August Hanning | Annette Ramelsberger

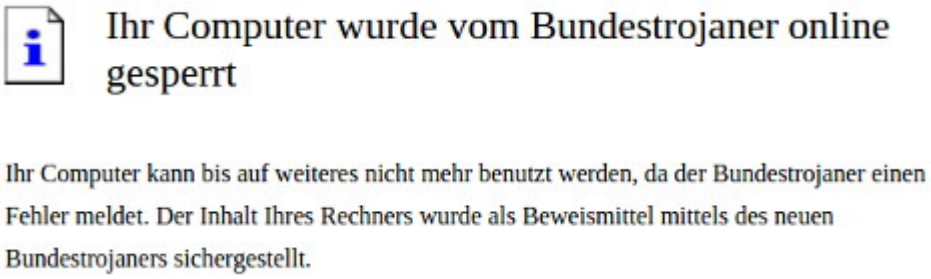
Im Wikipedia Artikel über Staatssekretär August Hanning fiel mir ein Link auf: „Annette Ramelsberger: Deckname Offenheit. In: Süddeutsche Zeitung. 6. Oktober 2004.“ Das betreffende Elaborat ist ein völlig unkritischer Jubel-Artikel: „Wie der Chef des Bundesnachrichtendienstes seine Behörde umkrempelt.“ – „Ein Mensch, der bis in die Fingerspitzen professionell agiert und der sich genau überlegt, wann er sich Gefühle erlaubt.“ – „Von Hannings Rückgrat erzählen seine Kollegen.“

Und dann muss ich noch einmal den Vorspann des Artikels in der Süddeutschen vom 17.12.2006 lesen, der den „Bundestrojaner-Hoax“ in die Welt gesetzt hat: „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.“ Die Autorin diesen Unfugs ist Annette Ramelsberger – genau die, die auch die Halleluja-Orgie über Hanning geschrieben hat.

Jetzt darf man drei Mal raten, wer der Informant Ramelsbergers dafür war, dass das BKA angeblich schon unsere Rechner durchsuchen kann…

Nachtrag 30.12. Dazu passt: „Redakteure würden sich gebauchpinselt fühlen, wenn ihnen Vertreter der Sicherheitsbehörden hin und wieder Informationsbröckchen zuwerfen, und sich diese „Quellen“ nicht verbauen wollen.“

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.

Embedded Journalism

Telepolis: „Wie der BND die deutschen Medien steuerte“. – „Geheimdienstexperte Erich Schmidt-Eenboom über Verbindungen der geheimen Dienste, die bis in die Chefredaktionen der größten deutschen Medien reichen“ Der Artikel wird aber nichts nützen.

Interessant ist, dass meine Vermutung über die Ramelsberger von der „Süddeutschen“ geteilt wird. Da sind wir dann wieder bei der „Online-Durchsuchung.“

Nie wieder in die USA

Wired: „The agents confiscated his laptop computer, a thumb drive and a digital camera. ICE held onto the equipment for 49 days – longer than the 30 days allowed in regulations – finally returning it only when the ACLU of Massachusetts intervened on his behalf with a letter.

Under the ‚border search exception, of United States criminal law, international travelers can be searched without a warrant as they enter the U.S..“

Ich frage mich, wie das die deutschen Korrespondenten machen, die in die USA reisen? Wiseo hört man nichts davon? Und wieso haben die deutschen Medien über das Thema nicht berichtet? Werden die alle durchgelassen, weil deutsche Medien Interviews autorisieren lassen und deshalb pe default harmlos sind? Oder zeigen die alle bereitwillig Ihre Rechner vor mit den Worten „jawoll, geliebte Obrigkeit“ auf den Lippen?

Die *American Civil Liberties Union (ACLU)* von Massachusetts, von der *Wired* die Story wohl hat, berichtet über diese Fälle noch detaillierter:
The government searched House's electronics for 183 keywords, turning up more than 26,000 potentially responsive

„files/objects.“ But even the government’s own invasive analysis of House’s information concluded that „no data was found that constituted evidence of a crime (and would justify ICE’s seizure of the materials).“

Das Ministerium für Innere Sicherheit der Vereinigten Staaten (United States Department of Homeland Security) arbeitet also mit dem Justizministerium zusammen, beschlagnahmt Rechner politischer Aktivisten und sucht darauf. Nein, sie löschen sogar die Daten: „the government has agreed to destroy all data it obtained from his laptop and other electronics when he entered the U.S. after a vacation“.

Man kann also davon ausgehen, dass man bei der Einreise in die USA alle sichtbaren Truecrypt-Container auf seinen Rechnern löschen muss. Ich habe ja schon 1979 nur ein begrenztes Visum in die USA erhalten im Gegensatz zu allen anderen, die ich kannte, die schon mal dort waren. Die haben mich also schon seit den siebziger Jahre in der Kartei.

Das wird hier auch noch so kommen – die ~~Klassenkämpfe~~ sozialen Spannungen werden hier auch zunehmen. Ich werde das wohl noch erleben. Mein Rechner wurde illegal über zwei jahre lang konfisziert, und es hat auch kaum jemanden interessiert (außer Heise), obwohl das Gericht, das mich endlich freigesprochen hatte, sogar ausdrücklich „rechtsstaatswidrige Weise“ ins Urteil schrieb. Hier gibt es eben keine *ACLU*, auf die man in einem solchen Fall bauen könnte.

Was sagen unsere Verschwörungstheoretiker von der „Online“-Durchsuchung eigentlich dazu? Warum machen die das in den USA so umständlich?

Annette Ramelsberger (Süddeutsche 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.“

Warum also Rechner beschlagnahmen, wenn das (angeblich) auch so geht?

Publikumsbeschimpfung

The Dissenter (via Fefe) lässt Gleen Greenwald ausführlich zu Wort kommen:
Another document that I probably shouldn’t share since it’s not published but I am going to share it with you anyway—and this one’s coming soon but you’re getting a little preview—It talks about how a brand new technology enables the National Security Agency to redirect into its repositories one billion cell phone calls every single day, one billion cell phone calls every single day.

What we are really talking about here is a globalized system that prevents any form of electronic communication from taking place without its being stored and monitored by the National

Security Agency.

Jetzt vergleichen wir die Krokodilstränen unserer politischen Kaste, von den US-Amerikanern ausgespäht zu werden, mit dem, was sie seit 2006 zum Thema „Online-Durchsuchung“ von sich gegeben haben. Was für eine heuchlerische, verlogene Bande! Das gilt auch für viele Journalisten. Mein hanebüchenstes Lieblingszitat (weil es Unfug ist) von 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.

Wenn die NSA und der englische Geheimdienst die elektronische Kommunikation in Deutschland komplett belauschen, welche Konsequenzen ziehen wir daraus? Keine? Wie viele Journalisten in Deutschland verschlüsseln ihre E-Mails? Mehr als hundert? Weniger? Was muss noch passieren, dass die sich vernünftig verhalten? Ich habe bei zahlreichen Redaktionen angefragt, was die zum Thema zu tun gedenken, von den meisten bekam ich gar keine Antwort.

Und wenn hier einer der wohlwollenden Leserinnen und geneigten Leser meint, mir in Zukunft eine unverschlüsselte E-Mail zu schicken – VERGESST ES! Bringt Euch das gefälligst SOFORT bei und verhaltet Euch wie rational denkende Menschen, sonst beschimpfe ich Euch als Pappnasen oder belege Euch mit noch schlimmeren Ausdrücken oder schicke Euch zum Psychologen oder Völkerkundler, um mir erklären zu lassen, warum erwachsene Menschen sich dermaßen bescheuert verhalten.

Ich werde jeden, der mir in Zukunft eine unverschlüsselte E-Mail schickt, als Wähler Angela Merkels oder Bosbach-Groupie abheften. Irgendwo müssen die doch sein. In meinem so genannten sozialen Umfeld gibt es niemanden, der CDU oder FDP

wählt. Irgendwo müssen diese Ignoranten ja frei herumlaufen.

Update: Aufruf zur Datenspende!

Honi soit qui mal y pense – unter Freibeutern und ihren JournalistenfreundInnen

„Im Mainzer Landtag haben SPD und Grüne gegen das von der CDU eingebrachte Misstrauensvotum gestimmt“, schreibt das ehemalige Nachrichtenmagazin.

Bevor wir weitermachen, übersetzen wir den holprigen Satz in gutes Deutsch. Wer tat was? SPD und Grüne taten etwas. Warum steht der Ort, an dem sie es taten, vorn und lenkt die Leser vom Wesentlichen ab. „Auf der Toilette verrichtete er sein Geschäft“? Wer redet so?

SPD und Grüne stimmten gegen…. halt: Warum kommt jetzt der Einschub „das von der CDU eingebrachte“? Weil der schludrige Schreiber gern alle Informationen in einen Satz packen wollte, damit die faulen Leser nicht mehr zur Kenntnis nehmen müssen als die erste Zeile?

„Gegen ein Misstrauensvotum stimmen“ ist auch nicht verständlich und hört sich an die „Verringerung der Erhöhung“ oder „der Anstieg der Arbeitslosigkeit verlangsamt sich“, um eine schlechte Nachricht als eine gute zu verkaufen.

SPD und Grüne sprachen Beck ihr Vertrauen aus. Sie stimmten gegen einen Antrag der CDU, der dem rheinland-pfälzischen Ministerpräsidenten das Misstrauen aussprechen sollte. Dass die Angelegenheit in Mainz stattfand und nicht in Nairobi, ist

klar und kann also weggelassen werden.

„Vertrauen aussprechen“ ist Blähdeutsch. Sie vertrauen ihm (richtig, taz!), obwohl er eine unfähige Pappnase ist. Er sprach ihr eine Begrüßung aus? Auch wieder Quatsch, aber wir haben uns an schlechtes Deutsch gewöhnt.

Die CDU wollte den rheinland-pfälzischen Ministerpräsidenten stürzen. SPD und Grüne vertrauen Beck aber und schmetterten jetzt das Misstrauensvotum ab.

Ich geb’s auf. Gutes Deutsch – schweres Deutsch. Vielleicht sollten doch besser die sprachbegabten Leserinnen und die des guten Deutschen kundigen Leser ran.

Zurück zu Beck:
Die Wörter „man“ und „es“ statt „ich“ verwendete Beck anschließend mehrfach bei der Beschreibung all jener Fehler, die nun zur Zahlungsunfähigkeit der zu 90 Prozent landeseigenen Nürburgring GmbH und dem Verlust von womöglich mehr als 200 Millionen Euro Steuergeldern führte. (FAZ)

Das Projekt Nürburgring 2009, in das rund 350 Millionen Euro aus Steuergeldern flossen, führte im Sommer 2009 zum Rücktritt des rheinland-pfälzischen Finanzministers und Aufsichtsratschef der Nürburgring GmbH, Ingolf Deubel [SPD] sowie Anfang Dezember 2009 zur Entlassung des Hauptgeschäftsführers der Nürburgring GmbH, Dr. Walter Kafitz. [Jahresgehalt bei 300.000 Euro] (Wikipedia)

Da die Medien ja noch nicht einmal den Versuch machen, mich darüber zu informieren, warum die Grünen den Versager Beck unterstützen, muss ich eigenhändig ein wenig recherieren.

PR-Artikel über Kafitz wie auf motorsport-total.com zeigen, wie versaut und verludert die mediale Berichterstattung über das Thema ist. *„Hier fällt es natürlich leicht, die nötige Leidenschaft zu entwickeln“, beschreibt Kafitz seinen Job als Hauptgeschäftsführer der Nürburgring GmbH und fügt schmunzelnd*

an: „Es ist schon ein anspruchsvoller Traumjob für mich.“

Exkurs: Bei anderen Themen ist es ja ähnlich. Annette Ramelsberger lobhudelt in der Süddeutschen (06.10.2004) über August Hanning, den Chef des Bundesnachrichtendienstes und glühenden Verfechter von „Online-Durchsuchungen“, dass es nur so schleimt („sie loben ihn alle“). Und einige Zeit später verbreitet sie dann den Hoax: „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.“ Das riecht für mich meilenweit danach, als wäre hier von den richtigen Leuten die richtigen Leute gebrieft worden, um Überwachungs-Propaganda in Medien unterzubringen. Honi soit qui mal y pense.

Ich schweife ab. Warum unterstützen die Grünen Beck? Drei grüne Minister hat das akuelle Kabinett in Rheinland-Pfalz. Es geht nicht um Inhalte, sondern darum, ob jemand seinen gut bezahlten Job verliert. Falls Neuwahlen in Rheinland-Pfalz angesetzt würden, könnten die Grünen sich nicht sicher sein, ob sie ihren warmen eurogefüllten Sessel behalten könnten.

In Berlin ist es ja auch nicht anders. Fragen wir meinen Lieblingskollegen Mathew D. Rose. („An Rose nervt, dass er jeden erwähnten Politiker als „Freibeuter“ bezeichnet“ – ja, liebe taz, aber er hat vollkommen recht: „Rose wundert sich, dass scheinbar kein Berliner Journalist die aktuellen Korruptionsskandale verfolgt“ – nein, nicht „scheinbar“ – sie tun es nicht!)

Unter Finanzsenator Elmar Pieroth (CDU) stieg die Verschuldung, laut Rose, in nur einer Legislaturperiode um 150 Prozent auf rund 25 Milliarden. Das war 1996. Heute sind „wir“ bei über 60 Milliarden Euro. Und zwischendurch wurden städtische Firmen wie Wasserbetriebe, Gasag und Bewag verkauft. Übrigens unter der als Sparkommisarin angetretenen

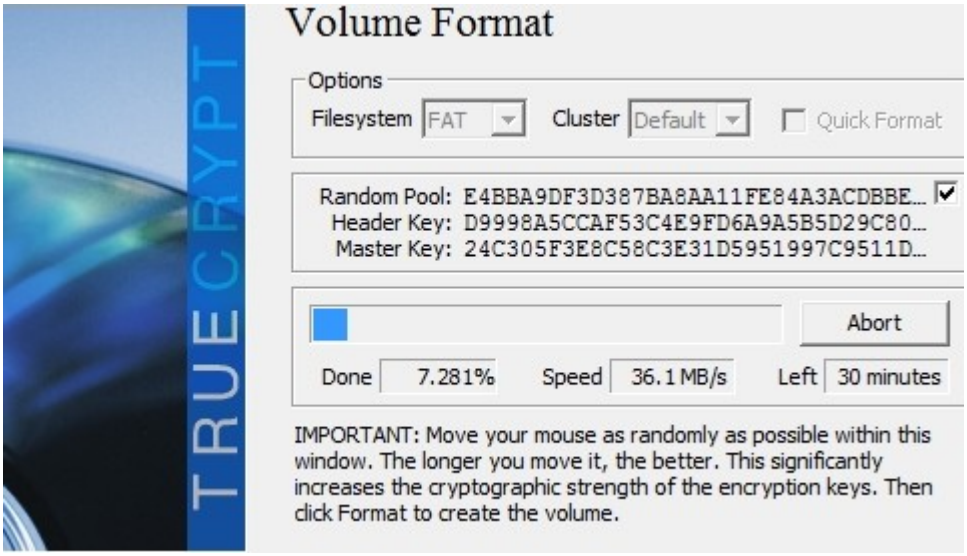
SPD-Frau Fugmann-Heesing (Schuldensteigerung in ihrer Amtszeit: „nur“ 40 Prozent).

Und was wählen die Leute? SPD und CDU.

Ich schrieb hier: „Mathew D. Rose, der den Berliner Bankenskandal fast im Alleingang aufdeckte, prägte den Lehrsatz, dass sich alle Probleme investigativer Recherche lösen ließen, wenn man nur zwei Fragen korrekt beantwortete: Wo kommt die ‘Kohle’ her? Wo geht sie hin?“

Wenn die Kohle in die Taschen der Grünen fließt, machen auch die jede Schweinerei mit.

Meine Rechner sind besenrein!



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

bei mir ist alles digital verrammelt und verriegelt.

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

Jetzt warte ich auf eine „Online-Durchsuchung." Mein Lieblingszitat: „Den meisten Computernutzern ist es nicht klar: Aber wenn sie im Internet surfen, können Verfassungsschützer oder Polizei online bei ihnen zu Hause auf die Festplatte zugreifen und nachschauen, ob sie strafbare Inhalte dort lagern – zum Beispiel Kinderpornographie oder auch Anleitungen zum Bombenbau."

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

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

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

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

„Mutmaßlich über verseuchte USB-Sticks gelangte er in

iranische Atomanlagen.“ Mutmaßlich? Seit wann verbeiten Journalisten Mutmaßungen und verschweigen sogar die Quelle der Gerüchte? Stand es in der Bild-Zeitung?

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

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

„Er will überdies nicht ausschließen, dass hinter vielen der aktuellen Hackerattacken heute Regierungen stecken.“ Ich will nicht ausschließen, dass ich mich bewerbe, Vorsitzender der Piratenpartei zu werden. Ich will auch nicht ausschließen, dass der Kaiser nackt ist und er gar keine neuen Kleider trägt.

„In Zukunft allerdings müssen wir mit Cyber-Attacken auf Fabriken, Flugzeuge und Kraftwerke rechnen.“ Nicht nur das: Auch mit Attacken auf harmlose kleine Privatrechner, die mit gaaaaanz vielen „Bundestrojanern“ nur so gespickt werden. Wie die Kollegin Annette Ramelsberger schon vor vielen Jahren schrieb: „Den meisten Computernutzern ist es nicht klar: Aber wenn sie im Internet surfen, können Verfassungsschützer oder Polizei online bei ihnen zu Hause auf die Festplatte zugreifen und nachschauen, ob sie strafbare Inhalte dort lagern – zum Beispiel Kinderpornographie oder auch Anleitungen zum Bombenbau.“

„Kasperski zum SPIEGEL: ‚Alles, was wir erreichen können ist,

zu verhindern, dass da draußen alles außer Kontrolle gerät.'“ Ja, genau! Kauft mehr „Anti-Viren-Programme“ von Kapersky! Das Ende ist nahe!

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!

Bayerisches Bespitzeln

Diese Pressemeldung der bayerischen Staatskanzlei interessierte mich *(Ich habe durch Spiegel Offline und Focus*

Offline davon erfahren, aber die verlinken das weltwelte Internet nicht, also verlinke ich sie auch nicht…) „Der Leiter des Büros des Ministerpräsidenten wurde wegen eines Dienstvergehens von seinen Aufgaben entbunden. Ein Disziplinarverfahren wird eingeleitet.“

„Leiter Büro Ministerpräsident“ lautet die Überschrift. Wollen die einem die Boolesche Algebra mit Google schon vorgeben oder ist der Genitiv in Bayern jetzt verboten?

Der abgelöste Herr heisst Zorzi, der Münchener Merkur schrieb vor zwei Jahren über ihn: „Die Zukunft von Landesgeschäftsführer Markus Zorzi (43), der als ranghöchster Mitarbeiter sogar im Parteipräsidium sitzt, ist offen. Zorzi hatte bisher die Aufsicht über die Strategie-Abteilung. Guttenberg sagt, Zorzi solle bleiben: „Ich würde auf ihn sehr, sehr ungern verzichten.“ Zorzi gehört zum CSU-Ortsverband Grafrath. Da steht Zorzi auch im Telefonbuch und da wohnt er auch.

By the way: Ich hatte mr in meinem Artikel Projekt Xanadu reloaded Gedanken gemacht, was geschähe, nähme man Online-Journalismus in Deutschland ernst. Diese „Gefahr“ droht bekanntlich nicht, da die Internet-Ausdrucker in der Medien die Zügel in der Hand und soviel Angst vor Links haben wie ein Schneemann vor der Sonne. Wenn aber eine bayerische Zeitung verrät, dass ein Mann eine öffentliche Funktion innehat, dann kann ja jedermann zum Telefonbuch greifen und ihn anrufen. Dann kann ich auch diese Nummer direkt verlinken, wie oben geschehen.

Die Münchener Abendzeitung platziert das bayerische Bespitzeln treffend direkt neben die Big-Brother-Brüste: „Markus Zorzi soll versucht haben, in den Dienstcomputer seines Nachfolgers einzudringen“. Aha. Eine private Online-Durchsuchung also? Zorzi wollte den Remote-Access-Zugriff? Wenn diese Offliner in den Medien auch nur einen Hauch von Ahnung hätten, wüsste man, was gemeint ist.

Die Abendzeitung: „..er habe in den Dienst-Computer in der CSU-Zentrale eindringen wollen, um auf das E-Mail-Postfach von Bernhard Schwab zuzugreifen.“ Wie denn? Was denn? Sind die nicht geschützt? Liegen die dienstlichen E-Mails dort unverschlüsselt herum?

Das mögliche Motiv: „Zorzi, der als braver Beamter und ausgezeichneter Stratege galt, der seine eigenen Interessen nie in den Vordergrund stellte, war sich mit dem Duo Neumeyer/Schwab noch nie grün. Er misstraute ihnen. Offensichtlich wollte er nun aus der Staatskanzlei kontrollieren, was Schwab in der CSU-Leitung so treibt und versuchte deshalb in den Computer der Partei-Spitze zu kommen.“ *(Das Handelsblatt schreibt über Zorzi: „dessen Arbeit in der Partei umstritten war“. Ach ja? Es kommt also immer darauf an, welcher Spezi einen gerade mit welchen Interessen brieft, liebe Kollegen? Ich kann mich vage daran erinnern, dass es nicht die Aufgabe von Journalisten ist, Gerüchte und Intrigen zu verbreiten. Und ein faktenfreies „der ist umstritten“ ist unstrittig diffamierend. Ich bin auch umstritten und tue alles, damit es so bleibt.)*

„In den Computer zu kommen“ – geht es auch ein wenig genauer? So einfach ist das nicht. Er wird ja wohl kaum die Batterien des Rechner versucht haben auszubauen, um das BIOS-Passwort zu verflüchtigen. Oder hat er nur versuchsweise ein Paar Passworte in die Tasten gehämmert, um den Webmail-Account Schwabs zu knacken – Susi, Mausi, Franz-Josef-Strauss, was einem CSU-Mann so als Passwort einfällt?

Die Süddeutsche ist etwas genauer, aber nicht genau genug: „Es war ein Sicherheitscheck in der CSU-Parteizentrale, der alles auslöste. Dabei wurde in der vergangenen Woche klar, dass im Februar jemand von außen in den Computer des neuen CSU-Landesgeschäftsführers Bernhard Schwab eingedrungen war. Schnell war auch klar: Dieser Jemand saß in der Staatskanzlei.“

Interessant. Man kann also *im nachhinein* feststellen, wer was an den Rechnern der CSU gemacht hat? Und „von außen“ meint ja wohl nicht, dass Zorzi zu einer real gar nicht möglichen „Online-Durchsuchung“ fähig gewesen wäre.

Was also ist eigentlich passiert? Das sollten ernst zu nehmende Journalisten herausfinden. Ich tippe übrigens auf Keylogger („Sicherheitscheck“), die auf den CSU-Computern installiert sind. Anders kann ich mir die rätselhaften Formulierungen nicht erklären.

Die Süddeutsche ist jedoch dafür bekannt, dass sie zum Thema Computer auch gern lächerliche Verschwörungstheorien verbreitet wie Annette Ramelsberger vor vier Jahren: „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.“

Vielleicht hat Zorzi das gelesen und geglaubt und wollte das versuchen. Selbst schuld.

Keinen Bedarf für des Kaisers neue Kleider

Wolfgang Bosbach hat sich zur Entenfrage wieder einmal geäußert. Es ist ihm gelungen, die Flughöhe zu halten – also so dicht wie möglich über dem Wasser, das niedrigstmögliche Niveau. Ein Satz jedoch ist geradezu genial, wenn nicht sogar wahr: „gab es wohl bis zur Stunde in der polizeilichen Praxis keinen Anwendungsfall, sodass wir zunächst einmal Erfahrungen

mit diesem neuen Ermittlungsinstrument abwarten sollten“.

Wie meinen? Sollte er dieses Buch gelesen haben? Bosbach wollte ja sogar das Grundgesetz ändern…By the way: lest Ramelsberger in der Süddeutschen! ich lasse es mir immr wieder auf der Zunge zergehen: „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.“ SIE sind schon drin!

Zur Erinerung: Bosbach sprach vor zwei Jahren in der Sendung „People and Politics“ (09.07.2007, ab Min. 6.00) über Online-Durchsuchungen. Die Pointe kommt am Schluss. Bosbach lästerte über die, die behaupten, so etwas gebe es gar nicht oder es sei technisch unmöglich. Bosbach, lächelnd: „Aber das wird schon gemacht.““. So. So ein tolles Ermittlungsinstrument, da alle dringend brauchten – und jetzt nutzt es die Polizei nicht?

Um es kurz zu machen: Die Erde ist eine Kugel, keine Scheibe. Die Amerikaner sind auf dem Mond gelandet. Der Terroranschlag am 11. September ging auf das Konto von Al Kaida. Den Hufeisenplan gibt es aber schon weniger, und eine real existierende Online-Durchsuchung hat es nicht gegeben und wird es so, wie es sich Klein Wolf..äh….Fritzchen das vorstellt, auch nie geben..

Bund Heimattreuer

Vereinsverbieter oder: Tai chi gegen Rechts

Ich bitte die wohlwollenden Stammleserinnen und geneigten Stammleser dieses kleinen libertären und anarchodyndikalistischfreundlichen Blogs, einen neuen Aktenordner für die sofortige ungelesene Ablage anzulegen. Alle Meldungen deutscher Medien, die den Begriff „Verbot“ in politischem Zusammenhang enthalten, sind ab sofort nicht mehr zu beachten und in die Tonne zu treten, weil eine rationale Diskussion nicht möglich ist. Ich hatte mich hier schon über den ärgerlichen Telepolis-Artikel „Schonfrist für den Nazi-Nachwuchs“ echauffiert, der – wie viele andere zum Thema auch – suggeriert, der Staat müsse doch gegen das Böse gefälligst härter durchgreifen, auch bekannt als *melden, durchführen und verbieten,* wobei die wesentlichen Tuwörter der deutschen Leitkultur umfassend beschrieben wären.

Aktuell geht es wieder um den politisch kackbraunen Verein „“Bund Heimattreuer Jugend“, dessen Verbot laut tagesschau offenbar bevorstehen soll. Derartige Anlässe sind immer eine willkommende Gelegenheit für Hardliner jeglicher politischer Couleur, die urdeutsche Tugend des Verbietens herauszukehren

und sich damit als potenzieller Innenminister anzubieten, wie hier der sattsam auch als „Innenexperte“ bekannte Sebastian Edathy, der schon mal in prophetischer Attitude für die nächste große Koalition den Schäuble-Imitator und -nachfolger gibt. „Ein HDJ-Verbot sei überfällig, betonte Edathy.“ Aber klar. Ob das politisch sinnig und effektiv ist, interessiert niemanden. Es wird noch nicht einmal mehr darüber gestritten, was ein untrügliches Zeichen dafür ist, dass wir es nicht mit Politik, sondern mit bloßer Moraltheologie der ideologisch stromlinienförmigen Mainstream-Medien zu tun haben.

Es findet sich auch unter den zahlreichen Pseudoliberalen im Bundestag niemand (in Worten: niemanden), der den Mut aufbringt, den Sinn des hektischen Aktivismus des staatlichen Antifaschismus zu bezweifeln (sorry für die Genitiv-Girlande). Als hätte es den achtjährigen lichterkettentragenden und daher völlig erfolglosen amtlichen „Kampf gegen Rechts“ nicht gegeben, wird weitergemacht wie bisher. Böse Nazi-Vereine werden durch die Dauerskandal-Truppe Verfassungsschutz den Medien *gemeldet*, die ein *Verbot* fordern, welchselbiges dann *durchgeführt* wird. Ich finde nicht nur Nazis zum Kotzen, sondern auch diese verlogenen „Anti-Nazis“.

„Die Durchsuchungen ’sollen uns Klarheit darüber verschaffen, ob sich die HDJ in aggressiv-kämpferischer Weise gegen die verfassungsmäßige Ordnung richtet oder ihre Tätigkeit den Strafgesetzen zuwiderläuft‘, sagte Innenstaatssekretär August Hanning.“ Die üblichen Verdächtigen. Blabla. Weich gefallen, Herr Hanning? „Am 1. Dezember 2005 wurde Hanning zum Staatssekretär im Bundesministerium des Innern ernannt. Er ist dort für Polizeiangelegenheiten, Angelegenheiten der Bundespolizei, Innere Sicherheit, Migration, Integration, Flüchtlinge, Europäische Harmonisierung sowie die Stabsstellen Krisenmanagement und BOS-Digitalfunk zuständig. Im Zusammenhang mit der Affäre um die Bespitzelung von Journalisten in den Jahren 1993 bis 1998 ist noch ungeklärt, ob auch Hanning von der vor seiner Amtszeit liegenden

teilweise rechtswidrigen Observation von Journalisten durch den BND zum Zwecke der Eigensicherung erfahren hat.“ Der rechte Mann am rechten Ort. Der Tagesschau wäre zu empfehlen, zumindest den Wikipedia-Eintrag zu Hanning zu verlinken, um die Leser in die Lage zu versetzen, mit welchen „Experten“ sie es zu tun haben. Aber die Tagesschau verweigert sich bekanntlich dem Online-Journalismus und setzt keine Links in berüchtigte Internet.

By the way: Hannig ist derjenige, über den die preisgekrönte Kollegin Annette Ramelsberger im Oktober 2004 ein bejubelndes Halleluja in der Süddeutschen verfasst hat („Sie loben ihn alle“). Nur wenige Monate danach erschien ihre mittlerweile berühmt-berüchtigte Falschmeldung, für die die „Sicherheitskreise“ sie offenbar ausführlich gebrieft und instrumentalisiert hatten, dass die Polizei und die Verfassungsschützer schon längt „drin“ in unseren Computern seien. Hony soit qui mal y pense.

Aber ich schweife ab. Auch Hannig tut, was man vom ihm erwartet, und sondert die bekannten Testbausteine ab: Der BHJ wende sich „in aggressiv-kämpferischer Weise gegen die verfassungsmäßige Ordnung“. Diese Formulierung hat das Bundesverfassungsgericht vorgeben als Voraussetzung für ein Verbot einer politischen Partei in Deutschland. Nur handelt es sich bei den kackbraunen „Freibund“ aka BHJ gar nicht um eine Partei, sondern um einen Verein, der viel leichter zu verbieten ist. Hanning hätte die schwere juristische Artillerei ruhig in der Garage lassen können.

Auch die Linke („Prüfung eines vereinsrechtlichen Ermittlungsverfahrens“) ist selbstredend nicht besser als die rechten Hardliner: „Die Linksfraktion betont, Ziel der HDJ sei die ideologische Einflussnahme auf Kinder und Jugendliche im Sinne der Verbreitung völkischer, rassistischer, nationalistischer und NS-verherrlichender Ansichten. Der Verein unterhalte zudem enge Kontakte zur NPD.“ Wie sagte schon Kaiser Wilhelm Zwo sinngemäß und völlig richtig über die

damalige Linke: „Ich kenne keine Parteien mehr, ich kenne nur noch deutsche Partei- und Vereinsverbieter“.

Übrigens: „Die Berliner Behörde teilte im Dezember 2007 auf Anfrage des Freibunds mit, dass die Verfassungsschutzberichte der Jahre 2006 und früher ‚keine Aussage (enthalten), dass der Freibund als rechtsextremistische Gruppierung angesehen wird.‘ Eine Aufnahme in den Berliner Verfassungsschutzbericht 2007 sei nicht beabsichtigt.“ Es handelt sich bei der gegenwärtigen Aktion gegen den kackbraunen Verein also wieder um populistische Umtriebe, die so sinnfrei sind wie Tai chi für Avatare (siehe Screenshot unten).

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?