Was ist und zu welchem Ende betreiben wir Social Engineering?

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“.

Panta rhei

Mein Avatar in Second Life denkt gerade über etwas nach. Es ist heiß, weil Wüste, und windig, weil Sandsturm.

Eigene Sim, alles selbst gebaut (Screenshot von heute).

Diesen Beitrag bitte nicht lesen. Er ist nur für mich selbst. Das Blog dient auch als digitales Tagebuch, immerhin schon seit dem 01.03.2003. Wenn ich also in alten Beiträgen herum“blättere“, fällt mir so Einiges wieder ein. Was ist seitdem nicht alles passiert! Und die virtuellen Ereignisse behalte ich genauso gut.

Ich schrieb am 27.06.2008: „Nur die eingefleischten Stammleser (eine Hand voll?) werden sich für meine Traktate über Second Life interessieren. (Wer das langweilig findet: Geht doch woanders hin!).“

Nach meiner Geburt in Secondlife am 25.01.2007 habe ich zunächst nur gechattet oder Ausstellungen organisiert oder bin

mit virtuellen Fahrzeugen herumgebrettert.

Screenshot vom November 2008 – mein Avatar bei der investigativen Recherche (Social Engineering).

Gosh – the memories! Einige Qualitätsmedien waren 2008 noch in Secondlife – wie etwa die BBC. Es gab Misswahlen, über die BILD berichtete, und es gab schon die ersten Sexcam-Angebote. Ich flog mit steampunkigen Fluggeräten herum und amüsierte mich.

Der erste virtuelle Bankencrash ließ nicht lange warten. Ich verdiente Geld mit Artikeln darüber. (Ich behaupte, dass ich der einzige Mensch auf der Welt bin, der einen Screenshot von der Wirecard Bank in Secondlife hat.

Ähm. Räusper. Das wird schnell langweilig, auch der Pixelsex, den damals, als die Avatare nur so vom virtuellen Himmel regneten, weil große Medien berichteten, jeder ausprobiert hat. Ich aber beschloss, dort irgendwie Geld zu verdienen. Ich hatte gerade real geheiratet und meine Frau studierte.

Also kaufte ich von einem Freund (hallo, M.!) einen virtuellen Puff (vgl. Screenshot oben), mit dem ich ein paar Monate Lindendollar einnahm (die man wieder in reales Geld umtauschen kann). Wie? Ich lebte vom virtuellen Verkauf virtueller Penisse und Vaginae, weil der Avatar ab Werk so etwas nicht hat, aber sich in einem virtuellen Puff irgendwie unvollständig vorkommt. Die Geschlechtsteile hingen kundenfreundlich an der Wand zum Kauf. („Welche Berufe haben Sie bisher ausgeübt?“ „Pimmelverkäufer“. „Wir melden uns“.) Das hat jetzt hoffentlich niemand gelesen.

Oh, sich sehe gerade, dass Trinity offenbar den Abgang gemacht hat – das schon vor zwei Jahren. Mit Ansage: Sex war dort verboten. Ich hatte damals einen Artikel geschrieben. Auch Exit Reality ist offline. Witzig, dass ich das als Avatar ausprobiert habe. Noch jemand außer mir? Hallo?

Bevor ich das virtuelle Rollenspiel und Gor entdeckte, saß ich am liebsten in virtuellen Raumschiffen, die ich selbst steuern konnte – wie hier im November 2008. Das besitze ich noch – und es fliegt noch immer. Oder ich reiste stilvoll zum Mond. (Das Tannhauser Gate vom Oktober 2017 – also neun Jahre nach meinem ersten virtuellen Mondflug – ist aber nicht zu toppen.)

Im Oktober 2008 geriet ich zufällig in eine merkwürdige Veranstaltung. Nackte Frauen mit Halsbändern auf Knien zum Verkauf. WTF? (Das musste ich mit einem Kirchenbesuch und mit einem Artikel im Rheinischen Merkur und auf Telepolis kompensieren.)

Die spätkarolingische

Georgskirche in Second Life 2009

Am 23.12.2008 war es dann soweit: „Burks Goes Gor“. Fantasy-Rollenspiel also. Zu Anfang schrieb ich viel dummes Zeug, weil ich keine Ahnung und keinen Plan hatte. Auch *inworld* muss man mich für total blöd gehalten haben, weil ich dort keinen blassen Schimmer von den Spielregeln hatte.

„Eine der größten Communities in Second Life und gleichzeitig eine, die sich hermetisch von gewöhnlichen Nutzern abschottet, sind die „Goreaner„. In „Gor“ findet ein kompliziertes und oft sexuell konnotiertes Rollenspiel statt: „Gor, the Counter-Earth, is the alternate-world setting for John Norman’s Chronicles of Gor, a series of twenty six novels that combine philosophy, erotica and science fiction.“ Wer mehr Informationen will, lese zum Beispiel den Wikipedia-Eintrag über Kajira („The phrase „la kajira“ is said to mean „I am a slave-girl“ in the Gorean language“) oder über „Male domination„. („Male dominance, or maledom, refers to BDSM activities where the dominant partner is male.“)

Es handelt sich also auf den ersten Blick um ein pseudo-mittelalterliches Fantasy-Rollenspiel anhand vorgegebener Trivialromane (deren Inhalt als bekannt vorausgesetzt wird, um überhaupt teilnehmen zu können). “

Ende 2008 traute ich mich zum ersten Mal, die ortsüblichen virtuellen Tierchen zu reiten.

Nach einer mehrmonatigen Pause aus privaten Gründen (u.a. der Scheidung) ging es im November 2009 weiter.

Vor zehn Jahren hatte ich zum ersten Mal eine eigene Sim – Tancred's Landing genannt. Die gibt es heute immer noch, sieht aber ganz anders aus – und ich bin da nie.

Februar 2010

Dann fingen andere Leute an, mich mit dem Bauen von Sims zu

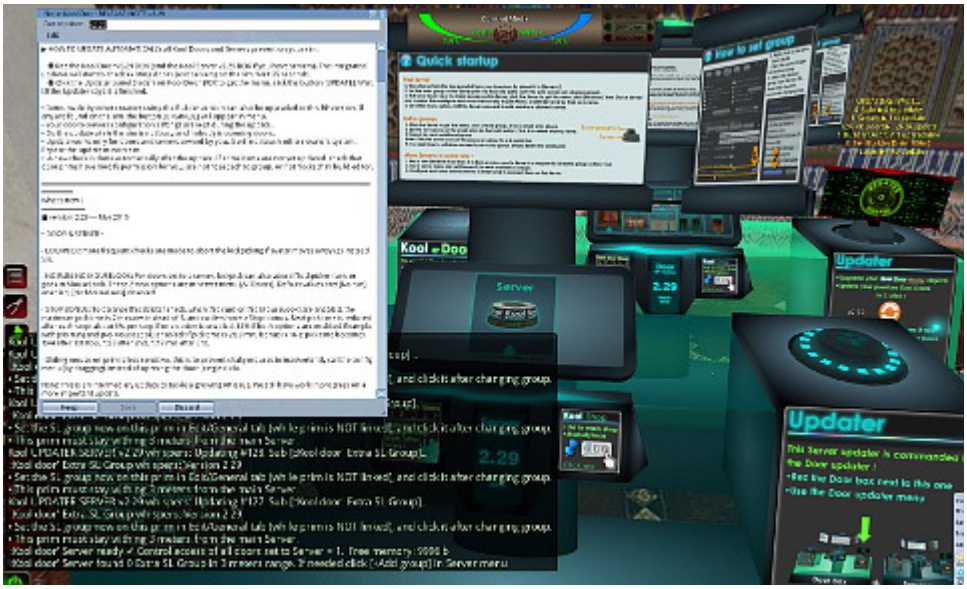
beautragen – für rund 100-300 Dollar macht man das, aber der Stundenlohn ist eigentlich lächerlich (und noch eine, Oktober 2017).

Dadurch wird man aber bekannt. Und schon gab es die ersten Filme über das, was man gebaut hat… Wie ein Insekt im Bernstein noch zu sehen, obwohl alles schon im virtuellen Nirwana ist und die Frau, die den Film produziert hat, im realen Leben gestorben ist.

Panta rhei. Genauso wie die virtuelle Steinzeit oder der Zwinger.

Jemand hatte sich im Februar 2012 die Mühe gemacht und von meinem Avatar in Gor (Second Life) eine Art Bleistiftzeichnung angefertigt;. Damals war ich gerade Administrator einer Sim geworden und gehörte damit zur virtuell herrschenden Klasse. Auch die Tiere wurden immer dicker.

Die schönste Sim, die ich jemals gebaut habe (es waren sogar drei), war Kasra. Auch die gibt es nur noch bei Youtube.



So sieht es aus, wenn man eine Sim in Secondlife verwaltet und die Türen (hier: 131) ein Update bekommen (müssen)…

Das kann einem schon den Schweiß auf die Stirn treiben. (31.03.2016)

Was habe ich nicht alles für virtuelle Dramen erlebt! Leute, die sich im Chat verfluchen und pausenlos beschimpfen. Admins, die Avatare gleich reihenweise von Sims verbannen. Zahlreiche Mordversuche und Attentate auf meine Avatar. (Gut, ich habe auch ein halbes Dutzend Leute virtuell umbringen lassen Meine angeheuerten Killer waren immer erfolgreich.) Überfälle auf und Belagerung von Städten, nur weil mein Avatar sich dort aufhielt. Mehrstündige heftige Schlachten, bis sich einem der Zeigefinger vom Mausklicken verkrampfte. Irgendwie schmeichelt es einem auch, wenn die virtuelle Präsenz andere Leute so aufregt.

Ich muss jetzt Aufhören mit dem „Herumblättern“ und Stöbern. Ich habe auch noch fast 5000 Screenshots aus Second Life seit 2007… Nein, die poste ich hier nicht.

Die virtuellen Karawanenführer können sich virtuell nicht über den virtuellen Weg zu einer virtuellen Oase einigen. (Mai 2023)

Pralle Blondinen in deiner Nachbarschaft

Die USA behaupten, sie hätten Computer des Iran stillgelegt „mit denen Raketen und Marschflugkörper gesteuert werden“. Das berichtet Heise und beruft sich auf die Washington Post.

Ich glaube nichts. Es gibt keine verlässlichen unabhängigen Quellen, und das Pentagon betreibt Propaganda.

„Seit Jahren würden iranische Agenten erfolgreich ausländische Flugdrohnen und wohl auch Schiffe hacken. Dazu komme eine große Social-Hacking-Kampagne: Angebliche attraktive Frauen würden online „einsame Seeleute“ der US-Kriegsmarine suchen, mit ihnen Kontakt aufnehmen und eine Art Beziehung vorgaukeln. Ziel sei, Informationen über Standorte und Fahrtrouten amerikanischer Kriegsschiffe zu erhalten.“

Wer nimmt den so etwas ernst? Ich habe aber mal jemand gekannt, der in Afghanistan Computer installiert hat, und der meinte, das Wort „Sicherheit“ könnten die noch nicht mal buchstabieren, auch nicht in Dari oder Paschtu. Und wer sich, wie die Iraner, den Kopf mit dem Koran und anderem religiösem

Quatsch zudröhnen lässt oder das tun muss, wird nicht klar denken können – wie alle Verehrer höherer und niederer Wesen.

By the way, Heise: „Spear-Phishing“ nannte man früher Social Engineering. So nach dem Motto: Wenn man mitten auf dem Ozean ist und auf dem Boardcomputer steht: „Frauen in deiner Nähe würde dich gerne kennen lernen.“ (Gegenrede)

Genauso realistisch ist auch folgendes Szenario: „…die US-Army hat bei allen iranischen Windows-PCs das Windows-Updates angeworfen und somit ein Weiterarbeiten der iranischen Armee über Stunden lahmgelegt. Danach wurden dann automatisch sämtliche glitzernden und flimmernden Spiele aus dem Microsoft-Store installiert, um auch noch das letzte Restchen Festplatte mit sinnlosem Zeug zu füllen, und nix ging mehr. Wenn die Iraner dann aufgeräumt haben und die PCs endlich mal neu gestartet haben, sehen sie dass die Windows-Aktivierung weg ist und nur noch telefonisch aktiviert werden kann. Da ist dann aber immer besetzt.“ (Rechtschreibung korrigiert)

Ich schrieb schon 2012 zum Thema:
Spiegel Online über einen Artikel der New York Times und Stuxxnet und „Obama Order Sped Up Wave of Cyberattacks Against Iran“:

„In die Anlage, die nicht mit dem Internet verbunden ist, gelangten die ersten Virus-Versionen Sanger zufolge über USB-Sticks, später seien auch andere, nicht näher benannte Methoden zum Einsatz gekommen.“

Trump setzt nur das fort, was Obama angefangen hat.

Internet-Voodoo und Computer-Mythologie

Welt online: „Er hackte ihre Konten, griff auf private Fotos und Informationen zu und verbreitete sie im Internet.“

Da wüsste man doch zu gern, wie der „gehackt“ hat: Jemand, der seinen Beruf ernst nimmt als Journalist, würde das recherchieren und dem Publikum erklären.

Hat Christopher Chaney Beschwörungsformeln vor seinem Monitor gemurmelt? „Abrakadabra, jetzt onlinedurchsuche ich dich!“ Oder wie?

Auf solch schwachsinniger Berichterstattung basieren die Computer-Mythen in Fernseh-Krimis und in Filmen – und in den Köpfen der DAUs.

Der Hacker ist der Schamane des 21. Jahrhunderts und wird von der ahnungslosen Journaille mit magischen Fertigkeiten ausgestattet wie der Zauberer eines Dorfes in Papua-Neuguinea. (Ja, das hatte ich vor fünf Jahren schon einmal geschrieben).

Guckst du bei Sawf News: „The photos of Christina Aguilera being leaked to the press were illegally obtained by a hacker who tapped into Christina’s personal stylist’s account“.

Aha. Ein Phishing-Angiff auf die E-Mail-Accounts des sozialen Umfelds der Opfer – technisches *social engineering* sozusagen.

Das funktioniert, weil DAUs mit eingeschaltetem Javascript surfen und E-Mails in HTML-Format erlauben. (Das ist leider ab Werk in den meisten E-Mail-Programmen so eingestellt, das kann man aber ändern!)

Supreme Commander – Der Hacker der Woche

Wired: „‘Supreme Commander’ of Fake Army Marches Into Jail Cell“

Yupeng Deng of Los Angeles pleaded guilty Wednesday to charges that he invented a fake army unit to dupe unsuspecting Chinese immigrants out of cash. Deng, who appointed himself the “supreme commander” of the phony outfit, is now headed to jail for theft by false pretenses, manufacturing deceptive government documents and counterfeit of an official government seal. Deng called his fake outfit the “U.S. Army/Military Special Forces Reserve unit” (MFSR) and held it out to Chinese immigrants as a glide path to U.S. citizenship. He charged each recruit between $300-400 to enlist and $120 a year for “renewal,” duping his victims into thinking they’d be eligible to become American citizens. Unfortunately for enlistees, that wasn’t the case.

Social Engineering vom Feinsten….

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“.

All your data belong to us

Heise: „Das Bundesministerium des Innern (BMI) und das

Bundesamt für Sicherheit in der Informationstechnik (BSI) haben eine Studie zum Identitätsdiebstahl und -missbrauch im Internet veröffentlicht. Das mehr als 400 Seiten starke Dokument betrachtet Identitätsdiebstahl und Identitätsmissbrauch aus technischer und rechtlicher Perspektive und leitet daraus Handlungsempfehlungen ab.“

Ich habe es mir mal angesehen, auch unter dem Aspekt der real gar nicht existierenden „Online-Durchsuchung“.

„Prinzipiell kann eine Infektion durch jegliche installierte Software auf dem Client-System stattfinden, die beispielsweise veraltet und daher auf irgendeiner Art und Weise verwundbar ist. Bei ihren Untersuchungen fand die Firma Trusteer des Weiteren heraus, dass auf fast 84 Prozent der Rechner eine verwundbare Version des Adobe-Readers installiert war. Durch bösartige pdf-Dokumente ist es so möglich, auf dem Endsystem des Nutzers Schadcode auszuführen. Natürlich. Hängt aber vom Betriebssystem und vom Browser ab. Frage: woher bekommt der Angreifer die (jeweils persönliche dynamische!) IP-Adresse des Zielobjekts, das ausgespäht werden soll? „Allerdings sind bisher keine Möglichkeiten bekannt, Addons automatisiert ohne Mitwissen des Nutzers zu installieren.“ Aha.

„Zu einer sehr gefährlichen Infektionsmethode gehört der Drive-By-Download, die eine Schwachstelle im Browser des Opfers ausnutzt. Aber auch der Versand per E-Mail war vor einiger Zeit sehr populär. Eine weitere Methode ist, an beliebte Software ein Trojanisches Pferd anzuhängen und anschließend auf Webseiten oder über P2P-Netzwerke illegal zum Download anzubieten.“ Funktioniert nur, wenn das Zielobjekt selbst aktiv mitspielt und sich wie ein DBU (denkbar bescheuertste User) verhält. Frage: woher bekommt der Angreifer die (jeweils persönliche dynamische!) IP-Adresse des Zielobjekts, das ausgespäht werden soll?

„Selbst durch die Nutzung erweiterter Mechanismen wie etwa speziellen Browser-Add-Ons (beispielsweise NoScript) lässt

sich kein vollständiger Schutz realisieren. Stattdessen leidet aber die Benutzerfreundlichkeit unter diesen Mechanismen, teilweise sind moderne *[was heisst hier „modern“? Das ist schlicht nicht barrierefrei! BS]* Webseiten (die zwingend *[Schwachfug BS]*auf Erweiterungen wie Javascript angewiesen sind) gar nicht mehr benutzbar. Zudem liegt das große Problem aktueller Antivirenprogramme in ihrer Reaktivität, denn sie können in den allermeisten Fällen nur Malware zuverlässig finden, die bereits bekannt ist. Technische Maßnahmen lösen zudem nicht alle Sicherheitsprobleme, vielmehr ist eine umfassende Aufklärung der Anwender von großer Bedeutung“. Deswegen plädiere ich ja schon seit langem vor, die Prügelstrafe für Webdesigner einzuführen, die einen zu Javascript zwingen wollen. Das eigentliche Problem hat also zwei Ohren und sitzt vor dem Monitor. Ich surfe grundsätzlich *ohne* Javascript. Und eine Website, die mich dazu zwingen will, boykottiere ich und stelle den Webdesigner unter den Generalverdacht, eine ignorante dämliche Pfeife zu sein.

„Cross-Site-Scripting (XSS) bezeichnet das Ausnutzen einer Sicherheitslücke in Webanwendungen, wobei Informationen aus einem nicht vertrauenswürdigen Kontext in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig gelten. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden. Ziel ist meist, an sensible Daten des Opfers zu gelangen, um beispielsweise Identitätsdiebstahl zu betreiben. Eine sehr verbreitete Methode hierfür ist, *bösartiges JavaScript* als Payload der XSS-Schwachstelle zu übergeben. Dieses JavaScript wird dann im vertrauenswürdigen Kontext im Browser des Opfers ausgeführt.“ Wie oft muss man also auf einen Webdesigner wohin einprügeln, damit er seine Finger von Javascript lässt? Javascript an sich kann nützlich sein. Wenn man aber Nutzer dazu erzieht, das nicht als Option, sondern per default aktiviert zu lassen, dann handelt man verantwortungslos.

„Die Infektion eines Clients vollzieht sich dabei in mehreren

Schritten: Zunächst muss der Client bzw. dessen Anwender auf eine Website gelockt werden, auf der der entsprechende Schadcode vorhanden ist. Gerne werden dazu Websites verwendet, denen der Benutzer ein gewisses Grundvertrauen entgegenbringt.“ Frage: woher bekommt der Angreifer die (jeweils persönliche dynamische!) IP-Adresse des Zielobjekts, das ausgespäht werden soll? „Surft ein Nutzer nun auf eine solche präparierte Webseite und ist sein Browser anfällig für den dort abgelegten Exploit, so erfolgt die Übernahme des PCs.“ Vermutlich hat so man Ziercke so instruiert, und das hat das natürlich nicht verstanden und machte dann daraus: „Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht.“ – „Initialer Schritt ist, dass der Client auf die manipulierte Website herein fällt.“ Nein, nicht der Client, sondern der Homo sapiens, der ihn benutzt, den der Angreifer als Homo sapiens aber gar nicht erkennen kann, sondern nur dessen IP-Adresse.

Eine hübsche Anmerkung der Studie zum normalen Sicherheitsstandard: „Somit kann fast jedes Telefonat heute durch einen Angriff auf das Internet mitgehört werden, und Notrufnummern können durch Intenet-basierte Denial-of-Service-Angriffe lahmgelegt werden.(…) Durch das Auftreten eines neuen, besonders aggressiven Internet-Wurms (Conficker *[gilt wieder nur für Windows!]*) wurden ganze Truppenteile der Bundeswehr und der französischen Luftwaffe lahmgelegt.“

Auch schön: „Die Suche nach Passwörtern unter Google lässt sich bspw. mit dem Suchstring *intext:“password|pass|passwd“ (ext:sql | ext:dump | ext:dmp) intext:values* realisieren.“ Bruhahaha.

„Zielgerichtete Angriffe auf Linux-Client-Systeme sind nach wie vor kaum zu verzeichnen. (…) Beispielsweise sind Drive-By Angriffe auf Browser unter Linux bisher nicht bekannt.“ Nur gut, dass „Gefährder“ und andere Bösewichter so gut wie nie Linux benutzen, Herr Chef des Bundeskriminalamtes – so hat man

Sie und Frau Ramelsberger doch sicher gebrieft?

Der wichtigste Satz der Studie: „Grundsätzlich kann Social Engineering als das Erlangen vertraulicher Informationen durch Annäherung an Geheimnisträger mittels gesellschaftlicher oder gespielter Kontakte definiert werden. Das grundlegende Problem beim Social Engineering ist die Tatsache, dass Menschen manipulierbar und generell das schwächste Glied in einer Kette sind“.

Die Studie beschäftigt sich auch mit dem neuen Personalausweis: „Der flächendeckende Einsatz des neuen Personalausweises allein wird Identitätsmissbrauch nicht verhindern können: Die von kriminellen Hackern eingesetzten Tools (die überwiegend auf Malware basieren, die im PC des Opfers ausgeführt wird) lassen sich sehr einfach an die bislang spezifizierten Sicherheitsmechanismen anpassen. (…) Es fehlt schlichtweg ein sicherer Betriebsmodus, in dem der Browser und der Bürgerclient ausgeführt werden können“. Das wird natürlich unsere Junta nicht daran hindern, den doch einzuführen.

„Es besteht offensichtlich ein erheblicher Bedarf an Information und Aufklärung. Es ist davon auszugehen, dass Nutzer oft über nur sehr geringes Wissen in Bezug auf die Gefahren des Internet und die Möglichkeiten zur Abwehr von Schäden verfügen.“ Ja, quod erat demonstrandum. Es ist auch davon auszugehen, dass die Nutzer nicht wissen, dass sie gar nichts wissen. Das war auch schon immer so.

Lesebefehl!

Nebelkerzen zur Online-Durchsuchung

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. Eine Presseerklärung irgendeines Innenministeriums gilt nicht als Beweis.

Der Deutschlandfunk hat jetzt eine schöne Nebelkerze geworfen: Man interviewte Peter Welchering, den FDP-Stadtverbandsvorsitzender und Kreisvorsitzender des DJV zum Thema. (Für Insider: Welchering und Karl Geibel sind in

demselben DJV-Verband.) Ach ja, Journalist ist Welchering auch noch und Erfinder des Tron-Netzes.

Sorry, aber ich vergesse nie etwas – Originalton Welchering in einem Artikel vor zwei Jahren: „Wird eine verschlüsselte Datei einmal auf die Festplatte eines Internet-Rechners kopiert, ist sie – auch wenn sie sofort danach wieder gelöscht wird – mit einigem Aufwand mittels Online-Durchsuchung für Datenspione sichtbar.“ Der gute Mann hat also keinen blassen Schimmer.

[Irrelevanter Einschub: Und deshalb war Welchering vermutlich der einzige Journalist, der versuchte, im MediumMagazin die PrivacyBox zu diskreditieren. Er meinte mich, prügelte aber auf die Privacybox ein. So funktioniert Mobbing im DJV. Ich habe ja seinen geliebten Großen Vorsitzenden Charly Geibel ständig angegriffen und der Unfähgkeit bezichtigt. Das tut man nicht unter Journalistenfunktionären. Und ausserdem war ich Chefredakteur von Berliner Journalisten, dem einzig ernst zu nehmenden Konkurrenten des MediumMagazins. Aber ich schweife ab…]

Irgendwie haben sie es ja gemerkt, dass es mit der Online-Durchsuchung nicht so weit her ist. Ja, wo durchsuchen sie denn? Manfred Kloiber fragt: „Welche technischen Probleme machen denn den BKA-Beamten das Leben schwer, Peter Welchering?“ Man muss sich die Anwort auf der Zunge zergehen lassen: „Denn diese Firewall, die verhindert, dass der sogenannte Infiltrationsschädling eindringen kann, das ist im wesentlichen ein Downloader, ein Trojaner, der sich ins System schleicht, um das eigentliche Überwachungsmodul, auf die es ja den Ermittlern ankommt, das dann auch die eigentliche Durchsuchungssoftware von einem BKA-Server herunterladen soll. Das ist insofern etwas verwunderlich, als die von den Geheimdiensten eingesetzten Bundestrojaner dieses Problem eigentlich schon gelöst hatten, und das schon vor einigen

Jahren.“ 

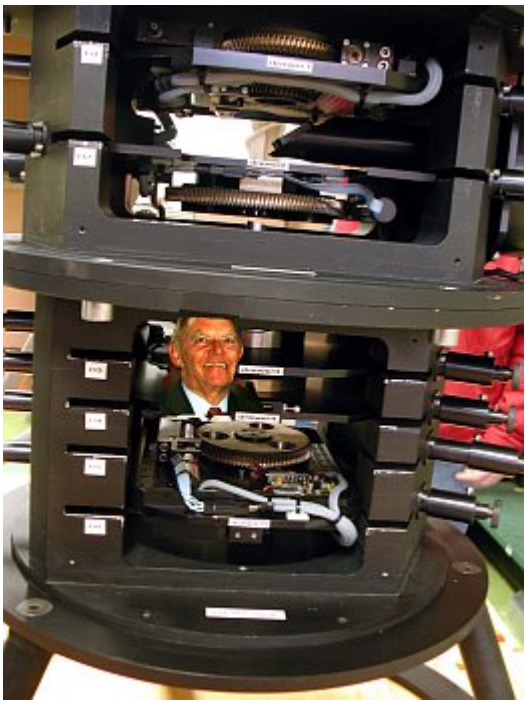
Ja, sie hatten „das Problem“ schon gelöst? Gibt es dazu vielleicht irgendeine winzige Tatsache, die aus einer unabhängigen Quelle stammt? Nein, gar nicht. Null. Es ist nur vages Gefasel. Und: Woher will Welchering das wissen? „Nach allem, was man aus den so schüchternen Sicherheitskreisen so hört“ – das ist. mit Verlaub und meiner Meinung nach pure Aufschneiderei. Mit „Sicherheitskreisen“ meinen Journalisten in der Regel die Presseabteilungen der Verfassungsschützer. Und die sind so seriös wie der ehemalige irakische Informationsminister.

Welchering behauptet allen Ernstes, der Bundesnachrichtendienst habe „solche Angriffsprogramme aus mehr oder weniger gut getarnten Quellen beschafft.“ Woher weiß er das? Das weiß ich wiederum: Von Focus Online, die das ständig mit wachsender Begeisterung, aber faktenfrei behaupten. Oder von Spiegel Online vom Frühjahr 2009: „Nach Informationen des SPIEGEL hat der Geheimdienst BND in den vergangenen Jahren in mindestens 2500 Fällen PCs im Ausland durchsucht“. Aber nicht „online“, sondern Keylogger physikalisch installiert und/oder schlicht die E-Mail-Accounts abgerufen wie beim afghanischen Handelsminister. Welchering weiß nicht mehr, als das, was in der Zeitung steht.

Jetzt fragt Kloiber: „Letztlich handelt es sich ja auch beim Bundestrojaner um ein Computervirus. Und deren Ausbreitung ist ja nicht völlig unter Kontrolle zu halten.“ Nonsens und Schwachfug, wie Wau Holland es funktioniert hätte. Jetzt ist der „Trojaner“ also ein „Virus“? Eine Lokomoive ist also irgendwie ein Auto, und das Usenet ist dasselbe wie das Word Wide Web, und ein Kamel ist auch irgendwie in Pferd? Wenn man etwas nicht kontrollieren kann, dann ist es

ermittlungstechnisch -und taktisch ohnehin Quatsch, von der Beweiskraft vor Gericht ganz zu schweigen.

Welcherung: „Offenbar war man in Wiesbaden mit den Parameterermittlungen, die es ja auch kommerziell zu kaufen gibt, nicht so übermäßig zufrieden. Und man hat deshalb einen anderen Weg eingeschlagen, solche Systemparameter auszuspähen, aber der ist auch nicht erfolgreich gewesen, der ist von den Betriebssystemherstellern dichtgemacht worden. Das funktioniert recht elegant. Die Ermittler haben einfach ein Sicherheitsupdate eines Betriebssystemherstellers genommen und dem einen Trojaner angehängt. Weil Sicherheitsupdates ja automatisch heruntergeladen werden, bemerken die Überwachten PC-Besitzer das gar nicht.“ Ach ja? Gibt es dafür Quellen? Nein, gibt es nicht. Welcherung ist der einzige Mensch auf der Welt, der davon weiß. Er weiß mehr als der Chaos Computer Club und die c’t zusammen. Vielleicht ist das der Grund, warum er in der FDP ist… Da sind ausschließlich solche klugen Menschen.



„Kloiber: Welche Strategien werden denn derzeit im BKA favorisiert, um die technischen Schwierigkeiten beim Einsatz des Bundestrojaners zu überwinden?
Welchering: Das ist schwierig zu ermitteln. Auf solche Fragen schweigt das BKA natürlich“.

Eben. Nichts Genaues weiß man nicht. Man weiß überhaupt nichts, auch nichts über Exploits, mit denen das laut Welchering angeblich gemacht wird. Um so lauter tönen diejenigen, die die magische Online-Durchsuchung herbeifantasieren wollen. irgendwie erinnert mich das geheimisvolle Getöne an Voodoo und Regenzauber. Irgendwelche obskuren Männer stehen im Kreis oder im Viereck und murmeln etwas gemeinsam, auf das die Welt so sei, wie sie es wünschen.

By the way: Wenn ihr das Buch nicht lesen wollt, dann lest die Artikel, die ich 2007 zum Thema gebloggt habe. Har har.

spiggel.de (07.02.2007): „Der Staats-Trojaner-Hoax“
spiggel.de (08.02.2007): „Der Staats-Trojaner-Hoax, update“
spiggel.de (09.02.2007): „Wie schütze ich mich vor dem Bundestrojaner?“
spiggel.de (11.02.2007): „Der SPIEGEL heizt den Hoax an“
spiggel.de (13.02.2007): „Jetzt ganz neu: Social Engineering“
spiggel.de (12.03.2007): „Online-Durchsuchungen, die 234te“
spiggel.de (18.03.2007): „Online-Kriminelle immer onliner und immer krimineller“
spiggel.de (07.04.2007): „Online-Durchsuchungen: Die Farce geht weiter“
spiggel.de (28.04.2007): „Schäuble ist nackt“
spiggel.de (06.05.2007): „Auch du, meine Christiane?“
spiggel.de (10.05.2007): „Der Koran, geile Titten und der Quelle-Katalog“
spiggel.de (10.05.2007): „Heimlicher Zugriff auf IT-Systeme“
spiggel.de (19.05.2007): „Online-Duchsuchung in Second Life!“
spiggel.de (30.06.2007): „Wie tötet man eine Online-Ente?“
spiggel.de (01.07.2007): „Digitale Spaltung?“
spiggel.de (08.07.2007): „Sex-Verbot für Terroristen?“
spiggel.de (12.07.2007): „Wie Enten geklont werden“
spiggel.de (15.07.2007): „Richter erklärt die Online-Durchsuchung zur Ente“
spiggel.de (19.07.2007): „Heise Hoax-verseucht“
spiggel.de (31.07.2007): „Hurra, so funktionieren Online-

Durchsuchungen!“
spiggel.de (25.08.2007): „Sie haben ein Attachment bekommen“
spiggel.de (28.08.2007): „Blauäugige Keylogger“
spiggel.de (30.08.2007): „Gefälschte Behörden-E-Mails?“
spiggel.de (03.10.2007): „Keine Chance für Online-Durchsuchung“
spiggel.de (07.10.2007): „Das Märchen vom Datenstrom“
spiggel.de (22.10.2007): „Technische Details offen“
spiggel.de (10.11.2007): „Neues vom Tron-Netz“
spiggel.de (13.11.2007): „Eintagstrojaner mit Verfallsdatum“
spiggel.de (10.11.2007): „Zierckes Traum“
spiggel.de (19.11.2007): „Terroristen nutzen Windows“
spiggel.de (16.12.2007): „HTTP 909 – Bundestrojaner-Online-Durchsuchung“

Geheimes Kaffeetrinken

Ja, ich gebe es zu: Ein starkes Motiv für meine Mitgliedschaft im Deutschen Journalisten-Verband (DJV) ist das Amusement. Man kann sich ständig totlachen. Welcher Verein bietet noch diesen Service? Außerdem sehe ich als gelernter Altgermanist gern altdeutsche Weisheiten live bestätigt, etwa: „Dummheit und Stolz wachsen auf einem Holz“. Oder: „Wer sich selbst eine Grube gräbt, fällt auch hinein.“ Da es sich um einen Journalisten-Verband handelt, trifft noch eine weiterer Lehrsatz zu, den man auf der Journalisten-Universität schon im ersten Semester auswenig lernen muss: „Einer quatscht immer“. Aber das werden die Apparatschiks beim DJV nie kapieren. Kein Wunder: Die sind eben keine Journalisten.

Der DJV lud also vor einiger Zeit alle Geschäftsführer der Landesverbände zum 12. März zu einer offiziellen Geschäftsführertagung nach Hannover in ein schickes Hotel ein.

Dann wurde das Treffen offiziell wieder abgesagt.

Da man seine Pappenheimer kennt, glaubt man natürlich prophylaktisch kein Wort. Und siehe da: Die Geschäftsführer der Landesverbände reisten – trotz der Absage – dennoch nach Hannover, einige schon am Vorabend. Alle – außer dem DJV Brandenburg. Den wollte man nicht dabeihaben und hatte ihn auch nicht von dem Event informiert. Warum? Darüber kann man nur spekulieren: Es ging um Geld. Da der DJV eine inoffizielle Schattenwirtschaft betreibt, eine Art „Reptilienfonds„, und sogar versucht, Gerichte damit hinter's Licht zu führen, soll alles geheim bleiben. Das funktioniert natürlich nicht, aber die Apparatschiks hätten es so gern. Wie schon erwähnt: Einer quatscht immer.

Die Damen und Herren trafen sich am Vorabend in einem anderen Hotel, um in trauter Runde zu mauscheln. Vermutlich fürchteten sie, dass irgendein Vertreter der Brandenburger im ursprünglich vorgesehenen Hotel anrufen würde, um herauszufinden, ob die Geschäftsführertagung dennoch stattfände. Diese gute alte Recherchemethode nennt man bekanntlich Social Engineering.

Am 12. März in der Frühe sprang man dann wohlgemut in Taxis und begab sich in die Geschäftsstelle des DJV Niedersachsen. Aber, welch' Wunder: Dort tauchte der gar nicht vorgesehene Geschäftsführer des DJV Brandenburg auf und setzte sich frech zu den Herrschaften, als sei nichts geschehen. Potztausend! Alle schwiegen betreten. Was tun? Wie kann man Gelder hin- und herschieben, wenn jemand zuhört, der das gar nicht wissen soll? Der Vertreter des DJV Brandenburg wurde also wieder hinausgebeten, Hausrecht und so. Es handele sich bei dem Treffen mitnichten um eine Geschäftsführertagung, obwohl ein rundes Dutzend GeschäftsführerInnen anwesend waren. Vermutlich waren die auf Kosten der Mitglieder nur zu einem geheimen Kaffeetrinken versammelt.

Ich habe offiziell nachgefragt. Frage: „Warum wurde dem vom

DJV Brandenberg benannten Geschäftsführer die Teilnahme an der Sitzung versagt?“ Antwort: „Da die Geschäftsführertagung abgesagt wurde, konnte dem Geschäftsführer des DJV Brandenburg auch nicht die Teilnahme verweigert werden.“ Eine bestechende Logik, auf die selbst die Scholastiker des Mittelalters nicht gekommen wären!

Was soll man zu diesem Kindergarten noch sagen? Deutscher Jux-Verband? Ich könnte mich immer wieder kringeln über die Gurkentruppe, die da das Sagen hat.

Online-Durchsuchung | Chronologie

Medienberichte über die „Online-Durchsuchung“ (Auswahl)

Focus 38/1993: „Nationales Netz. Unter Verwendung zentraler Mailboxen bauen Neonazis ein landesweites Computernetz auf

20.09.1999 | Florian Rötzer (Telepolis): Lizenz zum Abhören

10.04.2000 | Jelle van Buuren (Telepolis): Digitale Detektive in Holland

28.07.2000 | Armin Medosch (Telepolis): UK-RIP-Gesetz über Ermittlungsbefugnisse verabschiedet

22.11.2000 | Nicky Hager (Telepolis): Schnüffelnde Kiwis – Überwachung in Neuseeland

06.12.2000 | Florian Rötzer (Telepolis): Nichts mehr mit Pretty Good Privacy?

15.05.2001 | Hubert Erb (Telepolis): Die Cyberspace-Fallen des

FBI

21.11.2001 | Florian Rötzer (Telepolis): FBI entwickelt angeblich Virus zum Belauschen

13.12.2001 | Florian Rötzer (Telepolis): FBI bestätigt Entwicklung des Schnüffelprogramms Magic Lantern

06.07.2006 | Monika Düker MdL, innenpolitische Sprecherin der Grünen im nordrhein-westfälischen Landtag: „Erweiterte Kompetenzen für den Verfassungsschutz in NRW rechtlich fragwürdig“ *Zu § 5 Abs. 2 VSG NRW (allgemeine Befugnisse des Verfassungsschutzes): Die neue Formulierung des § 5 Abs. 2 Nr. 11 erlaubt dem Verfassungsschutz zukünftig ein völlig unbegrenztes heimliches Beobachten und Schnüffeln im Internet, gleich einem „Hacker“. Dass sich die Computer häufig im privaten Wohnraum der Betroffenen befinden, hat das Innenministerium in seiner Gesetzesbegründung gar nicht bedacht und begründet einen Eingriff in das Recht auf informationelle Selbstbestimmung mit der Zunahme der Kommunikationsverlagerung extremistischer Bestrebungen auf das Internet. Damit hat die Landesregierung übersehen, dass die im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten sowohl unter den Schutzbereichs des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG) als auch unter den Schutzbereich des Art. 13 GG, die Unverletzlichkeit der Wohnung fallen.*

23.08.2006 | heise.de: Schäuble und GdP fordern schärfere Überwachung von Netzinhalten. *„…verstärkte Inspektion der Kommunikationsströme im Internet, um online vorangetriebene Terrorplanungen und Hetzpropaganda zu verhindern. (…) Das Bundeskriminalamt (BKA) arbeitete in diesem Rahmen an einer zentralen Datenbank für Netzermittlungen. Zudem können Strafverfolger anhand der Vorgaben der Telekommunikations-Überwachungsverordnung (TKÜV) auch den E-Mail-Verkehr von Verdächtigen abhören.“*

24.08.2006 | Rüdiger Soldt (Frankfurter Allgemeine Zeitung/FAZ.net): Die virtuelle Welt des Terrorismus. *„‚Es gibt eine Sicherheitslücke. Die Propaganda im Internet radikalisiert sich, und zugleich wird das Verhalten der Islamisten immer konspirativer', sagt Johannes Schmalzl, Präsident des baden-württembergischen Landesamtes für Verfassungsschutz, der F.A.Z. Die Überwachung eines privaten Internetanschlusses sei, falls die zuständige G-10-Kommission dies genehmigt habe, für den Verfassungsschutz möglich. Mit Hilfe der ‚IP-Adresse' des Computers ließen sich E-Mails und die Nutzung von Internetseiten rekonstruieren. (…) Er plädiere deshalb dafür, die Inhaber solcher Cafés gesetzlich dazu zu zwingen, zum Beispiel den Verlauf des Internetprogramms und die temporären Dateien zu speichern sowie die persönlichen Daten der Kunden zu registrieren."*

24.08.2006 | Die Zeit – Interview mit Wolfgang Schäuble: Mehr Kontrolle!
„Wir müssen die Kontrolle des Internets verstärken."

25.08.2006 | Bundesministerium des Innern, Auszug aus der Pressekonferenz von Dr. Wolfgang Schäuble am 24.08.2006 „Auch ein großer Erfolg internationaler Zusammenarbeit" *Ich werde alles daran setzen, die Möglichkeiten der Sicherheitsbehörden – insbesondere des Verfassungsschutzes – zu verstärken, etwa in der Kontrolle des Internets…*

27.08.2006 | Heise Newticker: Schäuble und GdP fordern schärfere Überwachung von Netzinhalten

27.08.2006 | Heise Newticker: Überwachung des Internet soll verstärkt werden

28.08.2006 | Presseerklärung des Innenministeriums Nordrhein-Westfalen. *„Nur unter denselben strengen rechtsstaatlichen Anforderungen soll es dem Verfassungsschutz NRW zukünftig erlaubt sein, auf Rechner von Terroristen zuzugreifen."*

28.08.2006 | Die Welt: NRW will Internet-Kontrollen ausweiten.

„Bisher habe der Verfassungsschutz nur die Befugnis, Aktivitäten ausländischer Netzwerke im Internet zu verfolgen, sagte Wolf. ‚Das werden wir auf inländische Netzwerke ausweiten.‘

31.08.2006 | Heise Newticker: Verfassungsschutz soll auf Computer übers Internet zugreifen dürfen. *„Dabei soll der Verfassungsschutz aber auch auf Rechner von mutmaßlichen Terroristen über das Internet zugreifen können, die Rede ist vom Zugriff auf ‚Internet-Festplatten‘ (…) Konkret heißt es in der Gesetzesvorlage, dass die Verfassungsschutzbehörde folgende Maßnahmen anwenden darf: ‚heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen beziehungsweise die Suche nach ihnen sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel.‘*

01.09.2006 | Florian Rötzer (Telepolis): Der Verfassungsschutz soll „Emails auf Festplatten“ lesen dürfen.. *„Zu dieser offensiven Internetbeobachtung gehört neben der Beobachtung von Homepages auch das Lesen von e-mails auf Festplatten.“*

19.10.2006 | Pressemitteilung des Innenministeriums des Landes Nordrhein-Westfalen: „NRW-Verfassungsschutzgesetz garantiert Balance von Freiheit und Sicherheit – Innenminister Wolf: Schärfere Überwachung von Terroristen“. *„‚Wer die Überprüfung von Daten auf Rechnern potenzieller Terroristen für einen Einbruch in den grundgesetzlich geschützten Wohnraum hält, hat das Wesen des Internets nicht verstanden‘, betonte Wolf. Der Nutzer befinde sich weltweit online und verlasse damit bewusst und zielgerichtet die geschützte häusliche Sphäre. ‚Der Standort des Computers ist dabei völlig unerheblich. Es findet zudem keinerlei Überwachung der Vorgänge in der Wohnung selbst statt‘, erläuterte der Innenminister.“*

10.11.2006 | heise.de: 132 Millionen Euro für schärfere Überwachungsmaßnahmen freigegeben. *„…will der CDU-Politiker*

nun etwa terroristische Bestrebungen durch eine schärfere Überwachung von Online-Foren besser bekämpfen (…) Wichtiger Teil des Initiative ist die Einrichtung der „Internet Monitoring und Analysestelle“ (IMAS) am Gemeinsamen Terror-Abwehr-Zentrum von Polizei und Nachrichtendiensten (GTAZ) in Berlin. Allein 30 Millionen Euro sollen dort angeblich für neue Hardware ausgeben werden, mit der sich auch die Internet-Telefonie und geschlossene Chaträume anzapfen lassen. Die neue Überwachungstruppe hat zunächst die Aufgabe, mehr Transparenz in die dschihadistischen Netzumtriebe zu bringen. Sie soll auch Wege finden, um Hetzpropaganda und Anleitungen zum Bombenbau aus dem Cyberspace zu verbannen. Ob Schäuble ähnlich wie der nordrhein-westfälische Innenminister Ingo Wolf (FDP) dem Verfassungsschutz etwa auch verdeckten Zugriff auf ‚Festplatten‘ und andere ‚informationstechnische Systeme‘ im Internet geben will, ist noch unklar.“

07.12.2006 | Andreas Förster (Berliner Zeitung): Hacken für die Sicherheit. *„Das Bundeskriminalamt soll künftig online in die Personalcomputer von Verdächtigen eindringen und sie nach ‚verfahrensrelevanten Inhalten‘ durchsuchen können. Bundesinnenminister Wolfgang Schäuble (CDU) habe jetzt den Haushaltsausschuss des Bundestages darüber in Kenntnis gesetzt, dass die entsprechenden Computerprogramme, mit denen über die vorhandenen Kommunikationsnetze auf die Festplatten mutmaßlicher Krimineller und Terroristen zugegriffen werden kann, derzeit entwickelt werden, meldete jetzt die Bild-Zeitung. Die Dunkelziffer der ausgespähten und durch Viren ferngesteuerten PC in Firmen und Privathaushalten ist dagegen kaum zu schätzen. Zu einfach ist es für Experten – von denen einige auch Polizei und Geheimdiensten gern zur Hand gehen – , trotz angeblich ausgefeilter Abwehrtechnik online in Computer und Datennetzwerke einzudringen.“*

07.12.2006 | Heise Newticker: Online-Durchsuchung von PCs durch Strafverfolger und Verfassungsschutz. *„Das BKA soll auch Zugriff auf die PCs der Bürger über das Internet erhalte.“*

07.12.2006 | PC Professionell: BKA-Trojaner soll private PCs durchsuchen. *„Bald schon könnten Computerexperten des Bundeskriminalamts (BKA) bald private PCs unbemerkt via Internet durchsuchen. Das fordert Bundesinnenminister Wolfgang Schäuble (CDU). Die Durchsuchungen sollen dabei so erfolgen, dass Computerbesitzer, gegen die ein Strafverfahren läuft, nichts davon bemerken, meldet AFP United-News.“*

07.12.2006 | Annette Ramelsberger (Süddeutsche): Durchsuchung online. *„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.“*

07.12.2006 | Jörg Donner (sueddeutsche.de): Bundestrojaner im Computer. *„‚Es gab bereits Einzelfälle in Strafverfahren, bei denen richterlich angeordnet solche Durchsuchungen stattgefunden haben‘‘, sagt Dietmar Müller, Pressesprecher des BKA in Wiesbaden.“*

08.12.2006 | golem.de: Online-Durchsuchung durch BKA und Polizei?

08.12.2006 | Tagesspiegel: Die Ermittler surfen 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. (…) Im einfachsten Fall wird das Spionageprogramm per E-Mail auf den zu überwachenden PC eingeschleust. Die Zielperson kann aber auch zu einer Webseite gelockt werden, von wo aus sich unbemerkt im Hintergrund das Spionageprogramm installiert. Die Internetverbindung braucht das Programm nur, um sich auf dem Rechner zu installieren –*

danach sammelt es selbstständig im Hintergrund die gewünschten Daten. Ist der Vorgang abgeschlossen, wird das Ergebnis per Internet automatisch an die Fahnder übermittelt. Wird der PC vor Ende der Übertragung abgeschaltet, nimmt das Programm dieses nach dem nächsten Start wieder auf. Das in der Schweiz getestete Programm kann sogar noch mehr: Die Software kann auch das eingebaute Mikrofon oder angeschlossene Web-Kameras aktivieren und somit Räume überwachen.“

08.12.2006 | Florian Rötzer (Telepolis): Lauschangriff auf Festplatten

11.12.2006 | Christian Rath (taz): Polizei-Trojaner greifen Computer an

11.12.2006 | Christian Rath (taz): Die Polizei als Hacker

11.12.2006 | Christian Rath (Kommentar): Chaos Computer Polizei

11.12.2006 | heise.de: BGH verbietet Online-Durchsuchung von Computersystemen

14.12.2006 | Sigrid Averesch (Berliner Zeitung): Schaar lehnt staatliches Hacken ab – Datenschutzbeauftragter gegen Online-Durchsuchungen. *„Wie berichtet, soll das Bundeskriminalamt mit Hilfe einer speziellen Software, etwa mit Hilfe von Trojanern, die Daten auf privaten Rechnern durchsuchen können. (…) Kommende Woche wird der Landtag in Düsseldorf einen Gesetzentwurf aus seinem Hause beschließen, der dem Landesverfassungsschutz Online-Durchsuchungen ermöglicht.“*

14.12.2006 | Jochen Bittner und Florian Klenk (Die Zeit): Angriff auf den Rechtsstaat. *Eine neue Online-Ausforschungsmethode der Polizei bekam sogar den Segen eines Ermittlungsrichters am Bundesgerichtshof (BGH), obwohl für sie überhaupt keine gesetzliche Ermächtigung besteht. Mithilfe von Hacker-Programmen können Ermittler die Festplatten von Computern durchleuchten. Dafür hat Innenminister Wolfgang*

Schäuble dem BKA kürzlich zusätzliches Geld versprochen.

22.12.2006 | Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Petra Pau, Kersten Naumann und der Fraktion DIE LINKE. [Drucksache 16/3787].
[Frage] „Seit wann wenden deutsche Sicherheitsbehörden das Instrumentarium des ‚heimlichen Abziehens von Daten auf fremden Computern mittels spezieller Software' (Online-Durchsuchung) an?
[Antwort] Der Bundesregierung liegen keine Erkenntnisse über in Ermittlungsverfahren durchgeführte Online-Durchsuchungen vor. (…) Die vom Ermittlungsrichter des Bundesgerichtshofs am 21. Februar 2006 angeordnete Maßnahme wurde nicht durchgeführt. „

30.01.2007 | Christian Rath (taz) : Festplatten im Visier

05.02.2007 | netzpolitik.org: Überblick: Online-Durchsuchung beim Bundesverfassungsgericht (Medienspiegel)

05.02.2007 | Frankfurter Allgemeine Zeitung/FAZ.net: Wie Behörden Computer ausspionieren. *„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."*

06.02.2007 | Burkhard Schröder (Telepolis): Verdeckter Zugriff auf Festplatten

06.02.2007 | Holger Dambeck (Spiegel Online): Die Methoden der Staats-Hacker. *„Was sich die deutschen Ermittler wünschen, ist technisch nicht besonders kompliziert. Moderne Betriebssysteme und Computeranwendungen sind so komplex, dass sie kaum frei von Fehlern sein können. (…) Die Online-Ermittler hätten alle Möglichkeiten zur Verfügung, derer sich auch kriminelle Hacker bedienen, sagte Daniel Bachfeld, Sicherheitsexperte der Computerzeitschrift ‚c't': ‚Das BKA könnte zum Beispiel an einen Verdächtigen gezielt ein interessant erscheinendes Worddokument verschicken, das dann ein Spionageprogramm einschleust.' (…) An Experten, die PCs knacken können, herrscht auch in Deutschland kein Mangel."*

06.02.2007 | Holger Schmidt (Frankfurter Allgemeine Zeitung/FAZ.net): Nicht nur der Bund schickt Spionagesoftware. *„Im Auftrag der Bundesregierung wird gerade der „Bundestrojaner" programmiert. Die Software, die bis zu 200.000 Euro kostet, soll den Strafverfolgungsbehörden die Durchsuchung eines Internetcomputers ohne Wissen des Besitzers ermöglichen."*

07.02.2007 | Tagesspiegel: Skeptische Experten. *„Jürgen Kuhri [sic], stellvertretender Chefredakteur der Computerzeitschrift ‚c't', hält den Plan für einen ‚massiven Eingriff in die Privatsphäre'. Weiter sagte er: ‚Der Vorstoß ist ein Windei, denn er lässt sich technisch kaum umsetzen.'"*

07.02.2007 | Ursula Knapp (Tagesspiegel): Zugriff verweigert

07.02.2007 | Andreas Bogk (CCC): Der Bundestrojaner und die Online-Durchsuchung. *„Eher verwunderlich hingegen ist die bei Heise zur Schau gestellte Skepsis, was die technische Machbarkeit einer solchen Online-Durchsuchung angeht. Gut, von Burkhart [sic] Schröder sind wir ja Desinformation gewöhnt, aber daß auch Jürgen Kuri da die technische Phantasie fehlt, ist schon eher ungewöhnlich. (…) „Zum einen hat das BSI angefragt, ob ich nicht eine Schulung zum Thema ‚wie schreibe ich einen buffer overflow exploit' für Vertreter diverser*

Behörden und Organisationen mit Sicherheitsaufgaben halten könne. Zum anderen bekam mich eine Anfrage, doch ein Angebot zur Entwicklung einer transparent bridge abzugeben, die einen Download eines ausführbaren Programms erkennt und dieses on-the-fly mit einem Trojaner versieht.“

08.02.2007 | Christian Rath (taz) – Interview mit Bundesinnenminister Wolfgang Schäuble: „Terroristen sind auch klug“

09.02.2007 | Daniel Schulz und Astrid Geisler (taz): Die trojanische Kriegserklärung

13.02.2007 | Peter Zschunke/AP (Spiegel Online): Die Mär vom ‚Bundestrojaner‘. *„Das BKA arbeitet bereits an den technischen Voraussetzungen zum Einsatz von Späh-Programmen. Experten zweifeln allerdings an deren Tauglichkeit in der Praxis. (…) Andere setzen auf Strategien des „Social Engineerings“: Hierbei werden Gewohnheiten einer Zielperson erkundet und eingesetzt, um sie auf eine interessant erscheinende Web-Seite zu locken. Dort wird dann im Hintergrund ein Wurm heruntergeladen, der laut Hardy ’nichts anderes zu tun hat, als den eigentlichen Trojaner herunterzuladen und sich dann selbst zu löschen.'“*

13.02.2007 | Peter Zschunke/AP (stern.de): Wer braucht einen Bundestrojaner?

19.02.2007 | Bernd Kling (Telepolis): Die Vaporware des BKA

26.02.2007 | Telepolis: (Der Text der) Verfassungsbeschwerde gegen Online-Durchsuchungen

07.03.2007 | Annette Ramelsberger (Süddeutsche): BKA findet Anleitung zum Sprengsatzbau *Den Laptop, den die beiden für ihre Internet-Recherche nach Bombenbauanleitungen nutzten, hatte Hamad bei seiner Flucht aus Köln mit in den Libanon genommen. Die Festplatte des Computers hatte er jedoch gelöscht, kurz bevor er sich auf Anraten seiner Familie den*

libanesischen Behörden stellte. Den Experten des BKA ist es nun gelungen, die Festplatte zu spiegeln und aus den restlichen Daten ein Puzzle zusammenzusetzen.

11.03.2007 | Jürgen Schmidt (c't): Bundestrojaner: Geht was – was geht. Technische Optionen für die Online-Durchsuchung. *„Und um Missverständnissen vorzubeugen: Selbstverständlich kann man sich gegen all die hier geschilderten Einbruchsversuche schützen."*

11.03.2007 | koehntopp.de: „Bundestrojaner, Sina-Boxen und Mailüberwachung"

16.03.2007 | Welt.de: BKA sieht G-8-Gipfel als wahrscheinlichstes Ziel. *„"Nach BKA-Erkenntnissen wird das Internet auch immer mehr zum Tatwerkzeug. Eine Variante sei, mit Spam-Mails auf fremden PCs sogenannte Trojaner zu installieren, sagte Abteilungspräsident Jürgen Maurer. Mit den getarnten Programmen könne ein Straftäter fremde Rechner für seine Zwecke nutzen – etwa sie unbemerkt zusammenschalten, um mit massenhaften Anfragen Firmenserver lahmzulegen."*

23.03.2007 | Maximilian Steinbeis (handelsballt.com): Neuer Streit um heimliche Online-Razzien *„Wie oft wird von dieser Maßnahme überhaupt Gebrauch gemacht?" Das sei geheim, sagte eine Sprecherin des Bundesamts für Verfassungsschutz.*

24.03.2007 | heise.de: Innenministerium: Verfassungsschutz, MAD und BND können Online-Durchsuchungen durchführen.

26.03.2007 | Florian Rötzer (Telepolis): Online-Durchsuchungen bereits möglich?

26.03.2007 | taz/Interview mit Jörg Ziercke. *„Wie stellen Sie sicher, dass Sie bei der Durchsuchung nicht den besonders geschützten „Kernbereich der privater Lebensgestaltung" verletzen?*
Wir können über die Verwendung bestimmter Schlüsselbegriffe steuern, dass ganz private Daten von der Polizei gar nicht zur

Kenntnis genommen werden.“

05.04.2007 | Thomas Sigmund (Handelsblatt): Kommentar: Mangel an Alternativen. *„Alle islamistischen Täter haben in den vergangenen Jahren ihre Anschläge im Internet vorbereitet. Der ‚Cyber-Dschihadismus‘ ließ den Staat alt aussehen. Aufrufe zur Tat, Anschlagsziele und Bauanleitungen für Bomben kommen aus dem Netz. Die Terrorgruppe trifft sich im Chat-Room. Es reicht nicht mehr aus, nur einen PC zu beschlagnahmen, wenn man die Personen hinter den fingierten Decknamen identifizieren will.“*

25.04.2007 | Focus: Computer längst nicht mehr sicher. *„Deutsche Geheimdienste spähen schon seit 2005 heimlich über das Internet Computer von Verdächtigen aus.“*

25.04.2007 | Pressemitteilung der FPD-Fraktion im Bundestag/Gisela Piltz: Bundesregierung lässt bei Online-Durchsuchungen von Computern die Katze aus dem Sack

25.04.2007 |heise.de: Bundesregierung gibt zu: Online-Durchsuchungen laufen schon. *„Das Bundeskanzleramt hat am heutigen Mittwoch in der Sitzung des Innenausschusses des Bundestags eingeräumt, dass die umstrittenen heimlichen Online-Durchsuchungen von Computern durch Geheimdienste des Bundes bereits seit 2005 auf Basis einer Dienstvorschrift des damaligen Bundesinnenministers Otto Schily (SPD) stattfinden. Dies berichtet die innenpolitische Sprecherin der FDP-Bundestagsfraktion, Gisela Piltz, auf deren Antrag hin die Bundesregierung zu den pikanten Überwachungen privater PC und Speicherplattformen im Internet Stellung nehmen musste. (…) Zur Anzahl der bisher durchgeführten verdeckten Netzermittlungen gab die Bundesregierung keine Auskunft. Dem Vernehmen nach gibt es aber noch Probleme bei der praktischen Durchführung der Online-Durchsuchungen. So soll von Regierungsseite beklagt worden sein, dass so viele Daten gesammelt worden seien, dass man ihrer nicht Herr habe werden können.“*

25.04.2007 | stern.de: Online-Durchsuchungen – Geheimdienste spitzeln schon seit Jahren.

25.04.2007 | Thorsten Denkler (sueddeutsche.de): Bund schnüffelt bereits seit 2005

26.04.2007 |Frankfurter Allgemeine Zeitung/FAZ.net: Schäuble stoppt Online-Durchsuchungen. *„Das Kanzleramt hatte am Mittwoch eingeräumt, dass Verfassungsschutz und Bundesnachrichtendienst bereits seit 2005 heimlich über das Internet Computer ausspähen. Die Ermittlungen wurden auch fortgesetzt, nachdem der Bundesgerichtshof Online-Durchsuchungen der Polizei im Februar für unzulässig erklärt hatte.“*

27.04.2007 | tagesschau.de: Rund ein Dutzend Mal wurde geschnüffelt. *„Seit 2005 haben deutsche Geheimdienste nach Angaben des Bundesinnenministeriums knapp ein Dutzend Privatcomputer heimlich via Internet durchsucht. Eine genaue Zahl wollte die Sprecherin des Ministeriums nicht nennen.“*

28.04.2007 | Wolfram Leytz (tagesschau.de): Interview mit Wolfgang Wieland (Bündnis90/Die Grünen) – „Online-Durchsuchungen braucht man nicht“. *„Wir gehen auch davon aus, dass das noch nie richtig geklappt hat. Es gab technische Schwierigkeiten. Das Einschleusen hat nicht geklappt und gerade die gefährliche Szene wird Wege finden, sich vor Bundestrojanern zu schützen.“*

28.04.2007 | Manfred Kloiber im Gespräch mit Peter Welchering (Deutschlandradio): Brecheisen für den Bundestrojaner. Online-Durchsuchung kämpft mit technischen Problemen

02.05.2007 | heise.de: Staatssekretär: Schily wollte keine Online-Durchsuchungen. *„Zu der umstrittenen Dienstvorschrift Schilys betonte Diwell, der seit Ende 2005 Staatssekretär von Justizministerin Brigitte Zypries (SPD) ist, er habe das Parlamentarische Kontrollgremium (PKG) des Bundestags im Juli 2005 schriftlich über die neuen Möglichkeiten zur Internet-*

Beobachtung unterrichtet. Laut Diwell habe sich das Bundesamt für Verfassungsschutz an das Innenministerium gewandt und eine Erweiterung der Dienstvorschrift über die zulässigen nachrichtendienstlichen Mittel angeregt. Dabei sei es um die „offensive Beobachtung des Internets“ gegangen.“

02.05.2007 | Christian Rath (taz): Geheimdienst außer Kontrolle. *„Das Bundesamt für Verfassungsschutz fühlte sich von der Politik ermächtigt, mit Spionagesoftware auf die Festplatten von Privatcomputern zuzugreifen. Zwar hat es wohl nur wenige derartige Online-Durchsuchungen durch den Verfassungsschutz gegeben. (…) Denkbar ist aber auch, dass Geheimdienst und Innenministerium zunächst nur über eine Erlaubnis für die klandestine Beobachtung von Internet-Foren sprachen und sich erst später neue technische Möglichkeiten zum Festplatten-Zugriff ergaben.“*

03.05.2007 | Christiane Schulzki-Haddouti (Focus Online): So arbeiten staatliche Hacker. *„Polizei und Geheimdienste besitzen schon lange Werkzeuge, um Computer von Verdächtigen heimlich zu durchsuchen.“*

10.05.2007 | Netzeitung: Kein Schutz gegen Online-Durchsuchung möglich. *„Online-Durchsuchungen können mit den gängigen Computer-Programmen nicht verhindert werden. ‚Übliche Antivirenprogramme und Firewalls sind machtlos‘, sagte Constanze Kurz vom Chaos Computer Club der «Zeit». ‚Die Ermittler werden Schwachstellen nutzen, etwa im Mailprogramm oder Browser.'“*

11.05.2007 | ZEIT online: Spionage im Netz. *„Nach Ansicht des Chaos Computer Clubs (CCC) kann der einfache Computerbenutzer sich praktisch nicht gegen die von Bundesinnenminister Wolfgang Schäuble geforderten heimlichen Online-Durchsuchungen von Rechnern wehren. „Übliche Antivirenprogramme und Firewalls sind machtlos. Die Ermittler werden Schwachstellen nutzen, etwa im Mailprogramm oder Browser“, sagt Constanze Kurz vom CCC der Zeit.“*

16.06.2007 | Peter M. Buhr (Zeit online): Zugriff der Hacker. *„Wie ist es möglich, dass ein Polizist E-Mails auf meinem Computer lesen kann? Eine Erklärung“*

17.05.2007 | Lutz Herkner (Die Zeit): Hacken für den Staat. *„Polizei und Geheimdienst wollen Computer ausspähen. Womöglich sind nicht die juristischen Hürden das Problem, sondern die technischen.“*

02.06.2007 | Spiegel Online: Schäuble will für den Bundestrojaner das Grundgesetz ändern

07.06.2007 | netzpolitik.org: Schäuble stoibert über die Online-Durchsuchung

26.06.2007 | Ansbert Kneip (Spiegel Online): Hacken für jedermann. *„Auch die Spezialisten vom BKA würden über Sicherheitslücken in fremde PC eindringen, allerdings über andere, weniger bekannte Wege.“*

05.07.2007 | Nils Weisensee (Spiegel Online): Angriff auf die Ahnungslosen. *„IT-Experten halten den Vorstoß für eine Schnapsidee: technisch schwer umzusetzen und letztlich ein Werkzeug zur Überwachung von Ahnungslosen und Unschuldigen.“*

09.07.2007 | Der Spiegel, Interview mit Wolfgang Schäuble: ‚Es kann uns jederzeit treffen‘.
[Frage] „…die heimlichen Online-Durchsuchungen zeigen. Die haben die Sicherheitsbehörden ohne gesetzliche Grundlage jahrelang angewandt.
Schäuble: Moment. Es gab einen Anwendungsfall im Inland. Ich habe nach dem Urteil des Bundesgerichtshofs, mit dem die Richter die fehlende Rechtsgrundlage moniert haben, die Praxis gestoppt.“

18.07.2007 | heise.de: Heimliche Online-Durchsuchung in den USA: FBI setzte erstmals CIPAV ein.

18.07.2007 | heise.de: Skeptische Stimmen zur Online-

Durchsuchung

25.07.2007 | heise.de: Online-Durchsuchung: Ist die Festplatte eine Wohnung?

30.07.2007 | Welt online: Wie Online-Durchsuchungen funktionieren. *„Die nötige Software ist in seiner Behörde längst vorhanden.“*

03.08.2007 | Exklusiv: CHIP enttarnt Bundestrojaner. Der Bundestrojaner ist eine Wanze. *„Das mag in seltenen Fällen tatsächlich ein E-Mail-Trojaner sein; aufgrund der mageren Erfolgsaussichten bevorzugt man in Wiesbaden aber robustes Agenten-Handwerk: heimlich in die Wohnung eindringen und Images von allen PC-Festplatten ziehen. Diese Daten analysiert dann der BKA-Software-Entwickler und bastelt ein Tool, das perfekt auf die Rechner-Umgebung zugeschnitten ist.“*

03.08.2007 | heise.de: „Bundestrojaner“ heißt jetzt angeblich „Remote Forensic Software“

07.08.2007 | heise.de: SPD-Sprecher hält Online-Razzien derzeit für unverantwortbar

24.08.2007 | heise.de: Innenministerium verrät neue Details zu Online-Durchsuchungen. *„Alles deutet demnach darauf hin, dass die eigentliche Spyware-Komponente im Rahmen eines gängigen Trojaner-Angriffes auf einen Zielrechner gelangen soll. ‚Die Einbringung der RFS im Wege der E-Mail-Kommunikation kann je nach Einzelfall ein geeignetes Mittel darstellen‘, heißt es in der heise online vorliegenden Stellungnahme des von Minister Wolfgang Schäuble (CDU) geführten Hauses. Dazu werde ein Bestandteil des Werkzeugs zur ‚Datenerhebung‘ einer weiteren Datei beigefügt. Beim Öffnen dieses Anhangs werde die RFS auf dem Zielsystem installiert.“*

24.08.2007 | heise.de: Innenministerium bezeichnet Entdeckungsrisiko für Bundestrojaner als gering

25.08.2007 |heise.de: Heimliche Online-Durchsuchungen und der Schutz der Privatsphäre

25.08.2007 | heise.de: Bundesregierung sieht sich mit Online-Durchsuchungen nicht allein. *„Explizite Regelungen für die verdeckte Ausforschung informationstechnischer Systeme durch Sicherheitsbehörden bestehen laut einer heise online vorliegenden Antwort des Innenressorts auf einen Fragenkatalog des Bundesjustizministeriums in Europa bereits in den Ländern Rumänien, Zypern, Lettland und Spanien. (…) Die Regierungsbehörde vergisst auch nicht zu erwähnen, dass das FBI laut Presseberichten in den USA eine Software für eine Art Online-Razzia eingesetzt habe".*

27.08.2007 | Stefan Tomik (Frankfurter Allgemeine Zeitung/FAZ.net): Scheitert der Bundestrojaner am Virenscanner?

27.08.2007 | netzpolitik.org: Bundesinnenministerium beantwortet Fragen zur Online-Durchsuchung. *„Das Bundesjustizministerium hatte an das Bundesinnenministerium einen Fragenkatalog geschickt, der in dieser Datei beantwortet wird. Die SPD-Fraktion hatte an das Bundesinnenministerium einen Fragenkatalog geschickt, der in dieser Datei beantwortet wird."*

29.08.2007 | tagesschau.de: „Bundestrojaner" per Mail vom Finanzamt?

29.08.2007 | tagesschau.de: Anti-Viren-Spezialisten zu Späh-Programm-Plänen. „Der Bundestrojaner ist nicht vorstellbar"

28.08.2007 | Konrad Lischka (Spiegel Online): Bundes-Trojaner sind spähbereit *Das Bundeskriminalamt hat offenbar einen Computer-Trojaner fertiggestellt, der beliebige Rechner aus der Ferne durchsuchen kann.*

29.08.2007 | Konrad Lischka (Spiegel Online): Experten nehmen Bundes-Trojaner auseinander

06.09.2007 |c't: Von Datenschutz und Schäuble-Katalog: Terrorbekämpfung, TK-Überwachung, Online-Durchsuchung (alle Artikel, Linksammlung)

06.09.2007 | Mirjam Hauck (sueddeutsche.de): Brieftauben im Netz. *„So sollen amerikanische Behörden Spähprogramme auf den Rechnern der mutmaßlichen Terroristen platziert haben. Diese Informationen will das BKA auf Nachfrage weder ‚bestätigen noch dementieren'."*

12.09.2007 | Milos Vec (Frankfurter Allgemeine Zeitung/FAZ.net): „Heimat ist, wo meine Festplatte liegt. *„Dass die heimliche Plazierung solcher Programme nur über das Internet oder E-Mails gehen kann, ist auch dem Laien plausibel, und die Redewendung vom ‚Bundestrojaner' benennt klar das Täuschende, das hinzukommen muss. Doch auch der in der Datenwiese wühlende Maulwurf sieht sich vor Hürden wie Firewalls, Virenabwehrprogramme und ungewöhnliche Betriebssysteme gestellt, die von ihm umgangen werden müssten."*

14.09.2007 | Kai Biermann (Die Zeit): Polizei im Anti-Terrorkampf (über das BKA-Gesetz)

17.09.2007 | Focus 38 (2007): Gefesselter Bundestrojaner

04.10.2007 | heise.de: Gutachter bezweifeln Durchführbarkeit von heimlichen Online-Durchsuchungen

06.10.2007 | Spiegel Online: Bayerisches LKA und Zollfahnder spähen Rechner aus. *„Der Zollfahndungsdienst hat in zwei Fällen auf private Festplatten zugegriffen. Das geht aus einer Antwort der Bundesregierung auf eine Anfrage der FDP-Abgeordneten Gisela Piltz hervor, die dem SPIEGEL vorliegt. Allerdings geschieht dies nicht, um die Festplatten der Verdächtigen auszulesen, sondern um ihre verschlüsselten Internet-Telefonate zu überwachen."*

07.10.2007 | Tagesschau.de: Behörde bestreitet Einsatz von

Trojanern . LKA belauscht Internet-Telefonate

08.10.2007 | Christian Rath (taz): Behörden spähen Privatcomputer aus

09.10.2007 | Stefan Tomik (Frankfurter Allgemeine Zeitung/FAZ.net): Die Angst vorm Bundestrojaner. *„Die Gefahr aus dem Internet nimmt zu. Immer mehr Computeranwender geraten in die Fänge Krimineller, die Passwörter und Zugangsdaten ausspionieren, um damit zum Beispiel Bankkonten abzuräumen. (…) Technisch funktionieren solche Angriffe auf die gleiche Weise wie die geplante Online-Durchsuchung von Computern durch das Bundeskriminalamt (BKA).“*

10.10.2007 | Netzeitung: Verfassungsrichter von NRW-Gesetz verwirrt. *„In Karlsruhe stiftete der juristischer Vertreter des Landes, Dirk Heckmann, nun am Mittwoch Verwirrung. In dem Verfassungsschutzgesetz habe der Gesetzgeber nur die Erhebung von Kommunikationsdaten gemeint, nicht das Kopieren sämtlicher gespeicherten Informationen. ‚Es geht hier nicht um das Auslesen des gesamten Festplatteninhalts‘, so Heckmann.“*

10.10.2007 | Stefan Tomik (Frankfurter Allgemeine Zeitung/FAZ.net): Alles nicht so gemeint? *„Die monatelange Diskussion über einen Bundestrojaner habe „Assoziationen geweckt“, die keineswegs jene Maßnahmen beträfen, die die Landesregierung im Sinn gehabt hätte. (…) Heckmann erläuterte ausführlich jenen Passus im Verfassungsschutzgesetz, der ‚heimliches Beobachten und sonstiges Aufklären im Internet‘ betrifft. Darunter falle etwa die Teilnahme an Internetforen unter falschem Namen. Von einer Durchsuchung von Festplatten war da keine Rede mehr.“*

10.10.2007 | Hartmut Kistenfeger (Focus Online): Verfassungsgericht – Wenig Chancen für Online-Razzien

12.10.007 | Burkhard Schröder (Telepolis): Von Magischen Laternen und Bundestrojanern

17.10.2007 | heise.de: Österreich will heimliche Online-Durchsuchung 2008 einführen

11.11.2007 | taz: Die Gedanken bleiben frei. *„Ulrich Hebenstreit, Ermittlungsrichter am Bundesgerichtshof (BGH), hielt dem entgegen, dass die Polizei an solche Informationen ja durchaus herankommen könne. Computer dürften schon heute beschlagnahmt und ausgewertet werden. ‚Es muss eben offen passieren und nicht heimlich, das ist der gravierende Unterschied', betonte Hebenstreit, der im letzten November als erster Richter eine heimliche Computerausspähung nicht genehmigte und auf das Fehlen einer gesetzlichen Grundlage hinwies. Ziercke legt aber gerade Wert auf den heimlichen Blick in den Computer".*

17.10.2007 | Ö1 Inforadio: Koalition einig über Online-Fahndung. *„Vor allem der Innenminister verspricht sich vor von der Online-Durchsuchung besondere Fahndungserfolge, kann doch durch Trojaner, also spezielle Computerprogramme, künftig auf die Festplatte, also auch auf alte Daten zugegriffen werden. Bis dahin wird es allerdings noch ein bisschen dauern. Denn zuerst soll eine Expertengruppe, so Platter, alle technischen und gesetzlichen Details klären. Spätestens im Herbst 2008 soll dann die Online-Durchsuchung erstmals in Österreich möglich sein."*

14.11.2007 | heise.de: Polit-Posse um heimliche Online-Durchsuchungen unter Schily. *„Diwell habe ihm auf seine briefliche Ladung geantwortet, dass er sich außer Stande sehe, zu dem Thema vor den Abgeordneten zu sprechen. Der Staatssekretär hatte zuvor zum Ausdruck gebracht, die Tragweite der von ihm abgesegneten Formulierungen nicht erkannt zu haben. Seiner Einschätzung nach sei damit keine Lizenz für Online-Razzien verknüpft gewesen. Er habe geglaubt, dass es nur um die Beobachtung von abgeschotteten Internet-Foren gehe."*

15.11.2007 | heise.de: BKA-Chef: Zur Online-Durchsuchung gibt

es keine Alternative

23.11.2007 | heise.de: BKA-Tagung: Brieftauben verschlüsseln nicht. *„In der abschließenden Pressekonferenz erklärte Ziercke, dass Österreich, die Schweiz und Spanien die Länder sind, die die Technik der Online-Durchsuchung bereits umgesetzt hätten. Zumindest in Bezug auf Spanien gibt es für diese Aussage von dortigen Juristen keine Bestätigung, wie es auf der Bochumer Tagung zur Online-Durchsuchung bekannt wurde. Unter Verweis auf die europäische Dimension der Vorratsdatenspeicherung erklärte Ziercke, dass alle Länder schon erkannt haben, dass man handeln müsse. Bei zwei konkreten Anlässen habe man die Online-Durchsuchung benötigt.“*

07.12.2007 | heise.de: Bundesanwalt: Online-Razzien laufen ins Leere

25.12.2007 | Focus: Ermittler warnen vor Verzicht auf Online-Razzia

05.01.2008 | Focus Online: Verfassungsschützer installierten ‚Bundestrojaner‘ auf dem Rechner des Berliner Islamisten Reda Seyam. *„Technische Unterstützung für den Spähangriff holte sich der Inlandsgeheimdienst laut FOCUS bei Kollegen des Bundesnachrichtendienstes (BND), Spezialisten auf dem Gebiet der Online-Durchsuchung. Allein in den vergangenen beiden Jahren durchsuchten BND-Agenten die Computer von etwa 60 Zielpersonen im Ausland.“*

07.01.2008 | Focus/Focus Online: Verfassungsschützer installierten ‚Bundestrojaner‘ auf dem Rechner des Berliner Islamisten Reda Seyam. *„Technische Unterstützung für den Spähangriff holte sich der Inlandsgeheimdienst laut FOCUS bei Kollegen des Bundesnachrichtendienstes (BND), Spezialisten auf dem Gebiet der Online-Durchsuchung. Allein in den vergangenen beiden Jahren durchsuchten BND-Agenten die Computer von etwa 60 Zielpersonen im Ausland.“*

28.01.2008 | Burkhard Schröder (Telepolis): Großer Online-

Lauschangriff?