Do not even think of

Geheimdienst-Nummer

Der Westen: „Die klassische Geheimdienst- Nummer ist denkbar“

> *Burkhard Schröder etwa, der in seinem ‚Online-Tagebuch, über Politik, Wissenschaft und Medien seinen Angaben nach investigativ berichtet, schreibt in einem Telepolis-Artikel: ‚Bei der Online-Untersuchung handelt es sich also um eine reine Wunschvorstellung und mitnichten um eine real existierende Methode.‘ So genannte Bundestrojaner seien noch nie angewendet worden.*

Das heisst *nicht*, sie sei nicht möglich, sondern nur, dass sie noch nicht praktiziert worden ist.

> *‚Zu sagen, Online-Durchsuchungen sind nicht möglich, ist*

> *Blödsinn‘, klärt Dr. Christoph Wegener, Spezialist im Bereich IT-Sicherheit an der Ruhr-Universität Bochum, auf. ‚Durchsuchungen sind tendenziell möglich‘, nennt jedoch im gleichen Satz schon das Problem: ‚Man kann sich davor schützen.‘ Das kann der Verdächtige also auch tun.*

Was denn nun? Sind sie möglich, wenn man sich schützen kann? Oder deswegen nicht?

Schlechte Karten für „Bundestrojaner“

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

Neues Grundrecht | Papier holt die große Keule raus

Das nordrhein-westfälische Verfassungsschutzgesetz ist nichtig. Online-Durchsuchungen bleiben verboten. Noch mehr: Papier beginnt seine Begründung mit dem Satz, das Bundesverfassungsgericht konstituiere ein neues **Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme**. Schlimmer hätte es für Schäuble nicht kommen können.
Update (10.30 Uhr) Papier erteilt indirekt auch der Vorratsdatenspeicherung eine Absage. Der große Rundumschlag – ein Sieg der Bürgerrechte auf ganzer Linie.
Update: Das Urteil ist online.

Avision AV363C Scanner zu verkaufen

Ich verkaufe meinen Avision AV363C Flachbett-Scanner (am besten Selbstabholer – ich verschicke notfalls auch). Er hat nur einen Parallel-Port, kein USB. Mit Linux habe ich ihn nicht zum Laufen bekommen. Er arbeitet aber makellos. Software habe ich nicht, für Windows kann man aber zum Beispiel kostenlos Grewe Scanner-Interface 3.0 benutzen.

Die Online-Durchsuchung

Burks proudly presents, hier exklusiv. Erscheint Anfang September 2008.

Ausreichend Sachverstand

Fragenkatalog der SPD-Bundestagsfraktion / AG Kultur und Medien / AG Neue Medien an den Bundesinnenminister, 22. August 2007:

> *Frage:Wer berät sachverständig die Sicherheitsbehörden und das BMI bei der Konfiguration von Online-Durchsuchungen?*

> *Antwort:Die Sicherheitsbehörden und das Bundesministerium des Innern verfügen grundsätzlich über genügenden Sachverstand.*

Das hatte ich noch nicht gelesen…. Dann kann ja nichts mehr schiefgehen.

Datenkrake Google, die 456ste

Golem.de (25.02.2007): „Google: IP-Adressen sind keine personenbezogenen Daten“. Noch einmal zum Mitschreiben: Google sagt, das *sei* so. Das stimmt aber nicht. „Fleischer machte deutlich, dass Googles Geschäftsmodell auf der Nutzung von personenbezogenen IP-Adressen basiert: „Wir müssen wissen, wer wonach fragt – andernfalls könnte unser Unternehmen nicht funktionieren“. Fleischer wurde sekundiert von Microsoft-Vertreter Thomas Nyrup, der darauf hinwies, dass „das Internet nicht wäre, was es ist, gäbe es die Werbung nicht“. Google bestätigte in der Anhörung, die Inhalte von über Google-Mail versandten E-Mails zu Werbezwecken zu analysieren.“

Sehr schön gesagt: Das Internet wäre nicht das, was es ist, gäbe es Microsoft nicht. Das Erde wäre nicht das, was sie wäre, gäbe es die Sonne nicht. Burks‘ Blog wäre nicht das, was es ist, gäbe es Burks nicht. By the way: Welcher Vollidiot verschickt unverschlüsselte E-Mails via Google-Mail? Auch lesen: Heise Newsticker: „Datenschützer stoppt das Speichern von IP-Adressen“.

Cold Boot Attacks on Encryption Keys

Es geht doch nichts über den physischen Zugriff auf einen Rechner, wenn man an die Daten herankommen will. Das Center for Information Technology Policy der Universität von Princeton hat jetzt bewiesen, dass die meisten Verschlüsselungssysteme, unter anderem auch Truecrypt, unter bestimmten Bedingungen unsicher sind: „Contrary to popular assumption, DRAMs used in most modern computers retain their contents for seconds to minutes after power is lost, even at operating temperatures and even if removed from a motherboard. Although DRAMs become less reliable when they are not refreshed, they are not immediately erased, and their contents persist sufficiently for malicious (or forensic) acquisition of usable full-system memory images.“

Die *Technology Review* hat ein ausführliches Interview dazu mit Edward W. Felten im Angebot – Felten ist Professor für Informatik an der Princeton University und hat die ausführliche Studie verfasst.

Worum geht es? Die DRAM-Speicherchips (für: Dynamic Random Access Memory) erinnern sich an bestimmte Daten, auch wenn der Rechner schon abgeschaltet wurde. Das kann man wieder sichtbar machen – also auch bestimmte Passworte und Schlüssel, die der Chip temporär speichert. Ein Angreifer msus also, soll die vorgeschlagene Methode funktionieren, den Rechner aus- und zeitnah wieder anschalten. Als Pointe haben die Forscher die Chips sogar mit Stickstoff abgekühlt. Dann dauert es noch länger, bis alle Daten nach dem Ausschalten des Computers verschwunden sind.

> *TR: Kann Ihre Methode tatsächlich jedes Festplattenverschlüsselungssystem knacken, das heute auf dem Markt ist?*
> *Felten: Alle, die wir getestet haben, darunter Microsoft BitLocker, Apple FileVault, dm-crypt unter Linux und TrueCrypt. Microsofts System ist in bestimmten Konfigurationen etwas sicherer, aber es sieht wohl so aus, als seien die meisten oder gar alle verfügbaren Festplatten-Verschlüsseler mit großer Wahrscheinlichkeit angreifbar.*

Fazit: Man muss zum Beispiel einen Laptop immer ausschalten,

der „Hibernations“- oder Stand-by-Modus nutzt überhaupt nichts, auch wenn die Festplatte verschlüsselt ist.

> *TR: Der physische Zugriff auf eine Maschine bleibt also immer ein Risiko.*
> *Felten: Ja. Zuvor dachte man aber eben, dass eine Festplattenverschlüsselung die Dateien auf einem Laptop schützt, selbst wenn dieser verloren oder gestohlen wurde. Unsere Ergebnisse zeigen nun, dass das nicht stimmt.*

Pact on the Self-discipline

Wie Heise berichtet, haben sich chinesische Websites zu einem „Chinese Pact on the Self-discipline on Visual-Audio Programs and Services of the Internet“ zusammengeschlossen. Auch die Nachrichtenagentur Xinhua will offenbar „nur noch ‚positive und gesunde‘ Inhalte verbreiten“. „In recent years, the Authorities have taken a series of measure to deal with pornographic and illegal activities on line, and many domestic websites have been closed down for involvement in illegal publications or services.“

So etwas haben wir in Deutschland schon. Es wäre ja noch schöner, wenn uns andere Länder zuvorkommen würden, wenn es um (Selbst)Kontrolle geht. Laut *Heise* geht es den Chinesen darum, „Gewalt, Pornographie, terroristische Inhalte und Werbung für Glücksspiel aus dem Web fernzuhalten.“ Aha. Im Usenet darf man das also weiter verbreiten.

Das hört sich doch gut gemeint an. Also werden sich zahlreiche Websites der Initiative freiwillig anschließen. Spontan haben das getan: burks.de, burksblog.de, spiggel.de, burkhard-schroeder.org, burkhard-schroeder.com, burkhard-schroeder.info, burkhardschroeder.de, qwertzuiopue.de und al-arabi.info. Diese Websites haben niemals das Böse *[bitte selbst ausfüllen]* in das Web [sic] gelassen und werden das auch weiterhin nicht tun (vgl. das positive und gesunde Foto oben).

Online-Durchsuchung | Chronologie

Ich habe im Rahmen einer größeren Recherche die Medienberichte über die “Online-Durchsuchung” zusammengefasst (Auswahl). Sehr lustig, wenn man den Quatsch vergleicht, der zum Thema geschrieben wurde.

Irrationale Ängste?

Interview mit Albrecht Ude über die Vorratsdatenspeicherung: „Haben Sie irrationale Ängste vor der Vorratsdatenspeicherung, Herr Ude?“

Öffnen Sie den E-Mail-Anhang!

Quelle: vorwärts, Ausgabe 10/2007, Seite 47

Online-Durchsuchung 1993

Focus (38/1993): „Nationales Netz. Unter Verwendung zentraler Mailboxen bauen Neonazis ein landesweites Computernetz auf“. – „Die System Operators und ihre Überwacher experimentieren mit immer neuen Programmen. Hetzer alias Tetzlaff: ‚Eine Entschlüsselung ist für Unbefugte praktisch nicht mehr möglich.‘ Doch die Verfassungsschutztechniker dringen in die Mailboxen ein. Zunehmend knacken sie auch Paßwörter, die den Zugriff Unbefugter stoppen sollen. Die Beute: Veranstaltungstips, Hinweise auf neue Bücher und Szeneschriften…(…) Bayerns Verfassungsschutz- Vizepräsident Volker Haag: ‚Dann kann die Planungszeit für extremistische Aktionen eventuell so verkürzt werden, daß uns kaum noch eine Möglichkeit zum Eingreifen bleibt.'“

Wie sich die Worte gleichen….

Bundestrojaner zu Bundeswürmern

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

Milan Vojnovic hat ein Papier dazu publiziert [„On the race of worms, alerts and patches“, with A. Ganesh, journal submission, 2006 (conf ver ACM WORM 05)], das aber schön älter ist. Bruce Schneier wettert gegen die Idee („Benevolent Worms“) an sich, was zu erwarten war und womit er sicher Recht hat. Er bezieht sich auf einen Artikel der New Scientist.com: „Friendly ‚worms‘ could spread software fixes“. „Milan Vojnović and colleagues from Microsoft Research in Cambridge, UK, want to make useful pieces of information such as software updates behave more like computer worms: spreading between computers instead of being downloaded from central servers. The research may also help defend against malicious types of

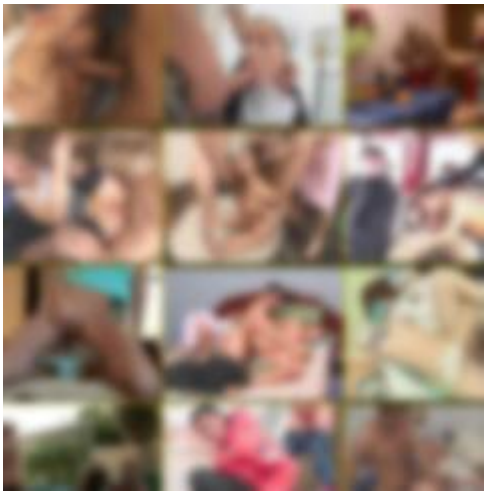
worm, the researchers say.“

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

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

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

Internet-Zensur



Heise hat die Liste der in Finnland zensierten Porno-Websites verlinkt. Sie stammt vom Bürgerrechtler Matti Nikki. „Doch seien die meisten Seiten auf dem finnischen Online-Index legale pornografische Angebote aus den USA oder EU-Ländern oder enthielten nicht einmal Pornografie, heißt es in einer Mitteilung der Electronic Frontier Foundation Finland (EFFI).“

Dennoch kann man eine größere Menge hochprozentirger alkoholischer Getränke verwetten, dass sich kein deutsches Medium (außer Heise) trauen wird, die URL-Sammlung Nikkis zu verlinken.

Ich habe meinen Tor-Button benutzt und mir einige dieser Seiten angesehen. Kinderpornografie im Sinne des Gesetzes habe ich nicht gefunden. Auch www.x-preteens.com enthält keine Kinderpornografie, obwohl man sich vorstellen kann, welche Klientel sich da herumtreibt.

Natürlich: …“die meisten ISP wären zur Kooperation bereit und würden kinderpornografische Angebote gezielt sperren“. Die Websites werden zum größten Teil in den USA gehostet, aber auch deutsche sind dabei.

Es handelt sich also um die gewohnte sinnfreie Hysterie der Zensur-Fans. „Die Bürgerrechtler befürchten, die Internetzensur könne sich ausweiten.“ Quod erat demonstrandum. Irgendein Anlass, den totalitären Überwachungsstaat einzuführen, wird sich schon finden lassen. Die üblichen verdächtigen Themen kennen wir schon auswendig: (Rechts)Extremismus, Terrorismus, Kinderpornografie. Meyer, übernehmen Sie!

Journalistische Recherche | Werkzeuge

Zwei Tage lang habe ich Kolleginnen und Kollegen gequält mit „Investigativer Recherche im Internet„. Der nächste Kurs findet übrigens Anfang Mai statt – die Nachfrage war überraschend groß.

Die Linksammlung journalistischer Recherche, die ich schon auf der Website von Berliner Journalisten zusammenstellte, habe ich jetzt auf Burks‘ Blog aktualisiert.

Rechtsextremisten: Propaganda per Computer

Baden-Baden, 11. April (ap). Rechtsextremisten benutzen offenbar das Computernetz „Internet“ mit Millionen Benutzern weltweit für ihre Propagandazwecke, berichtet das SWF-Fernsehmagazin „Report“. Seit einigen Wochen werde in großen Mengen Material US-amerikanischer Revisionisten eingespeist, die den systematischen Völkermord der Nazis leugnen, so etwa der „Leuchter-Report.“
Michael Rotert, Geschäftsführer der „Internet“-Servicefirma Xlink in Karlsruhe, erläuterte auf Anfrage, er halte es für wahrscheinlich, daß tatsächlich größere Mengen rechtsextremer Propaganda in das Computernetz eingespeist werde. Der Zugang zum Netz sei nicht zu kontrollieren, die Verbreitung des Materials nicht zu verhindern. „Wenn es eine Möglichkeit gäbe, würde ich sie unterbinden.“
(*Frankfurter Rundschau, 12.04.1994*)

Schmutz im Internet

Das Internet ist – wieder einmal – ins Visier des deutschen Gesetzgebers geraten. Allerlei Schmutz werde da verbreitet, bemerkte dieser Tage Bundesinnenminister