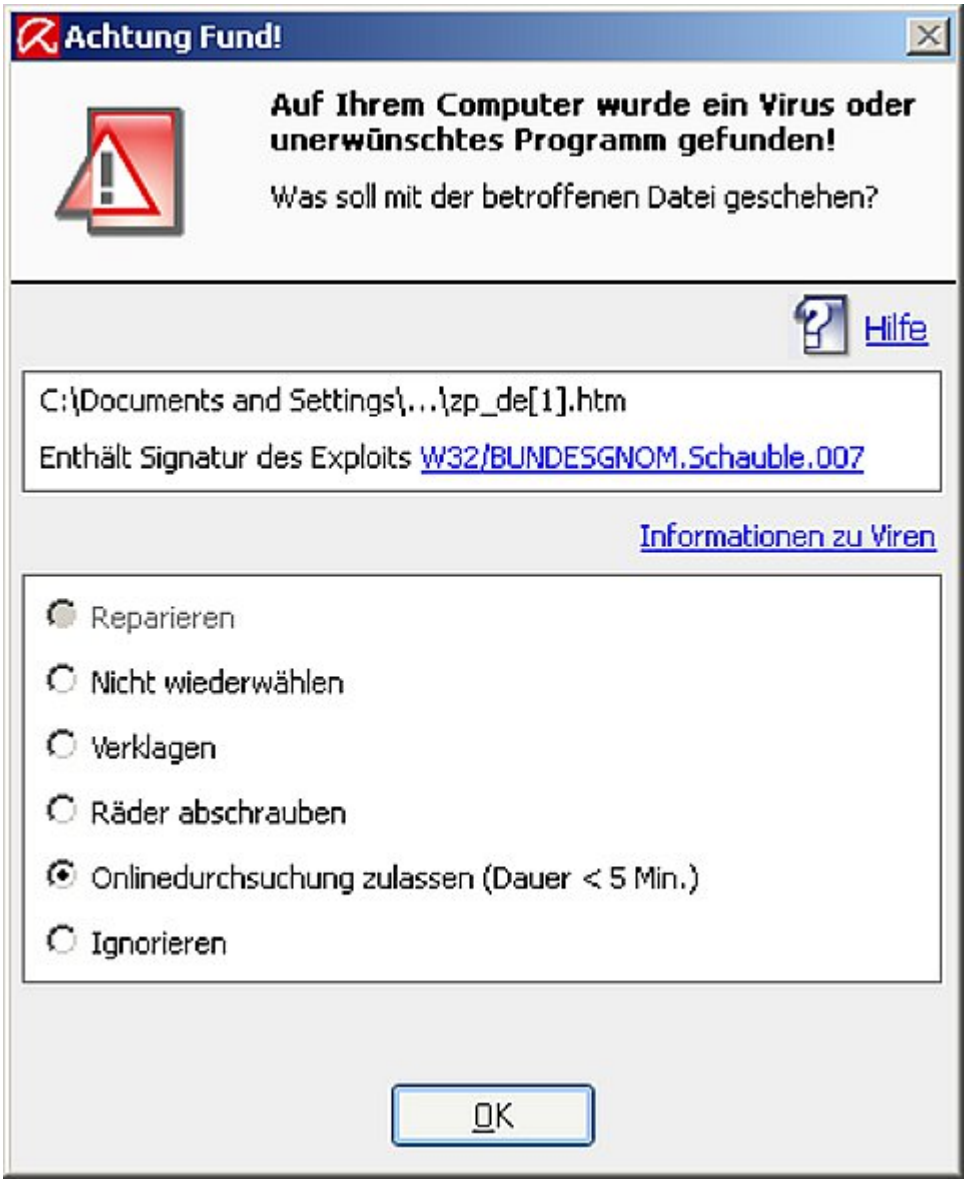
Bundestrojaner.zip

Hilfe, jemand wollte einen Bundestrojaner bei mir installieren! Nur gut, dass ich immer wachsam bin und die zunehmende Radikalisierung und Extremismusierung der E-Mail-Attachments bekämpfe!

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**

Bundestrojaner beim Afghanen?

Stefan Krempl scheibt bei Heise: „Der Bundesnachrichtendienst (BND) hat Berichten zufolge eine heimliche Online-Durchsuchung beim afghanischen Handels- und Industrieminister Amin Farhang durchgeführt, bei der auch die Kommunikation mit einer Spiegel-Reporterin erfasst worden sein soll.“ Ich glaube vorsichtshalber erst einmal gar nichts. Weiter heißt es: „Nach Informationen der Nachrichtenagentur ddp war es dem BND gelungen, mit Hilfe eines Trojaners auf der Festplatte von Farhang ein Spähprogramm zu installieren.“ Was sagen die Quellen?

Krempl zitiert sich in typischer Manier selbst: „Die monatelange Observation der Journalistin zwischen Juni und November 2006, die das Nachrichtenmagazin am Wochenende bekannt machte, war demnach offenbar ein ‚Nebenprodukt‘ der Bespitzelung des Spitzenpolitikers“. Das – der zweite Satz des Artikels – suggeriert, als sei die Observation eine „Online-Durchsuchung“ gewesen. Das war aber mitnichten so. Hinter dem

verlinkten „bekannt geworden verbirgt sich ein Artikel von Spiegel Online, in dem es lediglich heißt: „Der Bundesnachrichtendienst (BND) hat monatelang die E-Mail-Korrespondenz der 42-jährigen SPIEGEL-Reporterin mit dem afghanischen Politiker überwacht und mitgeschnitten.“ Das Abhören des Kommunikation hat mit einer Online-Durchsuchung nichts zu tun und ist ein Kinderspiel, wenn die Beteiligten ihre Korrespondenz nicht verschlüsseln. Typisch für das Niveau deutscher Recherche ist auch, dass das „Opfer“ Susanne Koelbl meinte, an einen afghanischen Politiker Postkarten schreiben zu müssen und „nicht ahnte“, dass auch andere Leute die lesen wollten – und das natürlich getan haben. Die Kollegin antwortet übrigens nicht auf meine E-Mails zum Thema.

Die Welt online berichtet: „…wurde zum Abschöpfen des E-Mail-Verkehrs zwischen der „Spiegel“-Journalistin Susanne Koelbl und dem Politiker aus Kabul zwischen Juni und November 2006 ein ‚Trojaner‘ eingesetzt. Das Spionageprogramm, für dessen Einsatz das Bundesverfassungsgericht unlängst hohe Hürden gesetzt hat, sei auf der Festplatte des Computers des Afghanen installiert worden, hieß es. Dabei seien auch ‚intime Bereiche‘ der persönlichen Lebensführung der Journalistin ausgespäht worden.“

Da haben wir’s. Jede Wette, dass der BND den physischen Zugriff auf den Rechner hatte und entweder einen Keylogger oder so etwas sie EnCase® Field Intelligence Model eingesetzt hat. [Vgl. c’t: Der weisse Spion]. Die Stattzeitung für Südbaden erwähnt ein weiteres interessantes Detail: Der heutige afghanische Wirtschaftsminister, ein ehemaliges Mitglied der deutschen Grünen uind „langjährig in Nord-Rhein-Westfalen ansässig,… (…) Die Ausspähung geschah ab 2006 per Trojaner. Also existiert schon ein funktionsfähiges Modell. Dabei wurde offiziell immer wieder geächzt, wie teuer so was sei und wie schwer zu installieren.“ Und genau das ist die Pointe: Der berüchtigte „Bundestrojaner“ wird im öffentlichen Diskurs als heimlciher Zugriff über das Internet verstanden.

Darum geht es hier aber gar nicht, sondern um ein Spionageprogramm, dass auf der Festplatte installiert worden war. Und so etwas ist gar nicht teuer und auch nicht kompliziert und existiert natürlich schon in verschiedenen Varianten.

Farhang hat das selbst bestätigt, wie die FTD meldet: „Er habe erfahren, dass der BND *seinen Computer im Büro* manipuliert habe. Er gehe davon aus, dass nicht nur einer seiner Computer für wenige Monate überwacht worden sei, wie der BND behaupte. „Ich habe das Vertrauen verloren und nehme an, dass deutsche Agenten alle meine Telefonate und E-Mails noch immer überwachen.“ Quod erat deminstrandum.

Falsch im Heise-Bericht ist definitiv: „Im Januar war bekannt geworden, dass der Geheimdienst bereits rund 60 Mal heimlich Zielrechner Verdächtiger im Ausland über das Internet ausgeschnüffelt haben soll“. Soll. Nicht hat. Dass das gar nicht stimmt und auch im damaligen Focus-Artikel falsch war, hat man mir mir telefonisch bestätigt. Es soll damals – durch den BND – nur *eine* „Online-Durchsuchung“ gegeben haben, und dafür auch nur eine Quelle. Es ist also gar nichts verifizierbar.

Schlechte Karten für „Bundestrojaner“

Das Urteil des Bundesverfassungsgerichts, das Verfassungsschutzgesetz in Nordrhein-Westfalen für nichtig zu erklären, ist salomonisch und listig: Es gestattet allen Beteiligten, das Gesicht zu wahren. Erst im Kleingedruckten – in der ausführlichen Begründung – wird deutlich, dass die

juristischen Hürden für die vom Bundesinnenministerium gewünschten „Online-Durchsuchungen“ fast unüberwindbar hoch sind.

Das neu eingeführte Gundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme als Teil des allgemeinen Persönlichkeitsrechts schließt einige juristische Lücken, die sich laut Gericht aus „neuartigen Gefährdungen“ im Zuge des „wissenschaftlich-technischen Fortschritts“ ergeben. Die durch das Grundgesetz garantierte „freie Entfaltung der Persönlichkeit“ musste exakter gefasst werden, weil Computer dafür eine immer größere Bedeutung erlangt haben, insbesondere in vernetzten Systemen. Das ist an sich nichts Neues. Interessant ist jedoch, dass das Bundesverfassungsgericht es für fragwürdig hält, prophylaktisch Informationen über Personen zu sammeln:

„Dabei handelt es sich nicht nur um Daten, die der Nutzer des Rechners bewusst anlegt oder speichert. Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können. In der Folge können sich im Arbeitsspeicher und auf den

Speichermedien solcher Systeme eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten des Nutzers finden. Werden diese Daten von Dritten erhoben und ausgewertet, so kann dies weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen“.

Daraus ergebe sich ein „erhebliches Schutzbedürfnis“, dem im Urteil Rechnung getragen wird. Der Einzelne sei darauf angewiesen, wenn er sich im Sinne des Grundgesetzes frei entfalten wolle, dass auch der Staat die Integrität und Vertraulichkeit informationstechnischer Systeme achte.

Der Schutz der „Persönlichkeit“ wird durch das Urteil erweitert auf die Technik, die die Person benutzt, um ihr Leben zu gestalten. Dazu passt, dass die Wohn-, Betriebs- und Geschäftsräume, die durch das Urteil zum Großen Lauschangriff vor dem Zugriff des Staates grundsätzlich geschützt wurden, jetzt auch die genutzten Rechnersysteme umfassen. Setzt sich jemand mit seinem Laptop in ein Cafe, gehört dieser automatisch zum „Kernbereich der privaten Lebensgestaltung“, in dem der Staat nicht einfach so herumschnüffeln darf. Der Bundesverfassungsgericht geht sogar ins Detail, Keylogger zu erwähnen und die elektromagnetische Abstrahlung des Computers, die man abfangen und auslesen könnte.

Selbst das bisherige Recht auf informationelle Selbstbestimmung ging dem Bundesverfassungsgericht nicht weit genug, weil heute jeder darauf angewiesen sei, Computer zu benutzen.

„Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung

schützt, weit hinaus.“

Das höchste deutsche Gericht beweist in seinem Urteil mehr technischen Sachverstand und hat investigativer zum Thema recherchiert als die meisten deutschen Medien. Es räumt auch gleich mit einigen urbanen Legenden auf. Hat es schon eine „Online-Durchsuchung“ privater Rechner gegeben? Es sei nichts über die Technik der bisherigen „Online-Durchsuchungen“ und über deren Erfolge bekannt. Die Präsidenten des BKA und des Verfassungsschutzes hatten keine Aussagegenehmigung. Das Bundesinnenministerium hatte auch in den Medien immer ausweichend reagiert und auf die Fragen des Bundesjustizministeriums geantwortet, die dazu nötigen Programmen würden erst noch entwickelt.

Im Verfassungsschutzgesetz Nordrhein-Westfalen findet sich die wolkige Formulierung, man wolle heimlich auf „informationstechnische System“ zugreifen. Noch schwammiger ist der „Zugriff auf Internet-Festplatten„. Von einer „Online-Durchsuchung“ war ursprünglich nicht die Rede. Letztlich lässt sich nicht mehr klären, ob der Gesetzgeber von Anfang an beabsichtigte, auch private Rechner durchsuchen zu lassen. Das Bundesverfassungsgericht hat die Diskussion kurz und bündig beendet. Nicht ganz humorlos wird erklärt, sowohl ein einzelner Rechner als auch das Internet als solches sei jeweils ein „informationstechnisches System“.

„Unter einem heimlichen Zugriff auf ein informationstechnisches System ist demgegenüber eine technische Infiltration zu verstehen, die etwa Sicherheitslücken des Zielsystems ausnutzt oder über die Installation eines Spähprogramms erfolgt. Die Infiltration des Zielsystems ermöglicht es, dessen Nutzung zu überwachen oder die Speichermedien durchzusehen oder gar das Zielsystem fernzusteuern. Die nordrhein-westfälische Landesregierung spricht bei solchen Maßnahmen von einer clientorientierten Aufklärung des Internet. Allerdings enthält die angegriffene Vorschrift keinen Hinweis darauf, dass sie ausschließlich Maßnahmen im Rahmen einer am Server-Client-Modell orientierten Netzwerkstruktur ermöglichen soll.“

Da der heimliche Zugriff auch auf private Rechner definitiv nicht ausgeschlossen sei, müsse man auch über die „Online-Durchsuchung“, wie sie allgemein diskutiert werde, urteilen.

Spannend ist das Urteil vor allem in den Passagen am Schluss, die die Ausnahmen regeln. Der Schutz des „Kernbereichsschutz“ wird aufgeweicht. Bisher mussten Lauscher die Mikrofone auschalten, wenn die Verdächtigen anfingen zu beten oder über Sex redeten. Praktisch war eine Überwachung kaum noch möglich. Das Bundesverfassungsgericht hat festgestellt, dass das im Prinzip auch für Computer gilt. Die aus technischer Sicht sehr

kühnen Thesen des Bundesinnenminsteriums, man könne einfach durch das Design der Software die Privatsphäre ausreichend schützen, ein Spionage-Programm werde keine anderen Programme des betroffenen Rechers beeinträchtigen und diesen nicht verändern, glaubt das Bundesverfassungsgericht nicht. Es sei „praktisch unvermeidbar“ bei einem heimlichen Zugriff, wenn er bei einem technisch unbedarften Verdächtigen funktioniere, auch an Daten zugelangen, die die Ermittler weder zur Kenntnis nehmen noch verwerten dürfen. Einen „rein lesenden Zugriff infolge der Infiltration“ gebe es nicht.

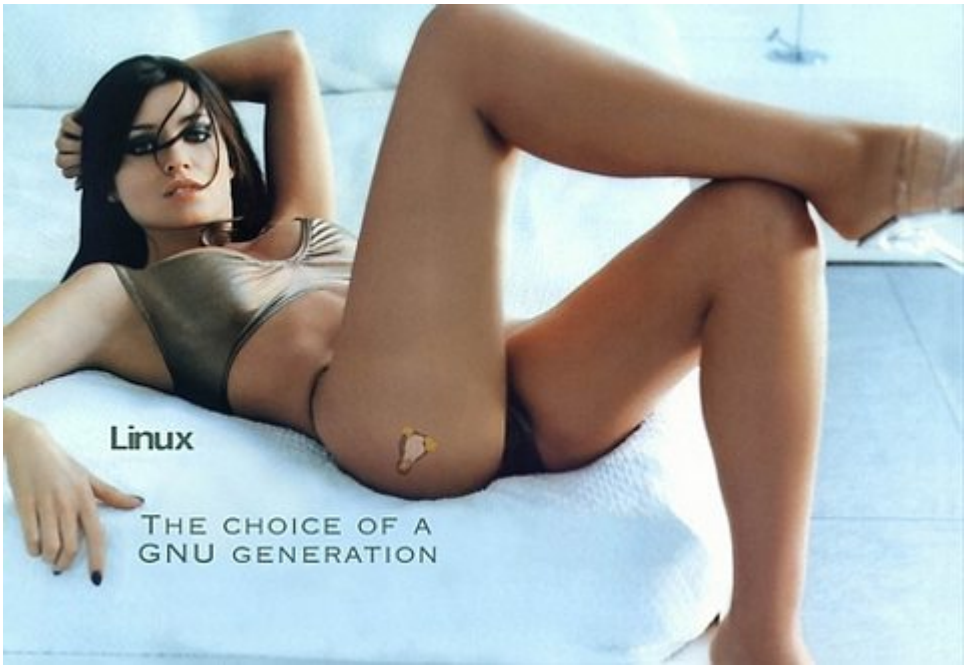
„Im Rahmen des heimlichen Zugriffs auf ein informationstechnisches System wird die Datenerhebung schon aus technischen Gründen zumindest überwiegend automatisiert erfolgen. Die Automatisierung erschwert es jedoch im Vergleich zu einer durch Personen durchgeführten Erhebung, schon bei der Erhebung Daten mit und ohne Bezug zum Kernbereich zu unterscheiden. Technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten arbeiten nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig, dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte.“

Das Bundesverfassungsgericht hat zur Kenntnis genommen, dass sich jeder vor einer „Online-Durchsuchung“ schützen kann – es verweist ausdrücklich auf die einschlägige Literatur. Dennoch könnte man allein deswegen diese Methode nicht ausschließen. Die Schranken für eine Überwachung eines privaten Rechners sind aber sehr hoch: Es muss eine konkrete Gefahr vorliegen, die ein „überragend wichtiges Rechtsgut“ bedroht. Klar ist auch, dass eine heimliche „Online-Durchsuchung“ immer einen schweren Grundrechtseingriff bedeutet, für ein ein Richtervorbehalt jetzt gesetzt ist. Das bedeutet: Nur bei unmittelbarer Gefahr für Leib und Leben einer Person oder bei konkreter Bedrohung für „den Bestand des Staates oder die Grundlagen der Existenz der Menschen“ dürfen die Ermittler

über eine „Online-Durchsuchung“ anfangen nachzudenken.

„Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann. Dagegen wird dem Gewicht des Grundrechtseingriffs, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, nicht hinreichend Rechnung getragen, wenn der tatsächliche Eingriffsanlass noch weitergehend in das Vorfeld einer im Einzelnen noch nicht absehbaren konkreten Gefahr für die Schutzgüter der Norm verlegt wird.“

Und wenn dann ein Richter dem zustimmte, bedürfe es noch besonderer Vorkehrungen, um den geschützten Privatbericht nicht zu behelligen. „Gibt es im Einzelfall konkrete Anhaltspunkte dafür, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berühren wird, so hat sie grundsätzlich zu unterbleiben.“



Durch das Urteil rückt das Sicherheitsinteresse der Staates ein wenig näher an die einzelnen Menschen heran. Der so

genannte „Kernbereich“ des Privaten ist kleiner geworden, dafür um so sicherer. Ein bloßes Gesetz schützte wenig vor privaten und staatlichen Datenkranken; ein Grundrecht jedoch, das als solches vom Bundesverfassungsgericht definiert ist, kann man kaum außer Acht lassen.

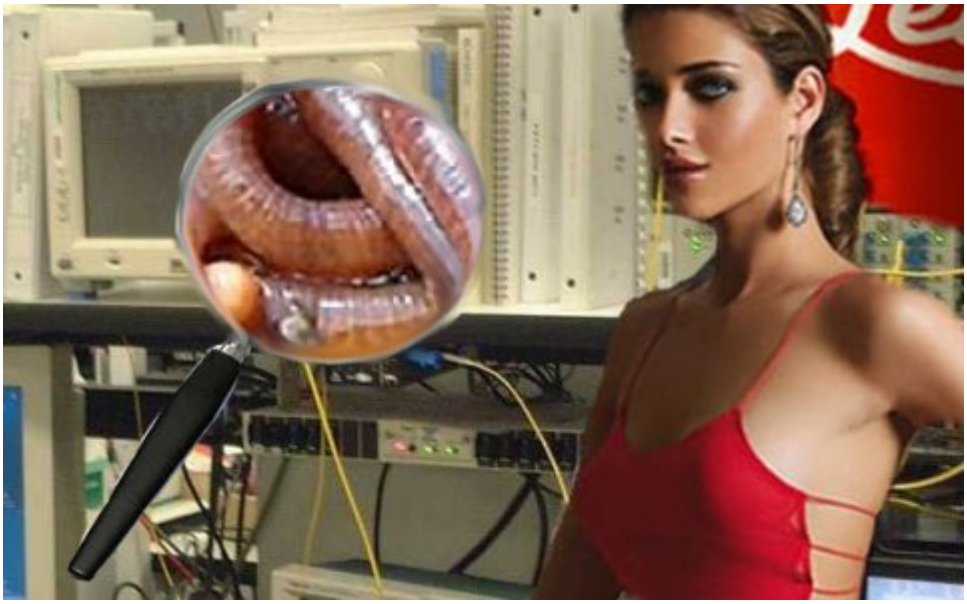
Die Hausaufgabe, die das Gericht dem Bundesinnenminister aufgegeben hat, ist so gut wie unlösbar, zumal eine Online-Überwachung durch die Polizei und das Bundeskriminalamt noch schwieriger ist als durch den Verfassungsschutz, der seine Daten für sich behalten kann. Die Ermittler hätten jedoch vor Gericht das zusätzliche Problem, beweisen zu müssen, dass die gefundenen Beweise auch echt sind. Möglicherweise, so steht es geheimnisvoll im Urteil, sei der „Beweiswert der Erkenntnisse gering“: Eine
„technische Echtheitsbestätigung der erhobenen Daten“ setze grundsätzlich „eine exklusive Kontrolle des Zielsystems im fraglichen Zeitpunkt voraus“. Und das muss man erst einmal technisch umsetzen und anschließend einem Richter beweisen – schlechte Karten für jede Art und Version eines „Bundestrojaners“.

Dieser Artikel von mir erschien am 27.02.2008 auf Telepolis.

Schlechte Karten für „Bundestrojaner“

Ein Artikel von mir auf Telepolis: ‚Schlechte Karten für „Bundestrojaner'“.
Nachtrag 28.02: Der Link zum Urteil ist falsch, darauf hat ein aufmerksamer Leser hingewiesen.

Bundestrojaner zu Bundeswürmern



„Wurm statt Windows-Update“ titelt der Heise-Newsticker. Eine typische Microsoft-Idee: Um einen Schädling zu entfernen, schleust man einen anderen Schädling ein, der zwar ein „Nützling“ ist, aber auch nur durch ein Leck im Betriebssystem eindringen kann. Die Methode ist nicht neu. Vor fünf Jahren lasen wir den hübschen Titel „Wurm jagt Wurm“. Auch da gruselt es den sicherheitsbewussten Computer-Nutzer: „Wenn der Wurm den Original-Blaster auf dem befallenen Rechner entdeckt, beendet er den zugehörigen Prozess, löscht die Wurmdatei msblast.exe und versucht den Microsoft-Patch zu installieren. Danach startet er den Rechner neu und macht sich auf die Jagd nach weiteren Opfern.“ Igitt.

Milan Vojnovic hat ein Papier dazu publiziert [„On the race of worms, alerts and patches“, with A. Ganesh, journal submission, 2006 (conf ver ACM WORM 05)], das aber schön älter ist. Bruce Schneier wettert gegen die Idee („Benevolent Worms“) an sich, was zu erwarten war und womit er sicher Recht

hat. Er bezieht sich auf einen Artikel der New Scientist.com: „Friendly ‚worms' could spread software fixes". „Milan Vojnović and colleagues from Microsoft Research in Cambridge, UK, want to make useful pieces of information such as software updates behave more like computer worms: spreading between computers instead of being downloaded from central servers. The research may also help defend against malicious types of worm, the researchers say."

Statt permanent „Patches" und neue „Sicherheitsupdates" in den löchrigen Käse zu stopfen, möchte das Microsoft durch „gute" Würmer erledigen lassen. Das erschließt sich mir theoretisch nicht ganz: Ein Wurm dringt prinzipiell über Schwachstellen im System (Windows!) ein. „Würmer warten andererseits nicht passiv darauf, dass sie mit infizierten Dateien weitergegeben werden. Sie versuchen auf unterschiedliche Art, aktiv via Netzwerk weitere Computer zu infizieren. Aber auch ein Wurm kann – wie ein Virus – in vertrauenswürdigen Dateien getarnt integriert sein, in diesem Fall hat man evtl. beide Übertragungsarten und daher eine Mischform. Als dritte Art gibt es noch die Trojaner (Trojanisches Pferd), diese zeichnen sich vor allem dadurch aus, dass sie eine Hintertür auf dem System installieren, über welche die Versender (etwa die Programmierer) Zugriff auf den kompromittierten Rechner haben. Heutzutage sind häufig Mischformen (Trojanerwürmer und Trojanerviren) anzutreffen."

Sollen die Windows-Benutzer bestimmte Sicherheitslücken jetzt bewusst offen lassen, damit die gutartigen und von Kleinweich autorisierten Würmer die bösen Würmer angreifen und auf dem Rechner eine digitalen Wurmkrieg beginnen? Schneier schreibt: „Giving the user more choice, making installation flexible and universal, allowing for uninstallation – all of these make worms harder to propagate. Designing a better software distribution mechanism, makes it a worse worm, and vice versa. On the other hand, making the worm quieter and less obvious to the user, making it smaller and easier to propagate, and

making it impossible to contain, all make for bad software distribution.“

Vielleicht denkt Microsoft ganz kommerziell? Wäre ein angeblich gutartiger Wurm nicht ein Exportartikel nach Deutschland? Bundestrojaner zu Bundeswürmern!

Cyberdings oder: Unter Staatsgriechen et al

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

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

Die Zwangsfilter, die in Betriebssysteme eingebaut werden wollten, sind zugleich das Allerletzte und das Allerlustigste.

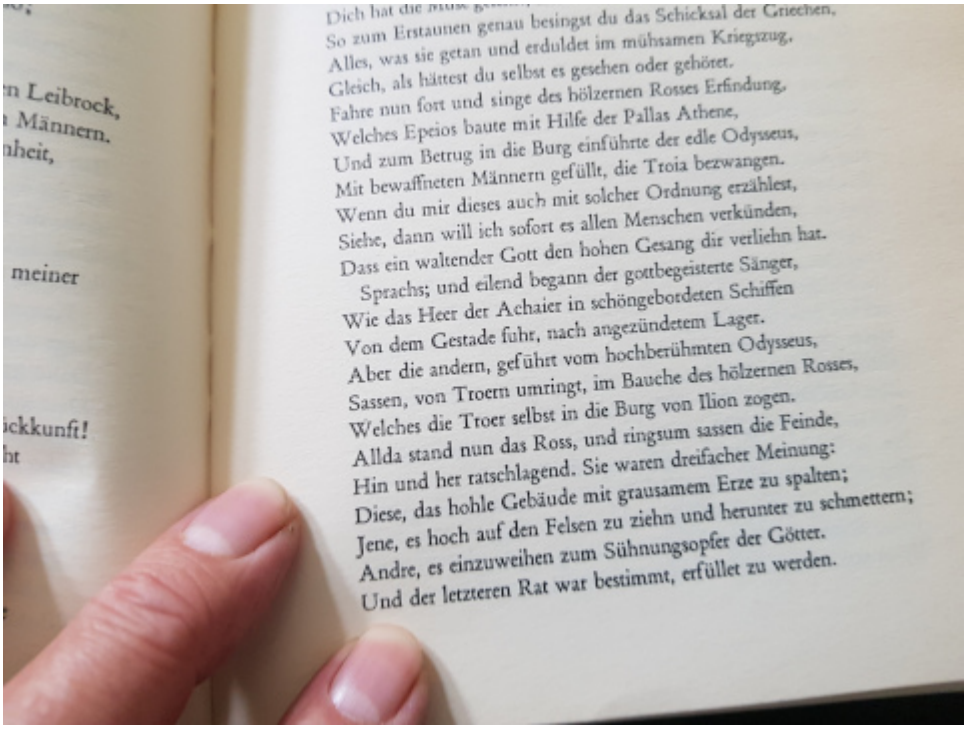
Ich möchte gerne mal die Gesichter der Leute sehen, die sich so etwas ausdenken: Eine Mischung aus Claudia Roth, Saskia Esken und Philipp Amthor?

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

Dann haben wir noch die x-te Version vom Staatstrojaner. Manchmal möchte ich den Kollegen Krempl einfach nur ohrfeigen, wenn er zm 1000-sten Mal mit seinen schlampigen Begriffen Schlampiges daherschreibt. Und warum müssten Journalisten bürokratisches Neusprech wie „Quellen-TKÜ plus" übernehmen? Das ist doch sowieso alles Unfug. Seit dem Erscheinen meines Buches hat mir immer noch niemand die Frage beantwortet, *wie* mir jemand ein Programm unterjubeln könnte, ohne dass ich mich vorher total bekloppt verhalten hätte? (FinSpy hatten wir hier schon.) Oder geht es gar nicht um meine Computer?

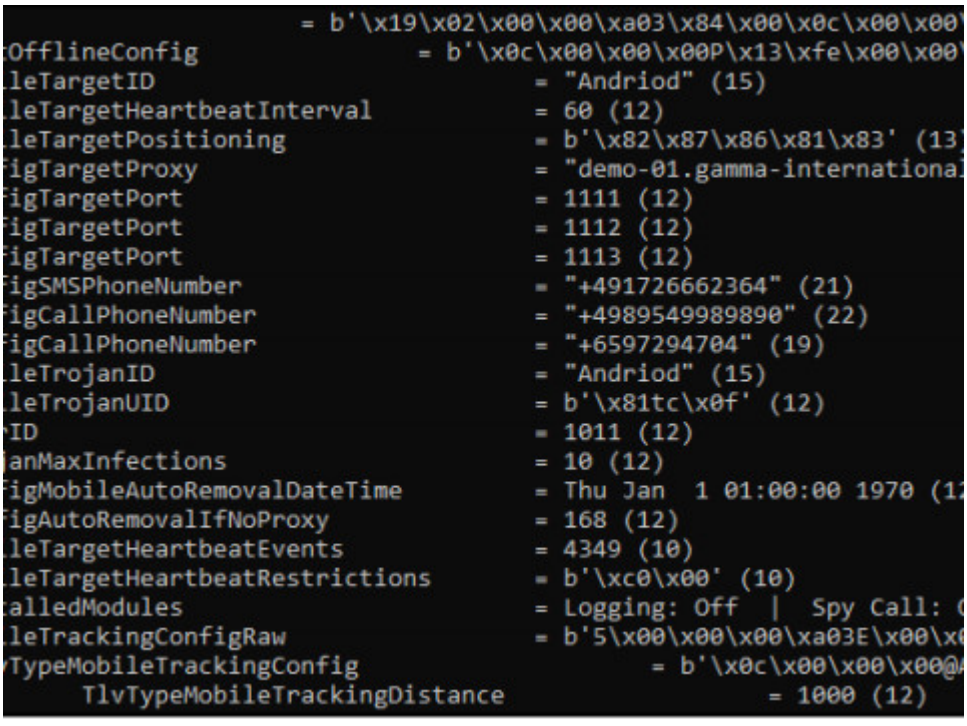
….sollte die Bundespolizei mithilfe des Bundestrojaners Messenger-Kommunikation etwa via WhatsApp, Signal oder Threema sowie Internet-Telefonate und Video-Calls… Gefasel und Bullshit-Bingo. Geht es nicht genauer? Mich regt noch mehr auf, dass die Journaille einfach nicht genauer nachfragt, sondern alles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

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



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

Bundestrojanische Gäule



Mit großem Interesse habe ich den Heise-Bericht über den „Spionage-Trojaner FinFisher“ gelesen. (Das heisst nicht „Trojaner“, sondern „Trojanisches Pferd“ – die Trojaner waren in Troja, und die Griechen saßen im Pferd.)

Schade, dass die Analyse des CCC „Evolution einer privatwirtschaftlichen
Schadsoftware für staatliche Akteure“ noch nicht erschienen war, als ich mein Buch veröffentlichte – es hätte Die Online-Durchsuchung gut ergänzt. Jetzt können wir „Butter bei die Fische“ tun. Kann die Frage: Wie fange ich mir so etwas ein? beantwortet werden?

Metzpolitik.org hatte schon vor vier Jahren geschrieben: „Die Begrenzung auf Windows 7 und Vista erscheint veraltet. Bereits vor zwei Jahren haben wir berichtet, dass FinSpy Mobile auch für alle mobilen Systeme (also iOS, Android, BlackBerry, Windows Mobile und Symbian) existiert. Und letztes Jahr haben interne Folien bestätigt, dass FinSpy alle großen Betriebssysteme (Windows, Linux und Mac OS X) infizieren kann.“

Der wichtigste Satz: „Über den Infektionsweg sagt das Team um Morgan Marquis-Boire wenig. Nur: Falls die Trojaner die mobilen Betriebssysteme nicht direkt angreifen, **benötigen alle untersuchten Exemplare eine Interaktion des Nutzers, wie dem Klicken auf einen Mail-Anhang oder eine Webseite**.“

Genau das – und nur das! – habe ich immer behauptet, während fast alle Medienberichte entweder das Problem, wie die Spionage-Software zu installieren sei, vornehm ignorierten oder zu Magie – der Hacker hackt und ist irgendwann drin – greifen mussten.

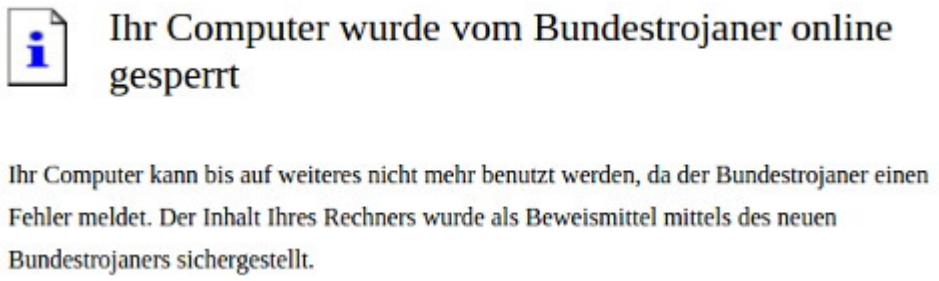
Aber wie soll das funktionieren, wenn das Zielobjekt nicht total bekloppt ist? Klicken auf einen Mail-Anhang? Oha! Oder gar auf einer Website? Mit oder ohne Javascript erlaubt? Selbst wenn ein unerfahrener Windows-Nutzer Virustotal nicht

kennt: Leben wir denn noch in Zeiten des Loveletter-Virus, als Outlook (wer nutzt das??) Anhänge nicht korrekt anzeigte?

Netzpolitik.org wies noch auf drei weitere Schwachstellen hin: Windows 7 SP1 – Acrobat Reader PDF Exploit, Windows 7 SP1 – Browsers Exploit, Windows 7 SP1 – Microsoft Office 2010 DOC-XLS Exploits. Schon klar. Das erinnert mich an 2003: „UK government gets bitten by Microsoft Word".

Hilfe, jemand wollte einen Bundestrojaner bei mir installieren! (25.06.2011) Nur gut, dass ich immer wachsam bin und die zunehmende Radikalisierung und Extremismusierung der E-Mail-Attachments bekämpfe!

Remote Communication Interception Software, reloaded [Update]



„Online-Durchsuchung bei Tätern, die nicht übers Internet kommunizieren“- großartige Zwischenüberschrift von Heise. Passt zum Niveau und zu den üblichen Textbausteinen, die seit 1993 zum Thema abgesondert werden.

In den Verhandlungen mit den Grünen zur anstehenden Verschärfung des Polizeigesetzes in dem südlichen Bundesland hatte Strobl bei der Online-Durchsuchung nachgeben müssen. Bei dem Instrument geht es um das heimliche Durchsuchen von Festplatten von Computern, um beispielsweise Terrorpläne zu vereiteln.

Immer diese Festplatten! 2006 ging es um die berüchtigten „Internet-Festplatten, wahlweise auch ohne Internet.

Man kann natürlich auch ersatzweise Harry Potter lesen. Magie ist bei beiden Themen im Spiel. Ceterum censeo: Wie wollt ihr das anstellen, wenn das auszuspähende Objekt die Minimalstandards des sicherheitsbewussten Online-Verhaltens einhält? (Mal abgesehen davon, dass man zuerst die IP-Adresse des Zielrechners kennen müsste.)

Die so genannte Remote Communication Interception Software gibt es auch für Linux?! Und vermutlich funktioniert sie *ohne* physischen Zugriff (USB! USB!) auf den Zielrechner? Das will ich sehen. Bisher hat noch *niemand* etwas darüber gesagt, auch wenn der CCC manchmal geheimnisvoll herumraunte:
Zu den konkreten Methoden macht das Bundeskriminalamt keine Angaben – ‚aus kriminaltaktischen Gründen‘, wie ein Sprecher sagte. Zwar gebe es keine speziell geschulten ‚Online-Durchsucher‘, jedoch Spezialisten, die herangezogen würden. Es

handele sich um Beamte, die ‚versiert auf dem Gebiet' seien. (…) Berichten zufolge haben die Sicherheitsdienste inzwischen auch Spionageprogramme entwickelt, die über das Trojaner-Prinzip hinausgehen. (…) Trojaner nutzen Sicherheitslücken, die nur mit großer Sachkenntnis gestopft werden können. ‚Der Privatnutzer kann sich dagegen kaum schützen', sagt Constanze Kurz, Sprecherin des Chaos Computer Clubs, einer Lobby-Organisation, die für möglichst wenig staatliche Überwachung im Internet eintritt.(FAZ.net, 05.02.2007)

Man kann sich nicht schützen? Das sagt der CCC? Was rauchen die da? Ich bin auch versiert, gefragt hat man mich aber noch nicht.

Jaja. Phishing E-Mails im Behördenauftrag?! Da kann Netzpolitik.org gern den Vertrag mit FinFisher veröffentlichen. Ich halte das für höheren volksverdummenden Blödsinn.

„Man könnte von ‚Durchsuchungssoftware' sprechen; bei bei Software für die Quellen-TKÜ von Remote Communication Interception Software (RCIS). De Facto ist es aber nichts anderes als Schadsoftware, die das Rechnersystem infiltriert und seine Funktion manipuliert."

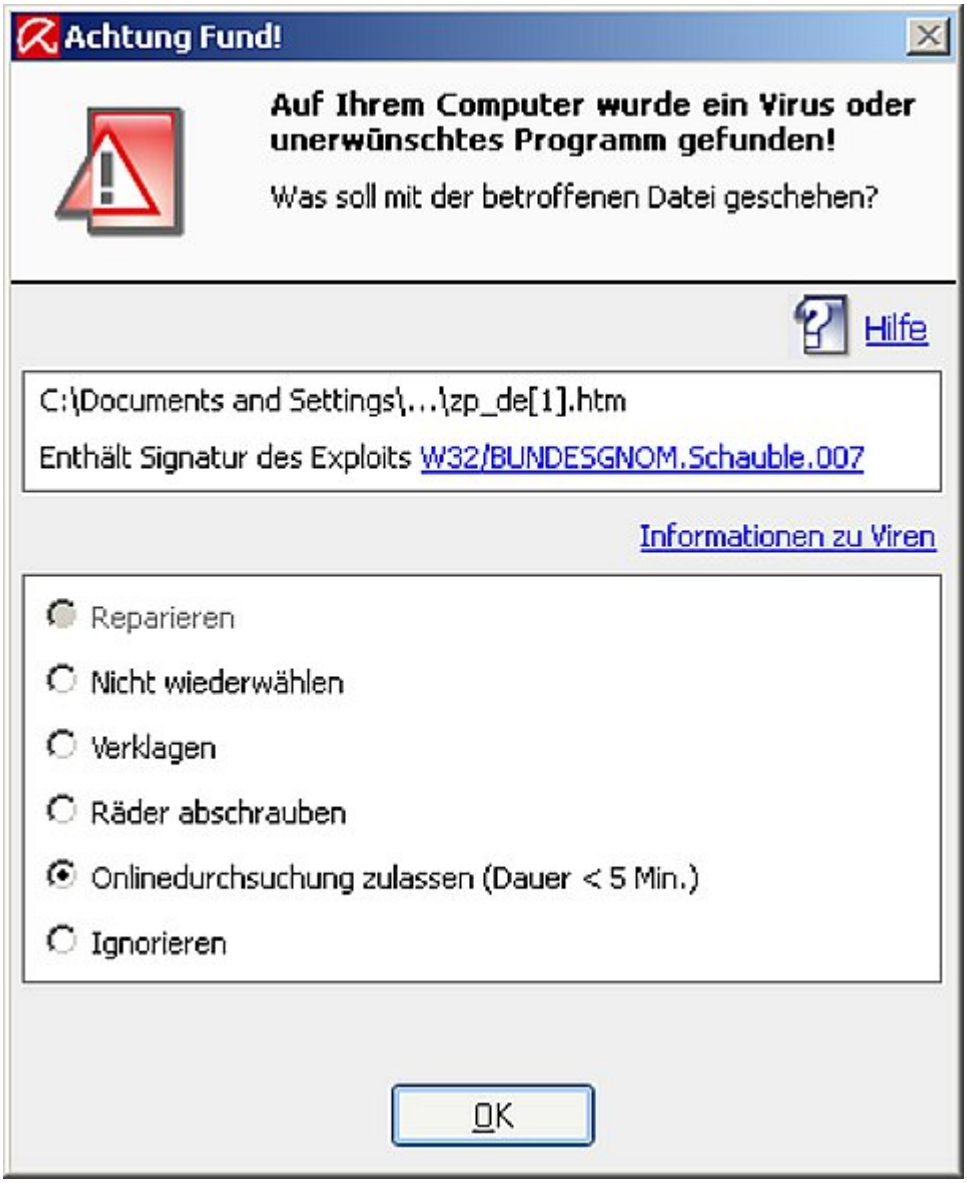
Wie? Wie? Wie? Der Kaiser ist nackt! De facto ist das ein Meme.

Legendär immer noch Annette Ramelsberger (Süddeutsche, 07.12.2006): „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."

Nein, das war mir bisher nicht klar, und wenn ich ehrlich sein soll, wurde es auch seitdem nicht klarer. Alle schreiben voneinander ab. Fakten werden sowieso überschätzt.

[Update] Ich habe *nie* behauptet, dass man keine Mal- oder Spionagesoftware auf fremden Rechnern installieren könne. Es funktioniert aber *nicht* so, wie sich das fast alle vorstellen: Von fern und weil irgendjemand das so will. Man braucht a) mindestens den (physikalischen) Zugriff auf den Zielrechner (um z.B. einen Keylogger oder per USB etwas aufspielen zu können) und b) muss sich der Nutzer selten dämlich anstellen (leider ist das wohl eher die Regel als die Ausnahme). Alles andere ist Humbug.

Online durchsuchen



Heise: „Wie Geheimdienste Cyberattacken durchführen – Ein Ex-FBI-Agent spricht über staatliche und nichtstaatliche Cyberangriffe, deren Zuschreibung und den Sony-Pictures-Hack.“

Komisch. Der spricht gar nicht über das Von-fern-auf-fremde-Rechner-zugreifen-und-online-durchsuchen!? Woran kann das nur liegen?

Online-Durchsuchung, revisited

Reporter ohne Grenzen (ROG) warnt vor Plänen des Bundesinnenministeriums, wonach deutsche Geheimdienste Medien im In- und Ausland künftig digital ausspionieren könnten. Einem Referentenentwurf zufolge sollen deutsche Inlands- und Auslandsgeheimdienste Server, Computer und Smartphones von Verlagen, Rundfunksendern sowie freiberuflichen

Journalistinnen und Journalisten hacken dürfen.

Dann hackt mal schön. Das ist doch wieder ein großer Schmarrn. Aber unsere „Online"-Journalisten werden das alle nachbeten.

Ich schrieb im Oktober 2009: Der Kaiser ist bekanntlich nackt und Online-Durchsuchungen hat es nie gegeben und wird es nie geben. Jedenfalls nicht so, wie sie der Volksmund und Klein Wolfgang verstehen: Da sitzt ein Ermittler irgendwo in einer Behörde und sucht und findet die IP-Adresse des Computers eines Verdächtigen, spielt dem dann „online" und unbemerkt ein Spionageprogramm auf und liest dann mit? Vergesst es. Keep on dreaming. Die real gar nicht existierende Online-Durchsuchung ist der einflussreichste Medien-Hoax, den ich kenne, ein hübsches urbanes Märchen, das vom Wünschen und Wollen ahnungsloser Internet-Ausdrucker und noch mehr vom ahnungslosen Geraune der Medien am Leben erhalten wird. Nicht *ich* muss beweisen, dass es bisher *keine* „Online-Durchsuchung gab, sondern diejenigem, die behaupten, so etwas würde gemacht, müssen Fakten, Fakten, Fakten liefern – wer, wie und

womit.

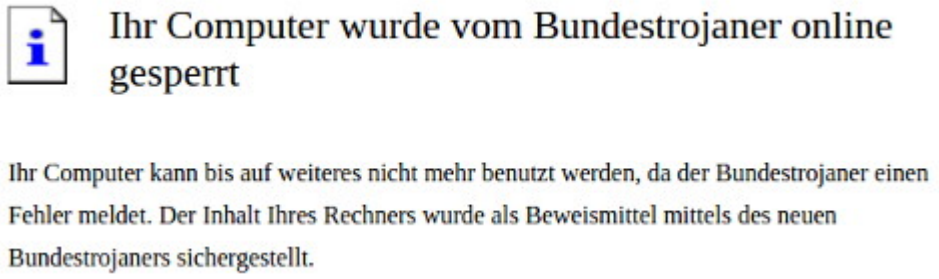
Wenn der Nutzer sich total dämlich anstellt, dann ginge es – und nur mit physischem Zugriff auf den Rechner. (Und welchen? Hackt ihr auch meinen Router und mein Intranet?)

Und kommt mir jetzt nicht mit FinFisher: *…Spionageprogramme, die bislang unbekannte Sicherheitslücken von Smartphones und Computern ausnutzen, um sämtliche Aktivitäten der Nutzer auszuspionieren: Mail-Korrespondenz, Adressbücher, Chat-Programme, Telefonanrufe – sie schalten sogar Kamera und Mikrofon nach Belieben ein, ohne dass der Nutzer dies merkt.*

Ach ja? PGP ist jetzt auch „gehackt“? Meine Mail-Korrespondenz, falls unverschlüsselt, wird doch schon durch die SINA-Box mitprotokolliert. Wozu jetzt noch mal draufsatteln? Meine Kameras schaltet niemand ein. Nur damit ihr’s wisst.

[Update] Fefe hat was über die Cyberpläne vom Cyberheimathorst.

Bitte durchsuchen Sie mein Gerät!



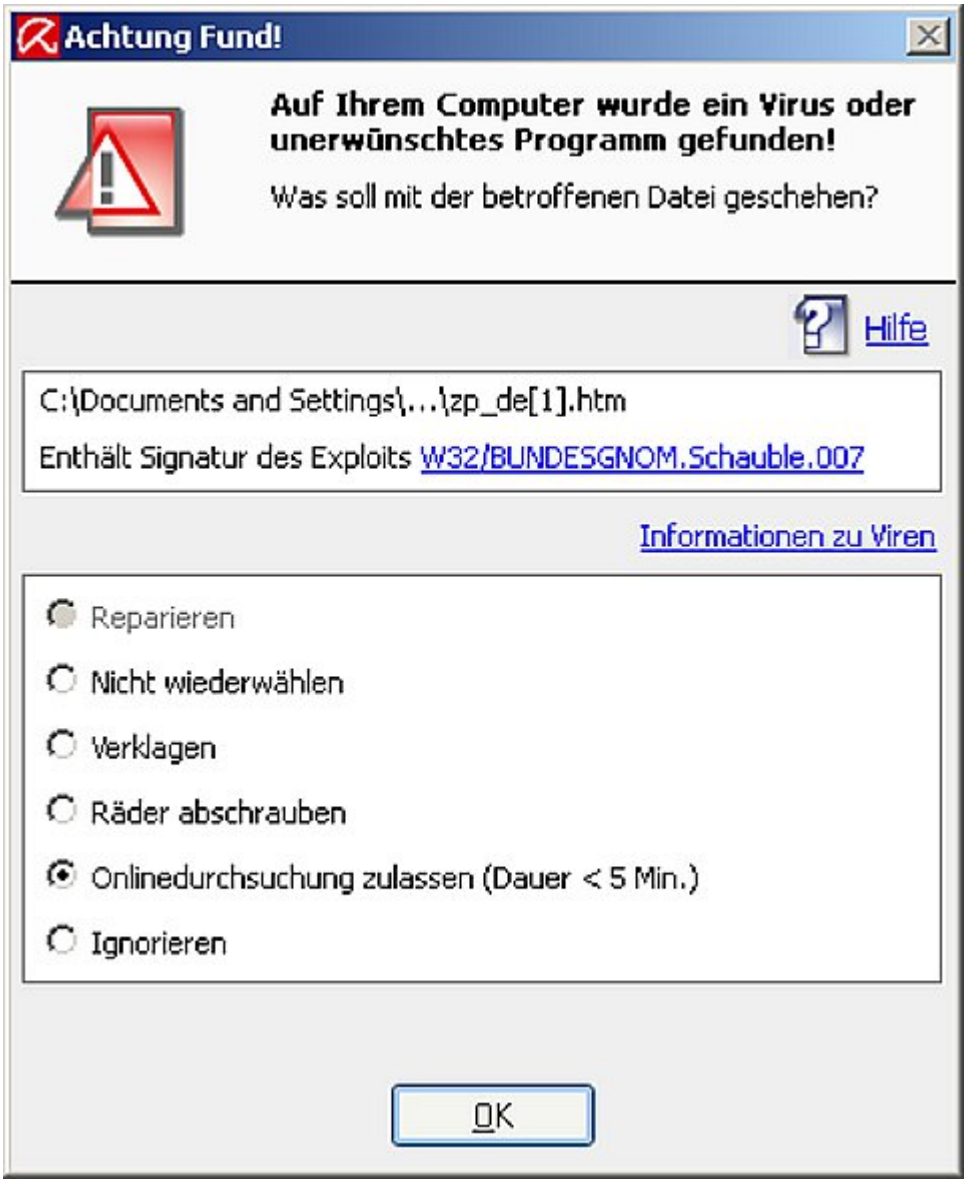
Ich habe eine kleine und unmaßgebliche Frage, die bekanntlich

niemanden interessiert: *Wie will man Computer „heimlich“ durchsuchen?*

„…ist es nötig, die Geräte der Betroffenen mit Schadsoftware in Form sogenannter Staatstrojaner zu infizieren.“

Wie? Wie? Wie?

Bundestrojanisches Pferd oder: Technisch dürfte es dabei Probleme geben



Heise: „Generell bleibt es dabei, dass Strafverfolger die Möglichkeit erhalten, Internet-Telefonate etwa per Skype und die Kommunikation über Messenger wie WhatsApp, Signal, Telegram oder Threema zu überwachen.“

Ach ja? Signal kann man also überwachen? Wie denn? Hat sich Edward Snowden geirrt? Oder ist das nur eine Verschwörungstheorie? Ich kriege schlechte Laune, wenn ich diesen Schwachfug lese.

„Mit dem derzeitigen Bundestrojaner, den IT-Experten vom BKA innerhalb von drei Jahren entwickelt hatten, können Messenger-Programme nicht abgehört werden. Berichten zufolge ist damit nur eine Quellen-TKÜ von Voice over IP (VoIP) über Skype auf

Desktop-Rechnern mit Windows möglich.“

Sonst nix. Was ist mit Skype für Linux? Fragen über Fragen. Und niemand macht sich die Mühe, das Publikum aufzukären. Nur geheimnisvolles Herumgeraune.

Berichten zufolge war schon vieles möglich. Wahr wird es dadurch nicht. Warum übernimmt der Autor Stefan Kremp die Terminologie derjenigen, die auf Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme missachten?

Wenn man sich ältere Berichte zum Thema anschaut: Wir kommt der Mist auf einen Rechner? Ja? Ich höre?!

Sind eigentlich alle irre? Soll das Journalismus sein?

Der Kaiser ist nackt!

```
.text:1000D4F7     loc_1000D4F7:                           ; CODE XREF: _0zapf-
tis_download_store_EXE+BBj
.text:1000D4F7 430       mov     eax, tmp_file_index
.text:1000D4FC 430       lea     edx, [esp+430h+FileName]
.text:1000D500 430       mov     ecx, eax
.text:1000D502 430       inc     eax
.text:1000D503 430       push    ecx
.text:1000D504 434       lea     ecx, [esp+434h+Buffer]
.text:1000D50B 434       push    ecx
.text:1000D50C 438       push    offset aSTmp08x_exe     ; "%s-tmp%08x-.exe"
.text:1000D511 43C       push    edx                     ; Destination Buffer <-
zu eng :-)
.text:1000D512 440       mov     tmp_file_index, eax
.text:1000D517 440       call    _sprintf
.text:1000D517
.text:1000D51C 440       lea     eax, [esp+440h+FileName]
.text:1000D520 440       push    eax                     ; lpFileName
.text:1000D521 444       call    _0zapftis_create_file
```

Heise meldet, dass die Bundesregierung behaupte, die Software zur Online-Durchsuchung sei einsatzbereit. Das ist aber nicht neu. Wie man der von mir erstellten Chronik der Medienberichte über die so genannte „Online“-Durchsuchung sehen kann, soll das schon vor acht Jahren möglich gewesen sein. Der *Tagesspiegel* titelte am 08.12.2006: „Die Ermittler surfen

[sic!!] mit“:

“Das System der sogenannten „Online-Durchsuchung“ sei bereits in diesem Jahr mehrfach angewandt worden und sei Teil des 132 Millionen Euro schweren Sonderprogramms zur Stärkung der inneren Sicherheit. Die Ermittler sollen sich dabei auf richterliche Anordnung unbemerkt via Internet in die Computer von Privatpersonen einloggen können, gegen die ein Strafverfahren läuft.

(Viele Links funktionieren nicht mehr, aber anhand des genauen Titels kann man sie noch finden, teilweise über archive.org)

Manchmal fühle ich mich wie allein gelassen unter lauter Irren. Was nützt mir ein derartiger Bericht wie der aktuelle bei Heise, wenn niemand fragt, wie die Überwachungssoftware auf den Rechner des „Zielobjekts“ gekommen ist? Das ist doch – jenseits der empörten Attitude – eine der wichtigsten Fragen überhaupt? Es braucht doch mindestens den physischen Zugriff (und dann müssen bestimmte Voraussetzungen gegeben sein), oder das „Opfer“ muss Malware wie Skype schon installiert haben.

Es geht aber mitnichten so, dass jemand „von fern“ irgendwas installiert. Außerdem müsste man ja auch die IP-Adresse wissen und eventuell noch den Router austricksen. (Jetzt fange hier niemand davon an, etwas von „Mail-Attachments“ zu faseln oder von „Websites, auf die man „gelockt“ werden soll. Ich kann es nicht mehr hören.) Christian Rath schrieb in der *taz* am 11.12.2006:

Denkbar sind verschiedene Wege. So kann die Polizei versuchen, ein „Trojanisches Pferd“ (kurz Trojaner) auf den Computer des Betroffenen zu schleusen. Ein Trojaner ist ein Programm, das heimlich Aktionen auf dem Computer ausführt, ohne dass der Benutzer dies bemerkt. Der Trojaner kann zum Beispiel als Anhang mit einer getarnten E-Mail auf den Rechner gelangen. Vorsichtige Computernutzer öffnen aber keine unbekannten Anhänge oder schützen ihren Computer mittels Firewall oder

Filter schon vor dem Zugang solcher Spionagesoftware.

Soll ich das jetzt noch kommentieren?

Am 08.10.2011 berichtete Heise:
Dem Chaos Computer Club (CCC) ist nach eigenen Angaben die staatliche Spionagesoftware zugespielt worden, die allgemein unter dem Begriff „Bundestrojaner“ oder in bundeslandspezifischen Versionen beispielsweise auch als „Bayerntrojaner“ bekannt wurde.

In der Analyse des CCC (LESEN!) heisst es: „Die Malware bestand aus einer Windows-DLL ohne exportierte Routinen.“ Ach so. Dann gibt es den „Trojaner“ nicht für Linux? Das ist aber schade.

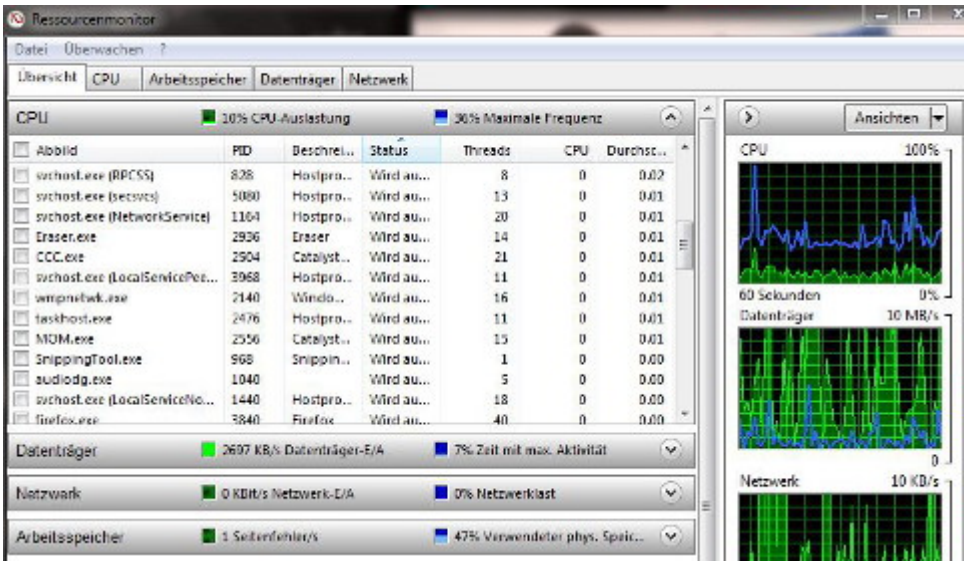
Wir haben keine Erkenntnisse über das Verfahren, wie die Schadsoftware auf dem Zielrechner installiert wurde. Eine naheliegende Vermutung ist, daß die Angreifer dafür physischen Zugriff auf den Rechner hatten. Andere mögliche Verfahren wären ähnliche Angriffe, wie sie von anderer Malware benutzt werden, also E-Mail-Attachments oder Drive-By-Downloads von Webseiten. Es gibt auch kommerzielle Anbieter von sogenannten Infection Proxies, die genau diese Installation für Behörden vornehmen

E-Mail-Attachments oder Drive-By-Downloads von Webseiten. Und so etwas schreibt der Chaos Computer Club?! OMG.

Ceterum censeo: Der Kaiser ist nackt!

Die Online-Durchsuchung live

beobachten

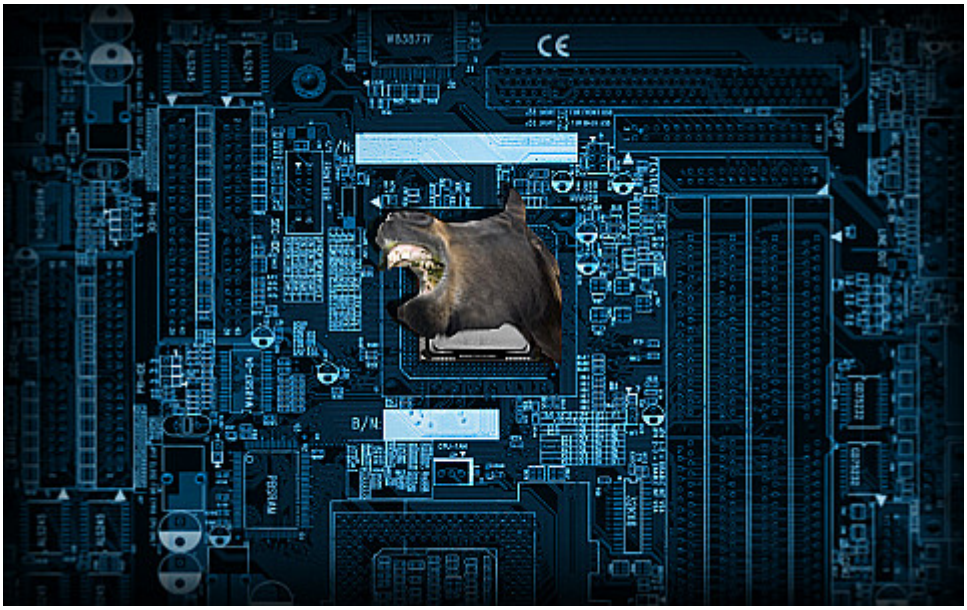


Kleiner Tipp am Rande für Windows(7)-Nutzer: Unter *Start* | *alle Programme* | *Zubehör* | *Systemprogramme* | *Ressourcenmonitor*
kann man sich alle laufenden Prozesse des Rechners anzeigen lassen.

Fall jemand eine unverschlüsselte E-Mail bekommen hat mit dem Betreff „Wir tun alles für Ihre Sicherheit!“ und das Attachment angeklickt hat und
die Frage *bundestrojaner_skype.exe is an unknown application – install anyway?* mit „ja“ beantwortet, kann dann live beobachten, was geschieht. Für Unix gibt es übrigens z.B. Monit.

Burks warnt vor einer neuen

Variante von digitaler Erpressung bei der Internetnutzung



Ihr Computer wurde vom Bundestrojaner online gesperrt.

Ihr Computer kann bis auf weiteres nicht mehr benutzt werden, da der Bundestrojaner einen Fehler meldet. Der Inhalt Ihres Rechners wurde als Beweismittel mittels des neuen Bundestrojaners sichergestellt.

Versuchen Sie Folgendes:

Sollten Sie noch eine Beta-Version des Bundestrojaners ohne automatische Updates installiert haben, installieren Sie die aktuellste Software-Version über die Update-Funktion in der Bundestrojaner-Software. (Sie finden diese in der Lautstärkeregelung unter Optionen/Aufnahme über den Eintrag BundesMIC). In Zukunft werden die Updates dann unbemerkt von Ihnen durchgeführt, was einen großen Vorteil in der Bedienbarkeit darstellt.

Stellen Sie sicher, dass Ihr Computer permanent online ist!

Auch Ihre Computer-Software (z. B. Microsoft Office, Notepad, Outlook, …) ist nur bedienbar, wenn eine ausfallsichere Online-Verbindung zum Bundestrojaner-Server garantiert ist. Der Bundestrojaner dient nur zu Ihrer eigenen Sicherheit.

Sollten Sie versucht haben, eine E-Mail zu versenden, überprüfen Sie die Empfänger-Adresse(n). Es sind nur validierte Empfänger-Adressen mit Top-Level-Domains aus dem deutschsprachigen Raum zugelassen, die zusätzlich auf der Bundestrojaner-Homepage als unproblematisch eingestuft wurden. Der Empfang von E-Mails ist zu Ihrer eigenen Sicherheit ebenfalls nur für vom Bundesstaat authentifizierte E-Mail-Adressen möglich.

Möglicherweise hat der Bundestrojaner eine Hardware-Änderung festgestellt, die noch nicht von der TÜP (Trojanischen Überwachungs-Polizei) abgenommen wurden. Vereinbaren Sie einen Termin mit Ihrem persönlichen TÜP-Sachbearbeiter und lassen Sie sich eine neue gültige Hardware-Plakette für Ihren Computer ausstellen. Ihr persönlicher TÜP-Sachbearbeiter wurde soeben informiert und wird sich mit Ihnen schnellstmöglich telefonisch in Verbindung setzen.

In brisanten Fällen – z. B. bei mehr oder weniger dringendem Tatverdacht – kann es vorkommen, dass die Bundestrojaner-Software den Zugriff auf das Internet und/oder Ihre Software gänzlich verweigert. Wenden Sie sich in diesem Fall an Ihre nächstliegende Polizeidienststelle. Sie benötigen hierbei lediglich Ihren Personalausweis mitzunehmen – alle weiteren Daten sind einfach über Ihre Personalausweis-Nummer abrufbar.

Sollten Sie nicht innerhalb der nächsten 24 Stunden erscheinen (können), werden Sie von uns abgeholt.

Eventuell tritt ein Port-Konflikt auf. Ändern Sie im Browser den Port auf einen anderen Wert als 80, da dieser vollständig für die Kommunikation des Bundestrojaners reserviert ist. Als ein im unteren Zahlenbereich liegender Wert reicht Port 80

meist eh nicht für große Datenübertragungen aus. Wählen Sie lieber eine vier- oder besser noch fünfstellige Zahl.

In sehr seltenen Fällen führt die Eingabe des Wortes ‚Bundestrojaner' in eine Suchmaschine dazu, dass Ihr Computer sofort gesperrt wird. Dieser Bug wird in der kommenden Version behoben werden.

Sie haben versucht, eine als gefährdet eingestufte Homepage aufzurufen (zu erkennen an dem 's' in ‚https'). Dieser Vorgang übermittelt verschlüsselte Daten, welche eine große Gefahr für die Staatssicherheit darstellen. Rufen Sie daher nur Seiten auf, die mit ‚http' beginnen – nur hier ist sichergestellt, dass die übertragenen Daten zu Ihrer Sicherheit vom Bundestrojaner überprüft werden können.

Sollten Sie nicht sicher sein, ob Sie den Bundestrojaner überhaupt auf Ihrem Rechner installiert haben – er läuft.

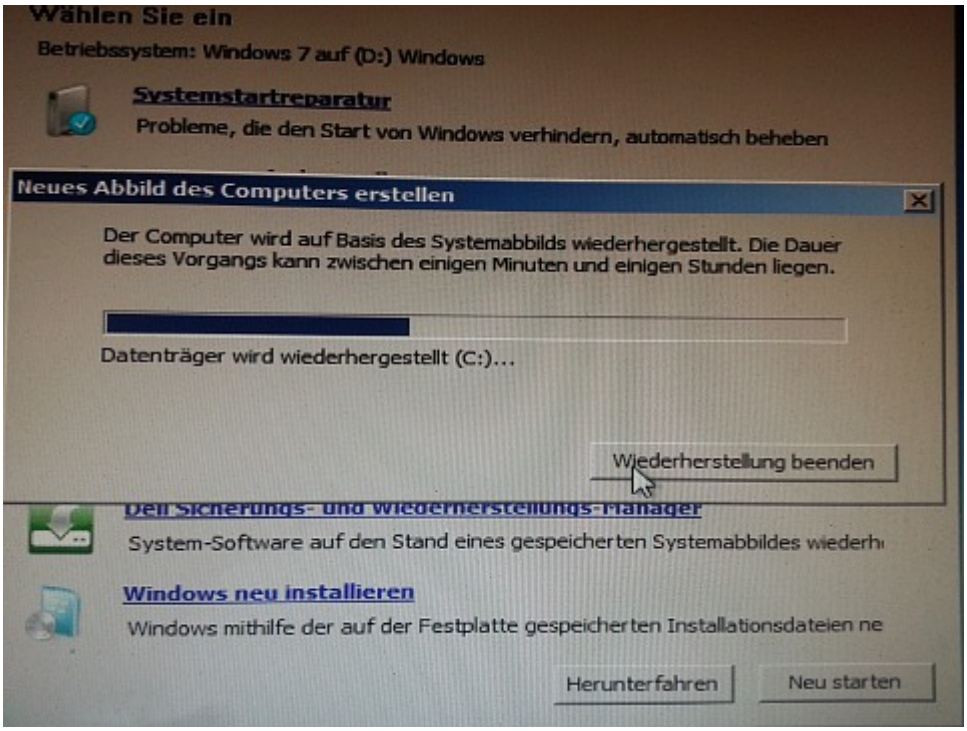
HTTP 909 – Bundestrojaner-Online-Durchsuchung

Seien Sie vorsichtig!

Die Berliner Polizei rät: „Bei unbekannten Absendern niemals die Anhänge der Mails öffnen! Seien Sie vorsichtig, auch wenn Ihnen die Mail grundsätzlich seriös vorkommt!"

Und was ist jetzt mit den Verschwörungstheorien, der real gar nicht existierende „Bundestrojaner" werde per Mail verschickt?

Regedit.exe



Vermutlich werden jetzt die wohlwollenden Stammleserinnen und die geneigten Stammleser hämisch grinsen. Wie allgemein bekannt, besitze ich zwei Windows- und zwei Linux-Rechner. Den Windows-Rechner, den ich meistens nutze, habe ich gestern zerschossen.

Man sollte eben nie, wenn man unkonzentriert ist und mehrere Sachen gleichzeitig tut, mal so eben nebenbei in der regedit.exe herumfummeln. Ein Chirurg entfernt auch nicht ein paar Organe eines Kunden, während er mit der linken Hand am Smartphone daddelt und gleichzeitig wahlweise mit der Narkoseärztin flirtet oder ein Käsebrot isst.

Ich bin ja nicht ganz unerfahren, um nicht zu sagen: ich bin ein Geek, und habe eine dreistellige Mitgliedsnummer aller deutschen Internet-Nutzer, aber wenn selbst der abgesicherte Modus in verschiedenen Versionen nicht dazu führt, dass man sich überhaupt anmelden kann – die Anmeldemaske von Windows 7 erschien, aber keine Nutzerkonten – und noch ein paar eklige Dinge undsoweiter undsofort und wenn nach zwei Stunden

inständigen Fluchens alles vergebens ist, dann wird es Zeit für die Hardcore-Maßnahmen, die man gemeinhin „plattmachen und Backup draufspielen“ nennt. Wo war noch mal das „Medium“ zur Systemwiederherstellung aka *rescue disk*? Zähneknirsch. Nicht vorhanden. (zum Glück hat einer der Laptops auch Windows 7).

Ein mahnendes Wort zu Vorgeschichte. Ich habe noch nie irgendwelche nutzlosen Placebos wie Virenscanner und anderen Regenzauber benutzt. Brauche ich nicht. Ich verhalte mich vernünftig – wie ungefähr ein Promille aller Internet-NutzerInnen. Es gibt keine – in Worten: *keine* Möglichkeit, mir Viren, Würmer, trojanische Pferde, Keylogger, real gar nicht existierende „Bundestrojaner“, Stuxxe und Flame und andere hässliche Programme unterzujubeln. Nein, es ist noch nicht einmal ein Risiko vorhanden. Alles verboten, und auf meinem Rechner geschieht nichts und installiert sich auch nichts, was ich nicht vorher erlaubt hätte. So wäre das eigentlich normal, auch wenn die deutsche Journaille, selbst ernannte „Sicherheits-Experten“ und Hochstapler aller Couleur mit penetranter Belehrungsresistenz den Kauf von „Virenscannern“ ankurbeln. (Und jetzt zu etwas fast ganz Anderem: oder die Pappnasen von der Geschäftstelle des DJV-Bundesverbands mich zwingen wollen, ihren „Newsletter“ in HTML zu lesen, mich also zum Dummen, Risikobehafteten, Bescheuerten und DAU-Mäßigem erziehen wollen: Nein, nein, nein, ihr könnt mich mal kreuzweise.)

Kurz vor der Party zu meinem Geburtstag fiel mir ein, dass es eine Fummelei ersten, zweiten und dritten Grades gewesen wäre, die Kabel meine Lautsprecheranlage an den Linux-Rechner anzuschließen. Außerdem wollte ich ohnehin ein paar Youtube-Videos meiner Sammlung einverleiben – auch solche, die die GEMA meint, mir verbieten zu können und die ich mit Proxtube entsperre.

Chip Online rät zu „Free YouTube Download“ (*„Hinweis: Während der Installation versucht das Setup einige Einstellungen am Browser zu verändern. Bevor Sie auf „Weiter“ klicken, sollten*

Sie daher alle gesetzten Häkchen abwählen.“)

Har har har. Das ist eine Malware, weil eine Browser-Toolbar installiert wird, *obwohl* ich *alles* während der Installation disabled/verboten/untersagt/nicht angekreuzt hatte. Wie kann eine „seriöse“ Website nur so einen abgefuckten Scheiss empfehlen?

Ich habe jedenfalls eine gute Stunde gebraucht, um die Malware rückstandslos zu entsorgen – sogar mit der Systemsteuerung funktionierte das nicht. Auch nach einer Neu-Installation von Firefox erschien die Schadsoftware wieder. Und jetzt, sehr verehrte Leserin und verehrter Leser, habt ihr mein Motiv, in der regedit.exe herumzufummeln, weil ich eh schon dabei war nachzusehen, ob eventuell noch gänzlich tote Leichenteile der Malware übriggeblieben waren.

Leider war mein Backup schon ziemlich alt, und ich habe fast den ganzen Tag gebraucht, um alles auf den aktuellen Stand zu bringen. So etwas wird mir nicht nochmal passieren. Und jetzt kann ich gleich Thunderbird komplett in einen Truecrpt-Container sperren, was ich eh schon lange wollte.

Günter Wallraff et al

Auf Ruhrbarone.de steht ein Artikel über die Journalisten-Legende Günter Wallraff und dessen Umgang mit „Mitarbeitern“ und Quellen: „Mobbing à la Wallraff oder ‚…bis bald, Dein Günter‘.“

Sehr interessant auch dieser Hinweis: „Wallraffs Anwalt steht übrigens nach Presseberichten als ‚Sprecher‘ in Diensten der Firma ‚DigiTask‘. ‚DigiTask‘? Ja, genau. Das ist ein Spezialunternehmen, das vor einiger Zeit durch den sogenannten

‚Bundestrojaner' Schlagzeilen machte – eine Virensoftware [*Unfug. Burks*], die von BND und anderen Geheimdiensten dieser Welt genutzt wird, um heimlich Computer auszuspähen."

Ja wo nutzen Sie denn? Mein Verhältnis zu Günter Wallraff habe ich übrigens schon am 12.12.2004 auf meinem Blog spiggel.de beschrieben.

Bekannte technische Enten-Parameter

Der Bericht des Bundesdatenschutzbeauftragten zum Einsatz staatlicher Überwachungssoftware – die oft falsch „Bundestrojaner" genannt wird -, ist geleakt worden.

Einbringungsphase: Die Einbringung der Überwachungssoftware (Capture-Unit) erfolge in Abstimmung zwischen KI 25 und dem jeweiligen Bedarfsträger. Bei der Einbringung wird i.d.R. ein Ladeprogramm auf dem Zielsystem zur Ausführung gebracht, durch welches die eigentliche Überwachungssoftware installiert wird. Bevor mit der eigentlichen Maßnahme begonnen wird, muss zunächst das Zielsystem anhand bekannter technischer Parameter verifiziert werden. Jede Einbringung steht unter dem Entscheidungsvorbehalt der Amts-leitung. Die Software werde entweder mittels physischem Zugriff auf das Ziel-system oder auf andere Weise eingebracht. Auf die Darstellung der Einzelheiten wird auf Wunsch des BKA hier verzichtet.

Quod erat demonstrandum. Das Wesentliche fehlt also. „Bekannte technischer Parameter" – meinen die im Ernst die IP-Adresse oder die MAC-Adresse oder was?

Ceterum censeo: „Online" kann man keine Spionagesoftware ohne

Wissen und Erlaubnis des „Opfers“ installieren – nur über einen physischen Zugriff (und das nur, wenn der Besitzer des Rechners eine Pappnase ist) oder „en passant“ über eine real schon installierte Software wie Skype, die das Abhören ohnehin gestattet.

Warum ist das so schwer zu verstehen?