißt es, auf dem erfolgreich angegriffenen Mail-Server hätten „größtenteils“ keine vertraulichen Daten gelegen. Momentan laufen noch Untersuchungen darüber, wie viele Daten entwendet wurden. Vor Kurzem gab es auch Berichte…“ Es gab Berichte.

Und was sagt uns das jetzt? Es gab auch Berichte, dass Hänsel und Gretel in den Wald gegangen seien. Man muss zugunsten des *Heise-Newtickers* anmerken, dass der nicht vorgaukelt, eigene Quellen zu besitzen oder selbst recherchiert zu haben. Nein, alles ist abgeschrieben. Was sagt also das Original?

„The Chinese military hacked into a Pentagon computer network in June in the most successful cyber attack on the US defence department, *say American officials*.

The Pentagon acknowledged shutting down part of a computer system serving the office of Robert Gates, defence secretary, but *declined to say* who it believed was behind the attack.

Current and former officials have told the *Financial Times* an internal investigation has revealed that the incursion came from the People’s Liberation Army.

One *senior US official said* the Pentagon had pinpointed the exact origins of the attack. *Another person familiar with the event said* there was a ‚very high level of confidence…trending towards total certainty' that the PLA was responsible."

Es ist also alles supergeheim, so supergeheim, dass eine Person, die mit dem Ereignis vertraut ist, es gleich ausplaudert. Der Rest nicht nur diesen Artikels, sondern auch aller, die von ihm abschreiben, ist gefüllt mit Textbausteinen über Merkels Besuch in China undsofort. hat also nichts damit zu tun. Der Kern ist ein Gerücht aus „gewöhnlich gut unterrichteten Kreisen." Um die Pointe gleich vorwegzunehmen: Die China-Hacker kommen nicht. Vielleicht bin ich ein notorischer Zweifler, Nörgler, Querulant, Besserwisser – aber ich glaube kein Wort. Das klingt so nach der Sprechblase: „Verfassungsschutz: Immer mehr Nazis nutzen das Internet."

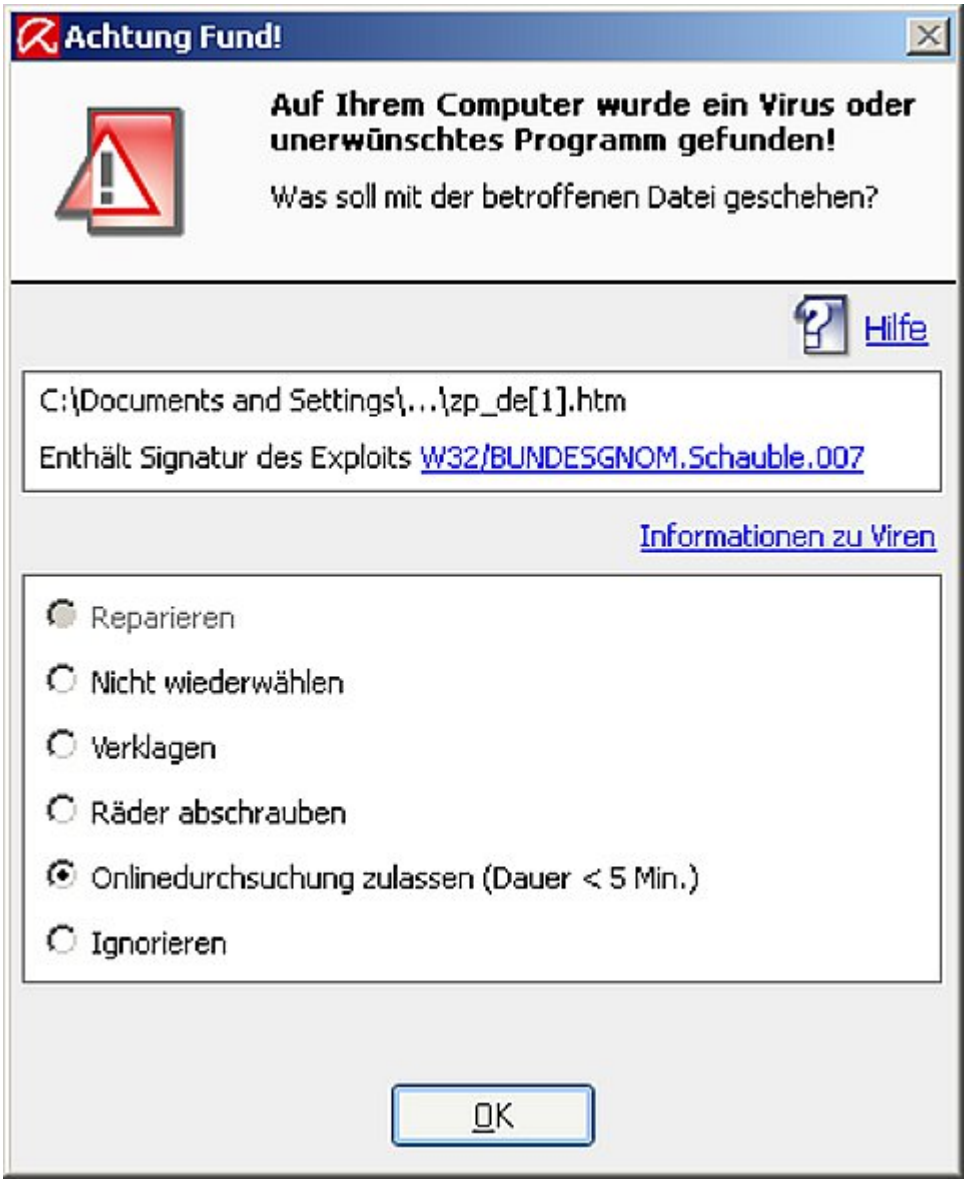
Ganz einfach. Oder offenbar auch nicht: Wer einen Server angreift, sollte und könnte vielleicht vorher auf die Idee kommen, seine Spuren zu verbergen – etwa mit schlichten Mitteln wie mit einem Tor-Server. Sollte die Volksbefreiungsarmee Rechner des Pentagon angreifen, ohne

dafür zu sorgen, dass ihre IP-Adressen vorher geschreddert werden? Wikipedia wäre nicht auf dem neuesten Stand, dort ist von „veralteter Kommunikationstechnik" in Chinas Streitkräften die Rede. Aber:

„Allerdings wurden in der Miliz Einheiten geschaffen, die sich auf moderne Kommunikationstechnik spezialisieren und aus Bewohnern der urbanen Zentren des Landes rekrutieren. Diese Fachleute sollen ihr zivil erworbenes Wissen um die Computertechnik in die VBA einbringen.“ Da haben wir’s: Die Miliz war es. Und die hat „zehn Millionen Angehörige“. Dann kann Schäuble bald damit rechnen, selbst ständig online durchsucht zu werden.

Bilder: Hacker der Zhōnggúo Rénmín Jiěfàng Jūn bei einer Parade (oben). Der chinesische Hacker-Minister 中国人民解放军/中國人民解放軍 (Mitte). Hacker der Volksbefreiungsarmee bereiten sich auf der Online-Durchsuchung von Second Life vor.

Bundestrojaner Chop Suey, revisited



Die Bundesregierung macht keine Angaben dazu, ob sie den Bundestrojaner gegen Terrorverdächtige einsetzt hat. Wer hätte das gedacht! Geht ja auch nicht. Sie können ja nicht sagen: Heyy, wir haben es nicht hingekriegt, weil wir nicht wussten, wie wir die Software auf den Rechner des Verdächtigen hätten beamen sollen. Er hat uns leider nicht heimlich in seine Wohnung gelassen.

Es reicht doch aus, den Medien wie Golem die Verschwörungstheorie verbreiten, es gäbe eine „Online-Durchsuchung“ (aka Fernwartung eines Privatrechners durch Ermittlungsbeamte). By the way: der so genannte „Trojaner“ (der gar kein Trojaner ist, sondern eine ganz normale Spionagesoftware), schnüffelt per Skype. **Das ist etwas**

anderes!

Richtig und falsch reinhacken

Richtig bei Heise Security: „Bei dem Diebstahl von rund 200.000 Kundendaten der Citibank mussten die Kriminellen nicht tief in die Trickkiste greifen, wie ein Sicherheitsexperte gegenüber der New York Times bekannt gegeben hat. Demnach gelang der unberechtigte Zugriff, den die US-Bank bei einer Routinekontrolle Anfang März entdeckt hat, durch das simple Manipulieren eines URL-Parameters.“

The method is seemingly simple, but the fact that the thieves knew to focus on this particular vulnerability marks the Citigroup attack as especially ingenious, security experts said.

Falsch bei Spiegel ~~online~~: „Den beiden Angeklagten wird vorgeworfen, zwischen März 2009 und März 2011 Computer von Musikfirmen manipuliert zu haben. Mit Spionageprogrammen, sogenannten Trojanern, stahlen sie laut Anklage bis dahin unbekannte Songs…“

Wer schützt unsere Kinder eigentlich vor den Verschwörungstheorien der Holzmedien, zu denen auch gedrucktes linkfreies Papier à la Spiegel ~~online~~ gehört? Lugt da wieder die real gar nicht existierende „Online-Durchsuchung“ hervor? Guckst du hier:

Spiegel Online (ein Link zur Quelle, o Wunder!) fantasiert wieder wahllos herum: „Denn Bronk hackte sich in deren E-Mail-Konten…“ Das hätte die Taz auch nicht schlechter formulieren können. Wie zum Teufel, „hackt“ man sich in E-Mail-Konten? Etwa mit einer real gar nicht existierenden „Online-

Durchsuchung“?

Nein, der Kerl war kein echter „Hacker“, sonder jemand, der sich des guten alten Social Engineering bediente: „Ausgestattet mit dem derart zusammengetragenen Hintergrundwissen ging er daran, die E-Mail-Passwörter seiner Opfer zu ändern. Dazu machte er sich nicht etwa die Mühe, zuerst deren Passwort herauszufinden. Stattdessen gab er sich deren E-Mail-Providern gegenüber als Inhaber des jeweiligen Accounts aus und beantragte, mit der Begründung, er habe sein Passwort vergessen, online ein neues. Weil viele Provider immer noch Standardabfragen, beispielsweise nach dem Mädchennamen der Mutter, verwenden, um in solchen Fällen die Identität des Antragstellers zu überprüfen, fiel es Bronk nicht schwer, die E-Mail-Konten zu übernehmen.“

„Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Daten oder Dinge zu gelangen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um Dinge wie geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking.“

Also bitte keine Computermythologie, Technik-Schamanismus oder anderen Regenzauber: Man kann sich nicht einfach so irgendwo „reinhacken“.

---

etc/init.d/ssh start

Udo Vetter über einen „Akt der deutschen Behörden“: „Ein

deutscher Staatsanwalt ist nicht verpflichtet, Server zu beschlagnahmen – bloß weil ausländische Ermittlungsbehörden das von ihm verlangen. Es gibt da keinen Automatismus wie zum Beispiel beim Europäischen Haftbefehl. Die Staatsanwaltschaft Darmstadt hatte also in eigener Regie und anhand der deutschen Gesetze zu prüfen, ob sie vom Bundeskriminalamt, wie heute geschehen, die Server der Piratenpartei vom Netz nehmen, einpacken und / oder spiegeln lässt."

„…obwohl nicht einmal ein Rechtshilfeersuchen vorlag – das wurde nachgeholt", schreibt Hal Faber: „Die flüchtige Datei, die solchermaßen inhaftiert werden sollte, soll angeblich ein SSH-Schlüssel sein, der zum Angriff auf den französischen Energiekonzern EDF gestohlen wurde. Dass dieser Unsinn straffrei erzählt werden kann, zeugt nicht gerade vom Sachverstand der Beteiligten".

Sachverstand? Hat das jemand erwartet? Bei Ziercke? Hat jemand nach Sachverstand gefragt, wenn es um die real gar nicht existierende „Online-Durchsuchung" ging?

Vgl. auch der Schockwellenreiter: „Eine Demokratie findet nicht statt".

Nicht vergessen: heute ist in Bremen Bürgerschaftswahl!

Die Software lädt sich beim Surfen automatisch herunter

Eine Falschmeldung bei Focus Online: „Die Software lädt sich beim Surfen automatisch herunter und installiert sich selbstständig auf dem infizierten Computer."

Das ist mitnichten so. Nichts passiert „automatisch“, nur wenn sich ein Internet-Nutzer absolut bescheuert verhält – offenbar wie ein Focus-Redakteur, der, wie hier, keine Ahnung hat, wovon er redet. Schon mal etwas von Noscript gehört oder vom Browsercheck? Oder von Betriebssystem Linux? Nein? Quod erat demonstrandum.

Kein Wunder, dass Focus Online das Märchen, der BND vollzöge „Online-Durchsuchungen“, mit großer Penetranz wiederholt.

Update verfügbar

Ich habe mir eigene eigene Verschwörungstheorie zurechtgelegt. Das abgrundtief dämliche und beratungsresistente Verhalten vieler Computer-Nutzer und die Verschwörungstheorie, es gäbe so etwas wie eine gezielte „Online-Durchsuchung“, kann ich mir nur erklären, weil Windows-Nutzer lernen, den Ausnahmezustand als normal zu erachten.

Jeden Morgen, wenn ich einen meiner Windows-Rechner anstelle, werde ich überschüttet mit Meldungen wie „neue Updates“ verfügbar und so weiter. Nicht nur das, viel schlimmer: Ich habe natürlich mein System so eingestellt werden, dass ich gefragt werde, ob ich etwas zulassen will. Ich bin ja nicht

bescheuert und lasse das Bill Gates entscheiden, oder?

Das aber wird von Windows als *Computerproblem* definiert, das *überprüft* werden müsse. Das wäre so, als würde ich ein Auto beim Fahrer darüber beschweren, dass nur er es mit dem Autoschlüssel öffnen kann, nicht aber jeder x-beliebige Tankwart, der Bundesinnenminister und noch zahllose weitere unbekannte Personen. Diesen Quatsch als normal anzusehen – dazu werden Windows-Nutzer tagtäglich trainiert.

„Normal“ finden viele Leute offenbar auch, dass irgendeine geheimnisvolle Person jeden Tag in ihren Rechner hineinschaut und feststellt, dass man „updaten“ müsse. Man fragt sich natürlich, wie doof Programmierer sein müssen, die ihr System – Windows – so gestalten, dass jeden Abend etwas kaputt geht, was dann am nächsten Morgen repariert werden muss. Das wäre so, als müsste ein Autobesitzer täglich zu einer viertelstündigen Inspektion in die Werkstatt. Kein Mensch würde sich noch ein Auto kaufen – nur Irre. Aber Irre gibt es bekanntlich genug.

Windows ist politisch reaktionär, weil es Leuten suggeriert, der Zugriff auf ihrer Privatsphäre – ihre Rechner – von außen sei normal und müsse per default gestattet werden. Das ist meine ganz private Verschwörungstheorie.

Screenshot oben: Windows 7, Screenshot unten: Linux Ubuntu 10.04 Lucid Lynx

أسامة بن لادن و تروكربت

Wenn es um die Themen Computer und Internet geht, sind deutsche Medien immer für Verschwörungstheorien („Online-Durchsuchung“), geheimnisvolles, aber ahnungsloses Geraune oder Dummschwätzerei gut.

„Nach ihrer Erstürmung des Verstecks haben die US-Navy-Seals große Mengen Daten und Dokumente in Bin Ladens Haus sichergestellt. In amerikanischen Medien ist von fünf Computern die Rede, darüber hinaus von zehn Festplatten und rund hundert Datenträgern, also vermutlich CDs oder Memory Sticks“, heisst es bei Spiegel offline.

Man muss jetzt unbedingt einen gar nicht so langen Artikel in elf (!) Teile zerhacken, ohne dass erkennbar wäre, warum der Leser nicht einfach scrollen könnte. aber es geht ja nicht um Information und Aufklärung, sondern um Klickarten! „So fühlt man Absicht, und man ist verstimmt.“, kommentierte schon Torquato Tasso diese dummdreiste Attitude.

Deutsche Journalisten gehen immer irrig davon aus, dass es auf den Rechnern andere Leute genau so chaotisch aussieht wie auf ihren eigenen und dass Ausländer genau so wenig Ahnung haben

wie sie. Warum sollte man auf den Computeren eines Terroristen, von dem man noch nicht einmal weiß, ob es in den letzten zwei Jahren einen Internet-Anschluss hatte, irgendetwas finden? Osama bi Laden wäre doch mit dem Klammerbeutel gepudert gewesen, hätte er Festplatten und USB-Sticks *nicht* mit Truecrypt verschlüsselt oder hätte er – wie Spiegel-offline-Redakteure -, nur elektronische Postkarten geschrieben. By the way: man kann E-Mails so verschlüsseln, dass kein Geheimdienst dieser Welt sie lesen kann. (Wer etwas anderes behauptet, hat im Mathematik-Unterricht beim Thema Algorithmen nicht aufgepasst oder ist ein Verschwörungstheoretiker und ein Dummkopf.)

„Truecrypt" heisst تروكربـــــت auf Arabisch. Falls ihr da etwas findet auf Osama bin Ladens Rechner, liebe Geheimdienstler, was so aussieht (vgl. Screenshot des Desktops bin Ladens oben, der burks.de exklusiv zugespielt wurde), dann vergesst den Rest einfach. Dumm gelaufen. Keine Chance wegen Kryptografie und so:

„Die Sicherheit der faktorisierungsbasierten Public-Key-Kryptographie liegt in der Verwendung eines Produkts aus großen Primzahlen, welches als öffentlicher Schlüssel dient. Der private Schlüssel besteht aus den dazugehörenden Primfaktoren bzw. davon abgeleiteten Werten. Die Zerlegung eines hinreichend großen öffentlichen Schlüssels gilt aufgrund der mathematisch sehr aufwendigen Faktorisierung als nicht praktikabel."

Das kann doch einen deutschen Journalisten nicht erschüttern. Fakten? Interessiert uns nicht. „An einem geheimen Ort, heißt es aus Washington, scannen Analysten der CIA und anderer Behörden bereits Material, um möglichst rasch einen Überblick zu erlangen." Heisst es aus Washington aus mindestens 25 unabhängigen Quellen…. Dann muss man es ja glauben und bei Spiegel offline und auch anderswo als „Tatsache" abdrucken.

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)

Zierckes Lügenmärchen, reloaded

SpOn: „Im Zuge der Ermittlungen hatte das BKA einen Trojaner für eine Online-Durchsuchung sowie eine Software für eine Telekommunikationsüberwachung auf seinem Rechner installiert. In abgehörten Gesprächen hätten die Drei den Bombenanschlag in Marrakesch ‚freudig begrüßt‘, berichtete Ziercke.“

Wie viele unabhängige Quellen haben wir für diese Behauptung, zumal Ziercke für das Thema der real nicht existierenden „Online-Durchsuchung“ hinreichend „qualifiziert“ ist? Wie wollen die das gemacht haben? Und was genau? Danach fragen deutsche Journalisten nicht. Quod erat demonstrandum. Sie würden auch keine Antwort bekommen.

Wahrscheinlich entpuppen sich ohnehin zwei Drittel der Mitglieder dieser „Terrorzelle“ wie gehabt als Spitzel des Verfassungsschutzes.

Bericht der EU-Kommission zur Evaluation der Vorratdatenspeicherung

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

Der Arbeitskreis Vorratsdatenspeicherung schreibt in seiner Bilanz dazu:

„Die verdachtsunabhängige und wahllose Vorratsdatenspeicherung ist die am tiefsten in die Privatsphäre eingreifende und unpopulärste Überwachungsmaßnahme, die die EU bis heute

hervorgebracht hat. Die EU-Richtlinie zur Vorratsdatenspeicherung verpflichtet alle EU-Staaten zur wahllosen Erfassung und Sammlung sensibler Informationen über soziale Kontakte (einschließlich Geschäftsbeziehungen), Bewegungen und das Privatleben (z.B. Kontakte zu Ärzten, Rechtsanwälten und Strafverteidigern, Betriebsräten, Psychotherapeuten, Beratungsstellen usw.) von 500 Millionen Europäern, die sich keines Fehlverhaltens verdächtig gemacht haben. Einer Umfrage zufolge lehnen 69,3% der Bürger eine Vorratsspeicherung aller Verbindungsdaten ab – kein anderes ‚Überwachungsgesetz' einschließlich biometrischer Pässe, Zugang zu Bankdaten, Online-Durchsuchung und Fluggastdatenspeicherung stößt auf so starke Ablehnung."

In einer Stellungnahme des AK Vorrat heisst es:

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

Bei Heise gibt es mehr dazu: „Die Nachweise, die EU-Länder für die Erforderlichkeit der tief in die Grundrechte einschneidenden Maßnahme erbracht hätten, seien zwar „begrenzt" gewesen, räumt die Brüsseler Regierungseinrichtung ein. Trotzdem verwiesen sie auf die wichtige Rolle, welche die Aufbewahrung von Telekommunikationsdaten für Ermittlungen

spiele. (…) … eine Studie des Wissenschaftlichen Dienstes des Bundestags hat aber bereits herausgefunden, dass die Vorratsdatenspeicherung in der EU die Aufklärungsquote in Ländern mit entsprechenden Auflagen nicht entscheidend verbessert hat. (…)

Für Alvaro zeigt die ‚mit siebenmonatiger Verspätung' vorgelegte Evaluierung, dass ‚wir einem Wildwuchs an nationaler Willkür gegenüberstehen'".

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

Quod erat demonstrandum.

Word bites DAUs in the Butt

„Internet-Kriminelle könnten demnach E-Mails mit Word-Dateien versenden, in denen entsprechend manipulierte Flash-Daten versteckt seien. Wer die Word-Dateien öffne, laufe Gefahr, sich eine Schadsoftware auf den Rechner zu holen," schreibt SpOn.

Dazu habe ich am 30.12.2004 schon etwas gesagt:

„Im Februar 2003 publizierte die britische Regierung ein Dossier über die angeblichen Erkenntnisse der Geheimdienste

über den Irak auf ihrer Website – der Text war ein Word-Dokument. Das war grob fahrlässig und dumm dazu: der Internet-Experte Glen Rangwala analysierte die Datei und entdeckte brisante Informationen. Eine Word-Datei verrät vieles über die Entstehungsgeschichte des Dokuments – was gelöscht wurde, in welcher Reihenfolge Textbausteine aneinandergereiht wurden und eventuell sogar andere Details."

Leider ist die Unsitte, Word-Attachments zu versenden, einfach nicht abzustellen.

Wikipedia gibt Auskunft über die Risiken und Nebenwirkungen von Word-Attachments. Hier eine leicht gekürzte Zusammenfassung von Richard M. Stallmann (engl.Version):

„Sie haben mir einen Anhang im Microsoft Word-Format geschickt, einem geheimen und proprietären Format, das ich deshalb nur schwer lesen kann. Wenn Sie mir einfachen Text senden, könnte ich es lesen.

Das Verschicken von Word-Dokumenten ist schlecht für Sie und für andere. Sie können nicht sicher sein, wie sie aussehen werden, wenn sie jemand mit einer anderen Version von Word betrachtet; vielleicht sind sie nicht einmal lesbar.

Das Erhalten von Word-Anhängen ist schlecht für Sie, weil sie Viren enthalten können. Das Senden von Word-Anhängen ist schlecht für Sie, weil ein Word-Dokument versteckte Informationen über den Autor enthält, die es Kennern erlaubt, Informationen über die Aktivitäten des Autors (vielleicht Sie) zu erlangen. Text, den Sie für gelöscht halten, kann immer noch peinlich präsent sein.

Aber vor allem übt das Versenden von Word-Anhängen Druck auf die Empfänger aus, Microsoft-Software zu benutzen, und führt dazu, dass ihnen keine Alternative bleibt. Damit werden Sie zu einer Stütze des Microsoft-Monopols. Dieses Problem ist ein Haupthindernis der breiten Akzeptanz von freier Software.

Würden Sie bitte den Gebrauch des Word-Formates überdenken, wenn sie mit anderen Menschen kommunizieren?“

Ich erwartete eigentlich die Meldung: „Die Online-Durchsuchung ist möglich! Man kann doch einfach E-Mail mit Word-Attachments verschicken!“ Das hat Tony Blair doch auch gemacht….“

Ihr könnt mir übrigens *keine* Word-Attachments schicken. Annahme verweigert – auf allen Rechnern. Das gilt auch für HTML-Mails (siehe oben).

Jetzt schnattert sie wieder…

Nein, Spiegel Offline, auch wenn ihr euch Mühe gebt, die Ente wiederzubeleben: Es gibt *keine* Online-Durchsuchung, auch wenn ihr die „landläufig“ so nennt. Das bayerische Landeskriminalamt hat nach der Methode „legal, illegal, scheissegal“ einem Bürger den Laptop weggenommen und dann eine Spionage-Software installiert.

„Denn der Kaufmann aus Bayern trug nach jener Kontrolle ein wenig mehr im Gepäck als vorher. Auf seinem Rechner hatte das bayerische Landeskriminalamt (LKA) eine Spionage-Software versteckt. Das heimlich am Flughafen installierte Programm sicherte der Polizei weitreichenden Zugriff auf den Laptop. Sobald sich das Gerät ins Internet einwählte, übermittelte es alle 30 Sekunden ein Foto des Bildschirms zu den Ermittlern – gut 60.000 in drei Monaten.“

Ein Keylogger also. Wie das? War der Rechner passwortgesichert? War er nicht mit Truecrpyt verschlüsselt? Konnte man mit admin-Rechten von externen Laufwerken einfach so booten? Wie haben die das also gemacht? *Das will ich wissen und das zu beschreiben wäre Journalismus, Kollege Steffen*

Winter und nicht so eine gequirlte Gerüchte-Scheiße wie in dem linkfreien Artikel!

„Im 30-Sekunden-Takt schickte es Fotos der Skype-Oberfläche und des Internet-Browsers an die Ermittler.“ Ach – es geht also nur um Skype? „Wenn das Programm der eigenen Leistungsbeschreibung gefolgt ist, hat es sich dort inzwischen selbst zerstört.“ Und wie heisst das Programm? So eins will ich auch – eine Software, die sich selbst vernichtet! Wieso ist Bill Gates da noch nicht drauf gekommen, so etwas zu erfinden?

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)

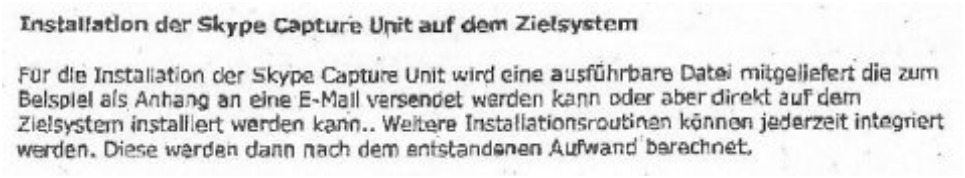
Bruhahahah. Das ist ja wieder ein gefundenes Fressen für unsere Verschwörungstheoretiker zum Thema „Online-Durchsuchung“. Hier geht es aber um Skype (vgl. auch den Beschluss des LG Landshut dazu.) Der Beschuldigte kommunizierte via Skype und benachrichtigte die Gesprächspartner vorher durch eine SMS.

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?

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“!