Ich denke nicht daran!

Barrierefreiheit im Internet: „Die Navigation ist ein besonders zentrales Element jeder Webseite, da sie benötigt wird, um überhaupt erst auf die Inhalte zugreifen zu können. Um so wichtiger ist es deshalb, dass sie in jedem Fall funktioniert – auch ohne CSS und JavaScript.“ Vgl. auch Aktiv gegen Diskriminierung.

Affinität zu Social Media und die fehlende Mobiloptimierung

B&#65533;roarbeiten von Mitgliederbetreuung und Korrespondenz bis zum Buchversand

VORAUSSETZUNGEN:
erste Erfahrungen beim Schreiben von Pressemitteilungen / Meldungen
sehr gute Englisch-Kenntnisse, m&#65533;glichst Russisch-Kenntnisse, Franz&#65533;sisch von Vorteil
Erfahrungen bei der Pflege von Websites mit CMS typo3 von Vorteil
Affinit&#65533;t zu Social Media von Vorteil

Das Praktikum wird mit 350 Euro monatlich verg&#65533;tet.

BEWERBUNG:
Motivation, Lebenslauf, wichtigste Zeugnisse und ggf. ausgew&#65533;hlte journalistische Arbeitsproben bitte in EINEM PDF-Dokument (max. 2 MB) an:

Reporter ohne Grenzen
Silke Ballweg / Christoph Dreyer,
Pressereferenten
bewerbung(at)reporter-ohne-grenzen.de

Lästern ist natürlich einfach. Ich sage immer: E-Mail-schreiben ist schwerer, als man denkt. Man stelle sich vor, die obigen Stellenanzeige wäre genau so in einer Tageszeitung erschienen. Die Leute hätten sich kaputtgelacht. Was mich aber besonders nervt, sind nicht Fehler, die jeder macht, sondern die Resistenz der übergroßen Mehrheit der Leute einzusehen, dass *sie* ein Problem haben, nicht ich.

Ich rede hier nicht über barrierefreies Webdesign. Das ist ein anderes Thema. Webdesigner sind bekanntlich die natürlichen Feinde des Surfers und haben zum Thema „Sicherheit“ ein

Verhältnis wie Klaus Störtebeker zum Handelsrecht. Nimm einem Webdesigner Javascript weg und er heult wie ein Baby, den man dem Schnuller vorenthält. Ausnahmen bestätigen die Regel, aber nur, wenn sie einem auch noch etwas verkaufen wollen:

E-Mails werden zunehmend auf mobilen Endgeräten wie Smartphones oder Tablets genutzt. Dies verlangt nach einer Optimierung der E-Mails für die kleineren Bildschirme – geringere Breite, verkürzte Inhalte, grössere Buttons usw. Laut der artegic Studie Mobile E-Mail Marketing 2012 kritisieren 31,6 Prozent der mobilen E-Mail Nutzer die mangelhafte Darstellung mobiler E-Mails. Für Empfänger mit Sehschwäche stellt die fehlende Mobiloptimierung sogar ein noch grösseres Hindernis dar.

(„Fehlende Mobiloptimierung" – das verdient den Tag „Deutsch des Grauens").

„Barrierefrei" heißt also: Jedes Ausgabegerät zeigt eine E-Mail korrekt an. Wenn die Sonderzeichen zerhauen sind, ist das nicht *mein* Problem, sondern das des Senders. Vermutlich hat man bei „Reporter ohne Grenzen" auch vom Ten-Standard oder ganz komischen Sachen noch nie etwas gehört. Aber der ist – zugegeben! – eher was für die Spartaner und andere Kaltduscher unter den E-Mail-Schreibern.

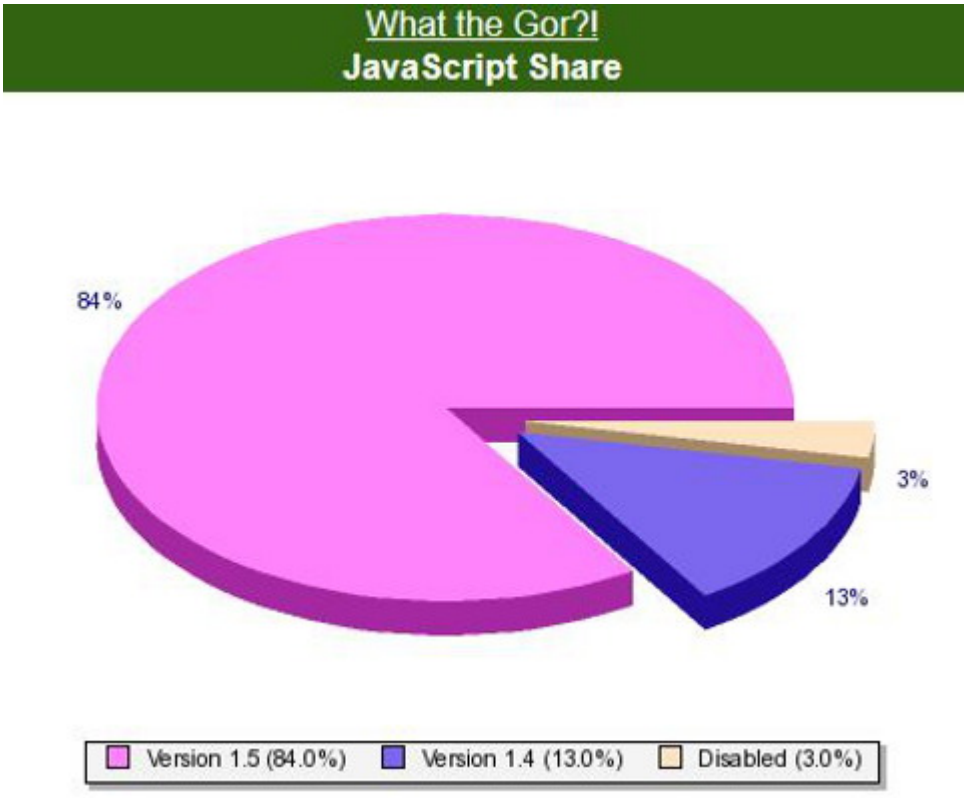
Was auch nervt, ist die merkwürdige Unsitte, dass @ nicht auszuschreiben, sondern, in der irrigen Hoffnung, weniger Werbung zu bekommen, stattdessen ein (at) zu setzen. Schön. Dann weiß man gleich, dass man es nicht mit Profis zu tun hat, sondern mit jemandem, auf den das vielseitig einsetzbare Gleichnis von den Fliegen zutrifft, die nicht irren, weil sie das tun, was alle tun. „Ist dem Crawler bekannt, dass (at) das Gleiche bedeutet wie @, so kann theoretisch auch diese Adresse zum Spam-Ziel werden." Der „Crawler" crawlt ja bekanntlich auch immer gern in unverschlüsselten E-Mails. Oder nicht?

350 Euro im Monat – das sind ungefähr 43 Stunden, also

meinetwegen sechs Tage. (Mehr dazu hier.) Und dann sollen die Bewerber und Bewerberinnen noch wissen, wie man die neuen „Datenschutzbestimmungen“ bei Facebook umgeht? Ach so? Soll man gar nicht wissen? Man muss nur „affin“ sein? Dachte ich mir. Einmal mit Profis arbeiten.

Ist wie beim DJV Berlin. Die Mitgliederversammlung hat denen per Beschluss verboten, eine offizielle Seite bei Facebook zu machen. Sie tun es aber trotzdem (Vorsicht, Facebook!). Wen interessieren schon die Mitglieder und was die wollen?

Hurra, ich bin eine Sekte!



Ich frage mich, ob die Statistik, was Javascript angeht, bei deutschen Websites ähnlich aussieht? Natürlich ist diese nicht repräsentativ, aber „What die Gor“ ist eine Satire-Website, die sich über das Rollenspiel in Gor-Secondlife lustig macht –

und von genau diesen Rollenspielern gemacht wird, also von Leuten, die ohnehin Internet-„affiner“ sind als der Rest. („What die Gor“ ist natürlich Insider-Humor, den niemand versteht, der nicht selbst dort aktiv ist, aber ich kann mich immer kringeln vor Lachen.)

Btw: Funktioniert das hier eigentlich noch beim Internet-Explorer?

Dunkle Materie entdeckt oder: Allah ist wie Jahwe

Wenn ich mich morgens durch die Nachrichten wühle, die zu lesen ich für wert erachte, finde ich meistens zahllose Gründe, mich zu ärgern: Ich werde nicht wirklich informiert, obwohl das Gegenteil behauptet wird, es handelt sich nicht um Journalismus, sondern um Propaganda, um Lautsprecher des Kapitals oder um getarnte Pressemeitteilungen, die darauf verzichten, auch unabhängige Quellen zu befragen, Deutsch des Grauens ist an der Tagesordnung.

Was mich interessiert, sind meistens Reportagen, mit denen ich mich ausführlich beschäftigen möchte, wozu mir aber die Zeit fehlt, oder verstörende Geschichten (Javascript erforderlich), die mich aber ratlos zurücklassen.

Fefe prägte heute den wunderbaren Begriff von der „Echokammer der Gleichgesinnten“, was auf große Teile der deutschen Medien ebenso zutrifft wie auf das Sekten-Milieu der Veganer, Esoteriker oder Binnen-I-Talibanesinnen.

Wenn ich mich wirklich erholen will, gehe ich zu den Wissenschaftlern. Die wissen wenigstens, wovon sie reden, und

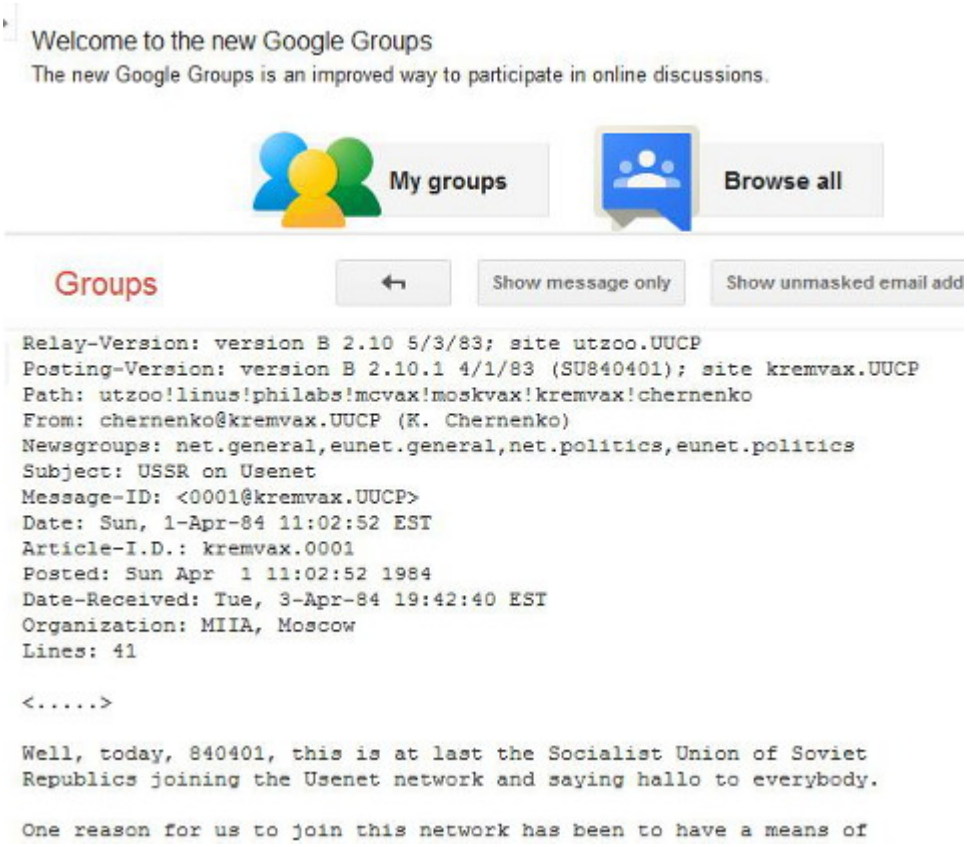
deren Aprilscherze (Javascript erforderlich) sind intellektuell anspruchsvoll und auch komisch.

Fazit: Ich brauche keine Zeitung mehr. Die *konkret* sollte ich endlich mal abonnieren, weil ich sie eh immer kaufe. Aber ohne Gremliza (geb. 1940) wäre die *konkret* vermutlich schnell tot und unlesbar. Ein ebenbürtiger Nachfolger ist nicht in Sicht. „Ich bestehe auf dem Recht, ja der Pflicht des Aufklärers, Allah so wenig zu achten und nach Kräften zu verspotten, wie irgendwelche anderen Götter, von Jesus C. bis L. Ron Hubbard. Die Religionsfreiheit, die ich meine, ist die Freiheit von Religion. Damit das klar ist.“ Wer sagt so etwas sonst noch?

Die Jungle World könnte ich online lesen, vergesse es aber immer, und außerdem nervt mich bei der*Jungle World*, dass sie sich dem E-Mai-Verschlüsseln konsequent verweigern und stattdessen auf Facebook herumtrollen. Was soll an dieser Attitude „links“ sein? Nicht mit mir.

Ich weiß gar nicht, ob ich mein eigenes Blog lesen würde, wenn ich nicht ich wäre. Gute Frage, die nur die wohlwollenden Leserinnen und geneigten Leser beantworten können.

Das Ende (des Usenet) ist nahe



Vor 13 Jahren kaufte Google die Datenbestände der insolventen Betreiberfirma des Usenet-Archivs Deja News auf. Dabei handelte es sich um etwa eine halbe Milliarde Postings. Seitdem hat Google mit der Domain groups.google.com das Quasi-Monopol der Browser-basierten Suche im Usenet, dem ältesten Dienst des öffentlich zugänglichen Internet.

Bei Wikipedia lesen wir: „Beispielsweise werden in der allgemeinen Websuche von Google mittlerweile keine Treffer mehr aus Google Groups angezeigt. Hierzu muss in der allgemeinen Websuche der Unterpunkt ‚Diskussionen' aus der Navigationsleiste ausgewählt werden. Andererseits wurde der Index von Google Groups auf allgemeine Webforen ausgedehnt – dies auf Kosten des Usenet, das derzeit kaum noch nachgewiesen wird, abgesehen vom direkten und gezielten Durchsuchen von Newsgroups."

Das ist zwar nicht ganz richtig, es ist aber noch schlimmer: Seit Neuestem erzwingt Google Javascript, obwohl man bei purem Text, aus dem die Newsgroups bestehen, die nicht definitiv als „Binaries" ausgeweisen sind, Javascript zu allerletzt

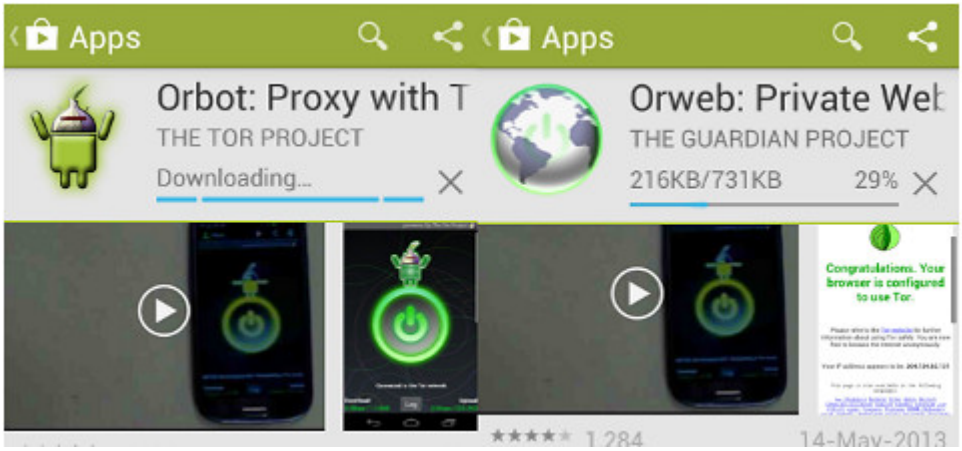
brauchte. Datenspionage geht halt bei Google vor Benutzerfreundlichkeit.

Zudem ist das Feature „Userprofil“ deaktiviert worden. Man konnt mit einem Mausklick auf die E-Mail-Adresse eines Nutzers alle dessen Usenet-Postings seit 1982 anzeigen lassen – eine hübsche Recherche-Möglichkeit, die ich früher oft genutzt habe. Außerdem ist die „Advanced Search“ ganz abgeschaltet worden: Noch vor einem halben Jahr konnte man die Suche nach Postings in Newsgroups zeitlich eingrenzen, etwa auf das Suchwort kremvax auf den Zeitraum zwischen dem 1.1.1984 und dem 5.6.1984.

Google will offenbar, dass man das Usenet vergisst und stattdessen bei „Gruppen“ – statt an „Newsgroups“ – nur noch an Google-Gruppen denkt. Im Usenet konnte man sogar anonym schreiben, das ist jetzt auch nocht mehr so ohne weiteres möglich.

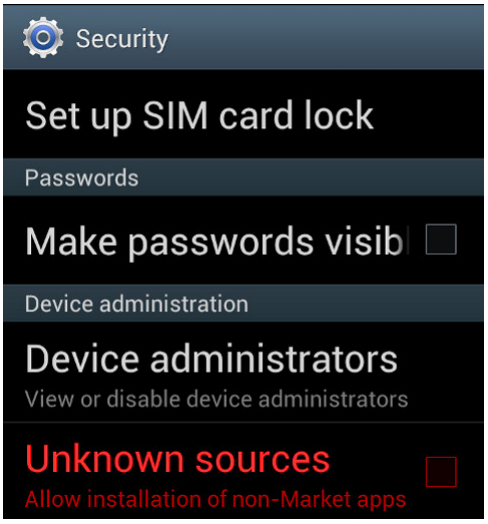
O tempora, o mores!

Anonym Surfen mit dem Smartphone



Oder auch: Secure Mobile Apps and Open-Source Code for a Better Tomorrow – sichere mobile Anwendungen und Open-Source-Software für eine bessere Zukunft.

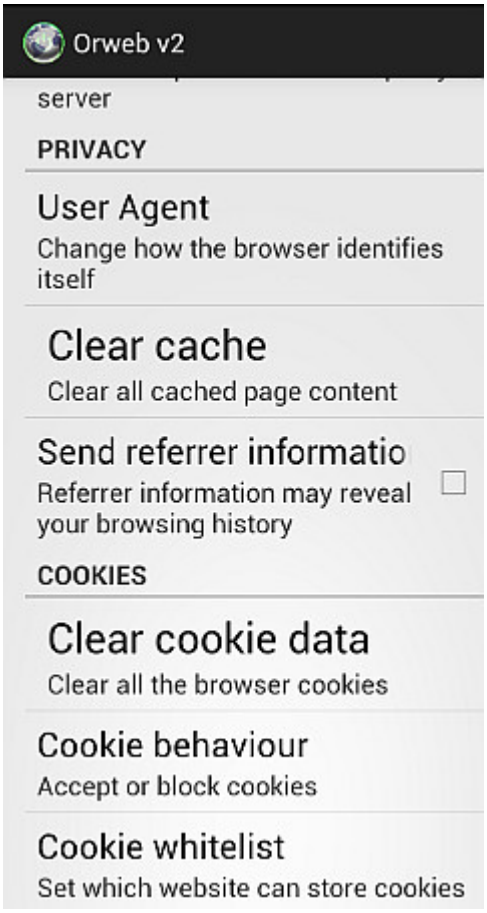
Eine der Geschäftsideen der Anbieter von Smartphones fußt auf der Datenspionage und dem Verkauf des Nutzerverhaltens. Das funktioniert hervorragend, werden doch die gewöhnlichen DAUs von faulen und unfähigen „Webdesignern“,



von Microsoft und Apple und von „Computerexperten“, die in den Mainstream-Medien zu Wort kommen, zu unsicherem Surfen ermutigt, erzogen, ja teilweise gezwungen.

Man sollte diesen Leuten aber eine Menge Sand in ihr gieriges Datenkrakengetriebe werfen. Für Smartphones gibt es zwei nette Anwendungen („Apps“), mit denen man anonym surfen kann: Orweb und Orbot (Proxy mit Tor). Orbot ist ein Proxy („Vermittler„), der die Daten zwischem dem Browser Orweb und dem Tor-Netz transportiert und Anonymität garantiert.

Man kann per Google Store die beiden Apps auf das Smartphone laden oder zunächst auf einen Rechner und von dort dann auf das gar nicht so „smarte“ Handy. Vernünftige Menschen schauen zunächst in die Voreinstellungen eines unsicheren Gerätes, bevor sie es in Betrieb nehmen: Normalerweise sollte man *verbieten*, dass Apps aus unbekannten Quellen installiert werden dürfen (also *kein* Häkchen). Hier müssen wir es ausnahmsweise erlauben (vgl. 2. Screenshot von oben).



Das *Guardian Project* sagt klar und angenehm, was erstens zweitens drittens käm:

Orweb is the most private and anonymous web browser on Android for visiting any website, even if it's normally censored, monitored, or on the hidden web.

– ACCEPT NO SUBSTITUTES: Orweb is the safest browser on Android. Period. Orweb evades tracking and censorship by bouncing your encrypted traffic several times through computers around the world, instead of connecting you directly like VPNs and proxies. This process takes a little longer, but the strongest privacy and identity protection available is worth the wait.

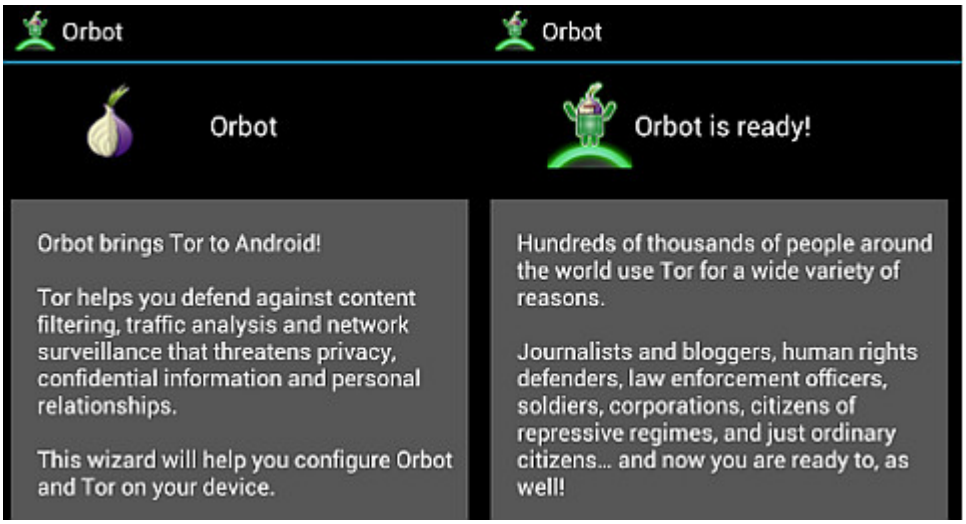
– CIRCUMVENT FIREWALLS AND RESTRICTIONS: Does your office, school, or region block certain websites? Not anymore. Orweb bypasses almost every kind of network restriction.

– BROWSE ANONYMOUSLY: As the New York Times writes, "when a

communication arrives from Tor, you can never know where or whom it’s from.” No technology is 100% effective, but Orweb is as close to anonymous as it’s possible to get on Android.

– PRIVACY YOU CAN TRUST: The Electronic Frontier Foundation (EFF) says „the groundbreaking work from the Tor project helps users everywhere improve the safety of their online communications.“

Fazit auf Deutsch: Orweb ist der sicherste Browser auf Android. Akzeptiere nie Zensur oder (Jugendschutz-)Filter, sondern umgehe sie. Orweb bietet die größtmögliche Anonymität. Die EFF sagt, das Tor-Projekt helfe allen Usern weltweit, sicher zu kommunizieren. Die EFF ist so etwas wie der Chaos Computer Club, nur ohne Verschwörungstheoretiker und Mobbing von Kritikern, dafür aber wesentlich politischer und libertärer.

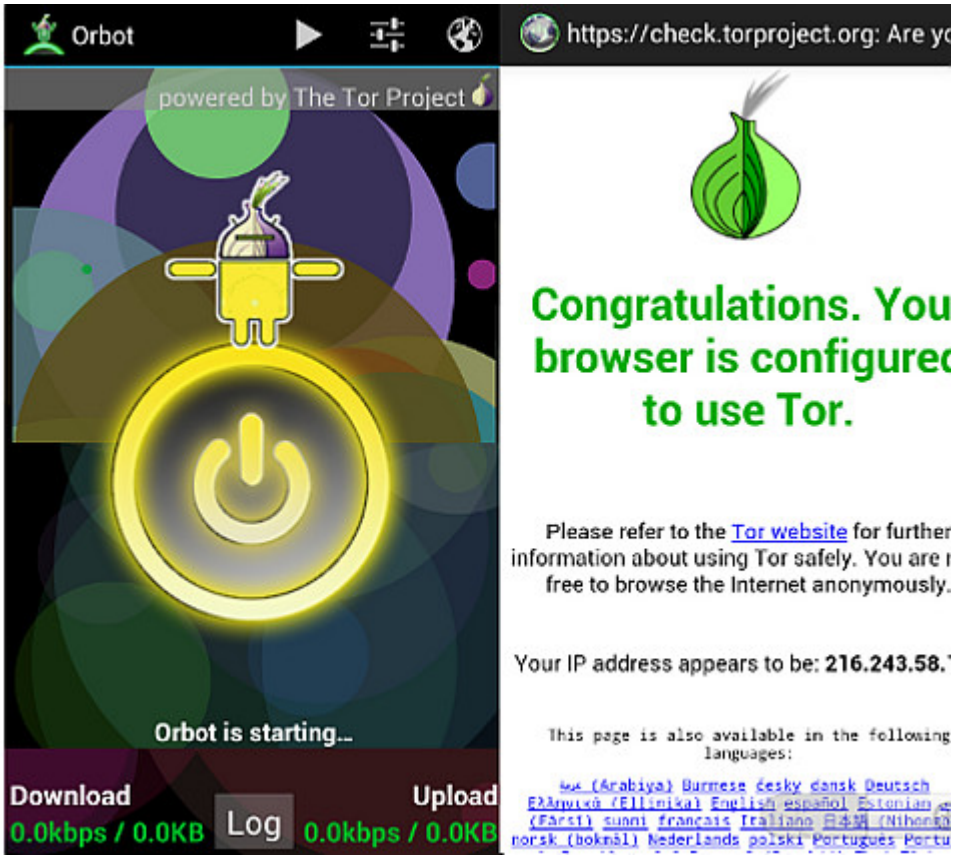


Wenn beide Apps installiert worden sind (nicht vergessen: das Häkchen in den „Options“ wieder entfernen, dass unbekannte Quellen installiert werden dürfen!), muss man sich – wie bei anderen Rechnern – mit den Voreinstellungen des Browsers beschäftigen. Wer Cookies, Referer und Javascript erlaubt, kann auch gleich das Schloss vor die Haustür nageln. (vgl. 3. Screenshot von oben)

Im Unterschied zum Tor Browser Bundle, der ohne weitere

Zusätze das anonyme Surfen ermöglicht, braucht *Orweb* den Proxy *Orbot*, den man zuerst einschalten muss. Bei mir hat die ganze Angelegenheit – Installieren und Einrichten – zehn Minuten benötigt.

Die Browser-Nutzeroberfläche verwirrt, weil man den „Go“-Button, der die Eingabe des Urls ermöglicht, nicht sofort findet (weil man danach nicht sucht). Ansonsten ist das Surfen wie gewohnt. Man hinterlässt nur keine Datenspuren mehr.



---

21 Fragen und ein Test: Bin ich eine Netzpolitikerin?

[Update: Einige Anworten]

Das Netz. Unendliche digitale Weiten. Aber wissen die so genannten „NetzpolitikerInnen“, was das „Netz“ ist? Ein kleiner Test eignet sich für die Selbstauskunft.

1. „World Wide Web“ ist *kein* Synonym für „Internet“. Könnten Sie in einer Talkshow den Unterschied erklären?

2. Was ist eine „Sina-Box“ und welche Bundesregierung hat große Provider gesetzlich verpflichtet, eine anzuschaffen? Wie heisst dieses Gesetz? [Die SINA-Box ist die Abhörschnittstelle aller großen Provider in Deutschland. die TKÜV 22.01.2002 vom Bundesministerium für Wirtschaft unter der rot-grünen Bundesregierung erlassen.]

3. Können Sie Ihre E-Mails verschlüsseln und bieten Sie auf Ihrer Website Ihren öffentlichen Schlüssel zum Download an? (Wenn Sie hier mit „nein“ antworten, sind Sie keine „Netzpolitikerin“: Jemand, der den Unterschied zwischen einem Brief und einer Postkarte nicht kennt, würde bei der Post noch nicht einmal als Briefträger angestellt.)

4. Können Sie bei Bedarf Ihre IP-Adresse beim Surfen anynomisieren?

5. Was hat „paketorientierte Datenübertragung“ mit Netzneutralität zu tun?

6. Was ist der Unterschied zwischen der Vorratsdatenspeicherung und der TKÜV? [Bei der TKÜV geht es darum, die Inhalte der Kommunikation zu belauschen, bei der Vorratsdatenspeichernung, wer mit wem kommuniziert.]

7. Nennen Sie *eine* Alternative für Tor beim Surfen im World Wide Web!

8. Haben Sie schon einmal Javascript in Ihrem Browser deaktiviert und wissen Sie, wozu das gut sein könnte?

9. Welches Programm würden sie für IRC benutzen?

10. Welches Land hat, gemessen an seiner Einwohnerzahl, weltweit die meisten Anfragen an Google gerichtet, Inhalte zu zensieren? [Deutschland]

Das Folgende muss man nicht wirklich auf Anhieb und auswendig wissen. Aber kennen Sie sich beim Thema Netz-Folklore aus?

11. Was ist der Kremvax-Hoax? Könnten Sie das Original auf ihren Monitor holen? Wer verfasste ihn? [eunet.politics, Usenet, 01.04.1984]

12. Welche Zeitschrift erfand das Wort „Cyberporn“, und was war der Irrtum des Redakteurs, der die Titelstory dazu schrieb? [Time Magazin, 03.07.19956, der Autor Philip Elmer-Dewitt hatte aber nicht im Internet recherchiert, sondern ausschließlich in Pornografie- Mailboxen (Bulletin Board System). Der Artikel führte aber zu einem der größten Hypes in der Geschichte des Internet über „Kinderpornografie“.]

13. Welche Zeitschrift behauptete, Hacker können fremde private Computer zu einer ferngesteuerten Bombe umprogrammieren? [Das satirische Magazin Weekly World News im Jahr 2000]

14. Die Bielefeld-Verschwörung stammt *nicht* aus dem „World Wide Web“. Wo wurde sie zuerst veröffentlicht? [1994 im deutschsprachigen Usenet]

15. Was ist der „Good-Times-Hoax„?

16. Für welche Organisation war derjenige juristischer Berater, der „Godwin’s Law“ formuliert hat? Und wie lautet Seitz‘ Addendum zu Godwin’s Law? [Mike Godwin beriet die Electronic Frontier Foundation. Seitz‘ Addendum zu Godwin’s Law lautet: „Dito für unpassende Kinderschänder-Vergleiche, allerdings mit der erhöhten Gefahr, dass die Diskussion nicht beendet wird.“

17. Welcher britische Politiker wurde wegen einer Word-Datei der Lüge überführt? [Tony Blair]

18. Wie hieß der Mann, der von einem deutschen Amtsgericht zu zwei Jahren Haft auf Bewährung verurteilt wurde, weil seine Firma ihren Kunden einen Dienst des Internet angeboten hatte? [Felix Somm wurde 1998 wegen „Mittäterschaft“ bei der Verbreitung von Kinder- und Tierpornographie zu zwei Jahren Bewährungsstrafe und der Zahlung von 100.000 Mark verurteilt, weil die Compuserve-Kunden Zugang zu Newgroups des Usenet hatten.]

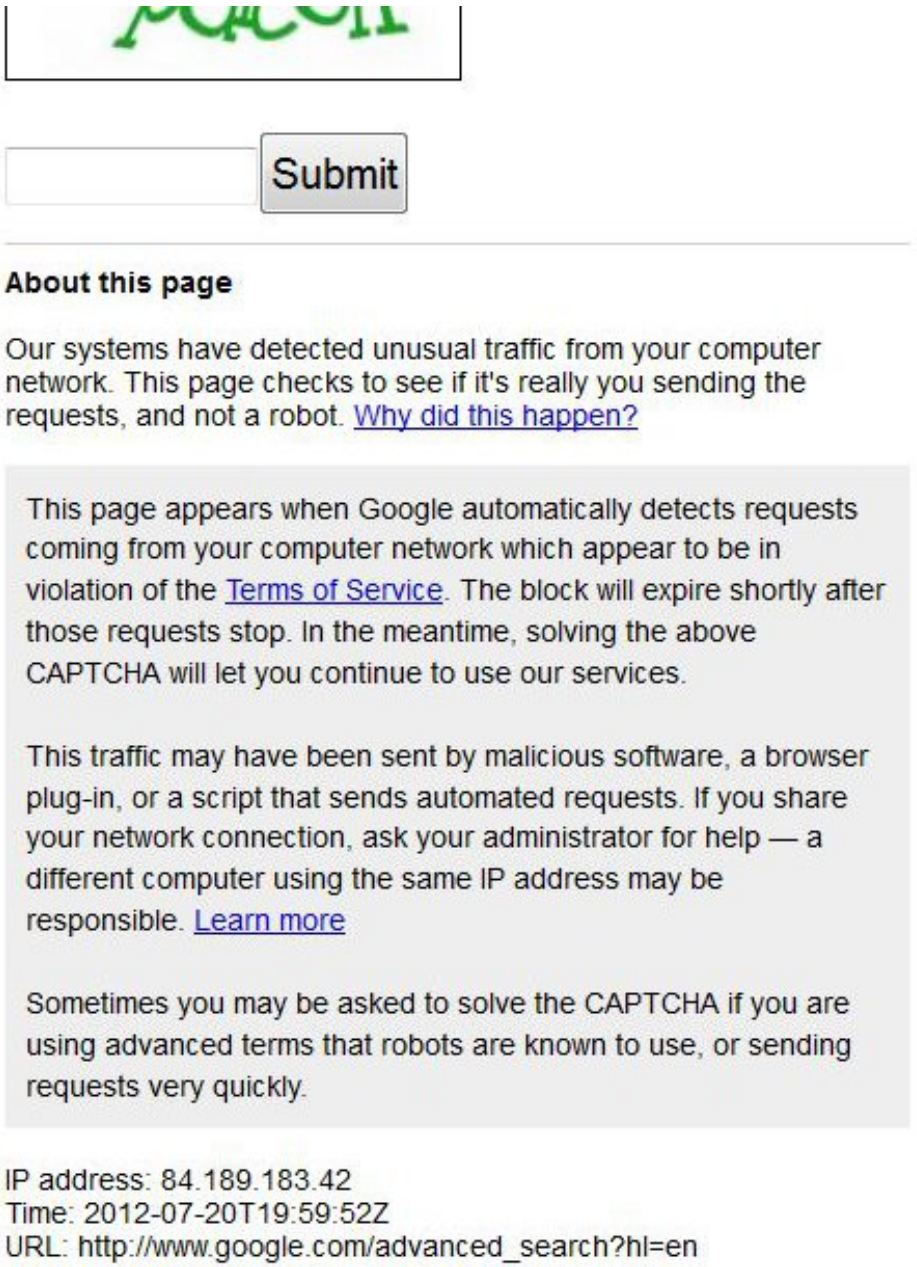
19. Welcher deutscher Innenminister plante wann, Verschlüsselung für private Nutzer zu verbieten? [Manfred Kanther 1998]

20. Was beeinträchtigte den Hacker, der so mit den Lippen pfeifen konnte, dass sich der Gebührenzähler seiner Telefonfirma ausschaltete und er gratis telefonieren konnte – und wie hieß er? [Joe Engressia war blind.]

21. Was war das Neue an der Software SATAN? [SATAN (Security Administrator Tool for Analyzing Networks) bot zum ersten Mal eine grafische Oberfläche zur Netzwerkanalyse]

Wenn Sie nicht mindestens 15 Fragen mit „ja“ oder richtig beantworten können (ohne die Hilfe einer Suchmaschine), sind Sie kein(e) Netzpolitiker(in), sondern sollten sich zunächst informieren, was das „Internet“ eigentlich ist. Aber da man in Bayern sogar Verkehrminister werden kann, wenn man einen Menschen totgefahren hat, wird Sie mein gut gemeinter Rat nicht interessieren.

Unusual traffic from your computer – was erlauben Google? [Update]



Gestern hatte ich ein interessantes Problem zu verstehen und zu lösen: Mein Firefox-Browser wollte und durfte Google nicht mehr benutzen, ohne ein Captcha vorher eingegeben zu haben. Begründung: Man habe ungewöhnlichen Traffic „von meinem Computer“ aus festgestellt. Potztausend – was erlauben Google?

Was hatte ich gemacht? Einer meiner Rechner und der Laptop waren in der Nacht online geblieben, um mit einem Text-Viewer mehrere Avatare auf einer Sim herumstehen zu lassen. Das kann es ja wohl nicht gewesen sein, dachte ich spontan, und mit dem „Terms of Service“ hat es auch nichts zu tun.

Was bietet Google an Erklärungen an? Angeblich könne es sich um Malware („malicious“) auf meinem Rechner handeln – man wird also auf Websites zum Erwerb und Download von „Virenscannern“ und anderen Placebos weitergeleitet. Da ich so etwa noch nie besessen habe, weil ich mich vernünftig verhalte und nichts ohne meine ausdrückliche Genehmigung auf meinen Rechner kommt, war ich natürlich schon auf 180. Zudem konnte ich selbstredend das Captcha sowieso nicht eingeben, weil man dazu alles Mögliche – unter anderem Cookies – erlauben muss. Ich weigere mich. Google auch nur einen Finger hinzustrecken – schon aus Prinzip. *Ihr* kriegt meine Cookies *niccht*!

Mein Zweitbrowser SRWare Iron konnte Google nach Eingabe des Captchas aufrufen. SRWare Iron nutze ich nur für ganz bestimmte Seiten wie Twtter, LiquidFeedback, Ebay oder Second Life Marketplace, wo man Cookies und eventuell auch Javascript erlauben muss.

Dennoch konnte ich danach immer noch nicht Google per Firefox benutzen. Das machte mich stutzig – war „mein Computer“ in Google-Sprech etwa doch nicht meine IP-Adresse? Ich probierte ein paar Variablen durch: Die Captcha-Website kam auch bei meinem Laptop und sogar mit meinem Linux-Rechner. Das Gefasel von „malicious software“ war sowieso wieder die übliche Volksverdummung. Ergo lag es also doch an meiner IP-Adresse. Die aber ist dynamisch und nicht immer dieselbe.

Dann habe ich auf allen Rechner JonDo eingeschaltet, um anonym zu surfen. Google akzeptierte meinen Firefox klaglos *ohne* Captcha. Am nächsten Tag war es genau das Gleiche.

Ein Freund, mit dem ich die Affäre besprach, sagte, das käme

auch manchmal vor, wenn man Tor benutzte – wenn mit der IP-Adresse vorher – von einem anderen Nutzer – irgendein Unsinn angestellt worden war. Also hilft ein Router-Resetting von mehreren Minuten.

Irgendein T-Online-Nutzer musste also vorher Google unangenehm aufgefallen sein, und ich musste die „Sperre“ der IP-Adresse dann ausbaden. Das hat mich weniger geärgert als der irreführende Quatsch, den Google verbreitet, um zu „erklären“, warum ein Captcha notwendig sei, und die Links zu „Anti-Viren-Software“, an denen Google wahrscheinlich auch noch verdient.

Google hat mich als „Kunden“ verloren. Ich benutze jetzt mit allen Rechner und Browsern StartPage als Suchmaschine und Startseite. Das hätte ich schon viel eher machen sollen.

[Update] Heise: „Google fordert Captcha-Eingabe von Suchmaschinennutzern“

Lena in Gefahr – Terror-Alarm in Deutschland [2. Update]

Es fällt mir immer schwerer, *nicht* von gleichgeschalteten Medien in Deutschland zu sprechen. Der Vergleich hinkt natürlich, weil die Vorzensur aus der Schere in den Köpfen besteht, kombiniert mit Dummheit und Faulheit. Niemand zwingt Journalisten dazu, gequirlten Unsinn zu schreiben. (Ich dürfte gar nicht meckern, hätte ich doch einen guten Artikel selbst schreiben zu können, aber ich bin gestern zu spät ins Bett gegangen.)

Ich habe mir also zum Frühstück das angeschaut, was mir als „Nachrichten“ und „Fakten“ zum Thema „Terrorgefahr in Deutschland“ angeboten wird. Dass Stefan Krempl bei Heise das Märchen von den „heimlichen Online-Durchsuchungen“ wieder aufwärmt, wundert mich jedoch nicht.

Mit „gleichgeschaltet“ meine ich: Das, was eine Behörde verlautbart, wird unkritisch übernommen (inklusive der suggestiven Sprachregelungen), ohne zu überprüfen, ob die Fakten stimmen. Im Sozialismus hieß eine derartige „Quelle“

schlicht „Agitprop“. Wenn viele Medien voneinander abschreiben, gilt eine These offenbar als verifiziert. Das war auch schon beim Thema Online-Durchsuchung so. Die Rheinische Post schießt den Vogel ab und gibt es auch noch zu: „Übereinstimmenden Medienberichten zufolge sollen die Festgenommenen einen größeren Anschlag in Deutschland geplant haben“. Dann *muss* es ja wahr sein, wenn alle anderen des Kaisers neue Kleider bewundern!

„Den Angaben zufolge wurde die Kommunikation der Männer überwacht. (…) Amid C. sei dafür verantwortlich gewesen, die ‚verschlüsselte und konspirative Kommunikation‘ untereinander sicherzustellen. Laut Ziercke war es den Behörden jedoch mit umfangreichen, monatelangen Überwachungsmaßnahmen gelungen, den mutmaßlichen Terroristen auf die Spur zukommen.“ (Focus) „Im Zuge der Ermittlungen hatte das BKA einen Trojaner für eine Online-Durchsuchung sowie eine Software für eine Telekommunikationsüberwachung auf seinem Rechner installiert.“ (Spiegel) „Das Bundeskriminalamt (BKA) ist den mutmaßlichen Terroristen durch Überwachung ihrer Handys und Computer auf die Spur gekommen.“ Süddeutsche) „Bei den Ermittlungen hatte das BKA dem „Spiegel“ zufolge einen Trojaner für eine Online-Durchsuchung sowie eine Software für eine Telekommunikationsüberwachung auf dem Rechner des Verdächtigen installiert.“ (FTD) „Den Angaben zufolge wurde die Kommunikation der Männer überwacht.“ Mitteldeutsche Zeitung)

Die FTD redet also von einem „Bundestrojaner“. Was aber soll das sein? Man kann einen Computer nur fernsteuern und überwachen, wenn man a) einen physikalischen Zugriff auf ihn hatte, b) wenn der Besitzer des Computers denselben nicht geschützt hatte und c) haben die Ergebnisse, die durch Spionage-Software auf einem Rechner gewonnen wurden, vor Gericht keinerlei Beweiswert, weil diese den Computer verändert. Man kann das vergleichen mit einem V-Mann, der eine Neonazi-Kameradschaft gründet und diese dann auffliegen lässt. (Darüber habe ich ein ganzes Buch geschrieben.)

Die Taz gibt sich wenigstens Mühe: „Permanent waren 50 Leute in Observationstrupps und weitere 76 Beamten für sonstige Überwachungsmaßnahmen im Einsatz. Dabei wurden Wohnungen und Telefone abgehört, Emails mitgelesen. Auf Computern wurden Spähsoftware installiert und verschlüsselte Internet-Telefonate wurden schon im Computer, also vor der Verschlüsselung (mittels Quellen-TKÜ) erfasst.“

Aha. Bei der angeblichen „Online-Durchsuchung“ wird es sich um das Abhören von Skype gehandelt haben. Verschlüsselte E-Mails kann man nicht lesen, es sei denn, man hätte einen Keylogger installiert und protokollierte die Tastatur-Anschläge a priori mit. (By the way, taz: „Quellen-TKÜ“ ist Neusprech des Wahrheitsministeriums.)

Und was lehrt uns das alles? Schauen wir doch ein wenig genauer hin, um hinter den Nebelkerzen ein paar winzige Fakten erkennen zu können.

„Dort habe er von einem ‚hochrangigen Al Qaida-Mitglied‘ den Auftrag bekommen, einen Anschlag in Deutschland auszuführen. Wer der Auftraggeber konkret war, wollten weder Ziercke noch Bundesanwalt Rainer Griesbaum sagen. “ (taz) Ich weiß, wer es war – Adil Hadi al Jazairi Bin Hamlili!

Regimetreue Medien geben der Totalüberwachungs-Lobby jetzt breiten Raum: „‚In Deutschland besteht weiterhin eine konkrete Terrorgefahr‘, sagte Uhl der ‚Welt am Sonntag‘. Gleichzeitig zeige der Fall, dass die Nachrichtendienste zu wenig Eingriffsrechte besäßen. Denn die entscheidenden Hinweise erhielten die deutschen Ermittler von der amerikanischen CIA. (…) ‚Wir müssen wissen, mit wem die Terroristen kommunizieren, um ihre Netzwerke ausfindig machen zu können‘, sagte er. ‚Dafür brauchen wir die Vorratsdatenspeicherung.'“

Passt schon. Wir haben verstanden.

Vermutlich wird bei der Gerichtsverhandlungen, die vielleicht noch in diesem Jahr stattfinden, von den Vorwürfen nicht viel

übrig bleiben. Aber das wird dann im Kleingedruckten stehen, das niemand mehr liest: „Bei der Hausdurchsuchung wurde kein Sprengstoff gefunden. Außerdem stellte das BKA fest, dass der Plan zur Herstellung eines Zünders gar nicht hätte gelingen können, weil die Terrorbastler die falschen Grillanzünder gekauft hatten."

Wie das? Stehen im Internet denn *falsche* Bombenbauanleitungen? Gehört es denn nicht verboten, *falsche* Bombenbauanleitungen zu verbreiten? (Akte aka Ulrich Meyer, übernehmen sie: „Es war unser Thema am vergangenen Donnerstag: Bombenbauanleitungen im Internet. Das Netz ist voll davon, Spezialisten haben über eine eigene Filtersoftware 680.000 Seiten weltweit aufgestöbert".)

„Dennoch erließ die BGH-Ermittlungsrichterin gegen alle drei Beschuldigte Haftbefehle." Quod erat demonstrandum.

Mich wundert, dass alle Medien, sogar die Krawallblätter, sich die einmalige Chance entgehen ließen, das Volk auf die anlass- und verdachtsunabhängige Totalüberwachung aka Vorratsdatenspeicherung mental einzustimmen. „Unterdessen verlautete aus Sicherheitskreisen, dass die drei Terrorverdächtigen einen Anschlag auf den Eurovision Song Contest geplant haben könnten. Allerdings hätten die Verdächtigen nicht konkret darüber gesprochen, hieß es." (Welt)

Burks.de hat daher die dazu passenden Schlagzeile gewählt.

„Sicherheitskreise": Das sind die Geheimdienstler, die Journalisten auf ihrer Gehaltsliste haben oder wissen, dass diese geschmeichelt sind, wenn man ihnen angebliche „vertrauliche Vorab-Informationen" zukommen lässt und die daher gern bereit sind, Agitprop, die man gern verbreitet hätte, Wort für Wort ohne Kritik zu publizieren.

„Die Terroristen wollen Lena umbringen. Das haben sie zwar nicht so gesagt, aber es könnte ja sein. Würden Sie das bitte

so bei Welt Online veröffentlichen? Danke.“

Update: EFF: „New FBI Documents Provide Details on Government’s Surveillance Spyware“. „The documents discuss technology that, when installed on a target’s computer, allows the FBI to collect the following information“..blabla..und wie bekommt man das auf den Computer des Zielobjekts?

Guckst du hier (burks.de, 31. Juli 2007):

„… es geht um CIPAV: „FBI-CIPAV.exe Is an Unknown Application. Install Anyway?“ Jetzt aber im Ernst: „Die Abkürzung steht für „Computer and Internet Protocol Address Verifier“, zu Deutsch: Computer- und Internet-Protokoll-Adressen-Verifizierer. Dieses Programm ist in der Lage, auf dem Rechner des Verdächtigen die Internet-Verbindungen und angesteuerten Homepage-Adressen samt Datum und Uhrzeit aufzuzeichnen. Die in Fachkreisen Trojaner genannte Software erfasst auch weitere Daten wie das Betriebssystem des ausgehorchten Computers, den Namen des bei der Windows-Registrierung angegebenen Nutzers, Teile der Windows-Registrierungsdatenbank oder eine Aufzählung aller laufenden Programme. Im vorliegenden Fall übermittelte CIPAV einige dieser Informationen per Internet an die FBI-Rechner.“ Das ist aber ein ultraböhzes Programm, fast so böse wie das Betriebssystsem, auf dem es nur läuft.

Wired dazu: „[1] the FBI sent its program specifically to Glazebrook’s then-anonymous MySpace profile … [2] „The CIPAV will be deployed through an electronic messaging program from an account controlled by the FBI. The computers sending and receiving the CIPAV data will be machines controlled by the FBI.“ … [3] More likely the FBI used a *software vulnerability*, either a published one that Glazebrook hadn’t patched against, or one that only the FBI knows.“ Genau, Software-Lücken, von denen nur das FBI etwa weiß. (…)

Die *Welt* betont sehr deutlich, dass der Schüler offenbar „arglos“ etwas abrief, vermutlich so, wie das *Welt*-Redakteure

machen mit ihrem Outlook und dem unverschlüsselten und mit Javascript-gespickten Spam, den sie das immer bekommen. Der Artikel ist also ein Schmarrn. Ich darf auf mein Blog vom 19.07.2007 hinweisen („Heise Hoax-verseucht“), in dem die Details zu CIPAV abgehandelt werden.“

2. Update: New York times: „Bild, Germany’s most widely read and generally reliable (sic!) newspaper, reported that the terrorist cell might have planned to hit the popular Eurovision Song Contest on May 14, though that event’s organizers said they had not been alerted to any such threat. „>. Qood erat demonstrandum. (via Überschaubare Relevanz)

Fehler: Umleitungsfehler oder: Die nie beendete Anfrage

Nur damit das klar ist: Ich bin *nicht* schuld. Wenn etwas nicht funktioniert, muss ich mir *nicht* einen Browser herunterladen, ich muss *nicht* die Sicherheitseinstellungen verändern. Nein. Nie.

Die Betreiber der Website, die ich *nicht* ansehen kann, sind schuld. Es sind Trottel, DAUs, Ignoranten oder sie wollen mich, ohne dass sie mir das verraten, ausspionieren. Es ist *nicht* selbstverständlich, dass jemand Cookies per default gestattet, es ist *nicht* selbstverständlich, dass jemand Javascript per default erlaubt. Merkt euch das!

Ich muss *nicht* den Traffic auf euer bescheidenen Website

erhöhen; ich kann auch woanders hingehen. Es ist wie im realen Leben: *Ich* bleibe so, wie ich bin, und wenn euch das nicht gefällt, dann müsst *ihr* euch ändern oder den Kontakt mit mir vermeiden. (So, jetzt geht es mir wieder besser und genug Kaffee habe ich jetzt auch getrunken.)

Ich darf auch an mein Posting vom November 2008 erinnern: „Ein einfaches Sicherheitskonzept für Daten“ sowie an das vom Dezember 2010: „Browser-”Lücken” – Experte ist nicht alarmiert“.

Bgsound

Golem: „Stefan Münz, der mit Selfhtml über viele Jahre für die deutschsprachige HTML-Referenz verantwortlich war, hat ein Handbuch zu HTML5 veröffentlicht. Das Ende 2010 erschienene Buch steht nun auch online kostenlos zur Verfügung.“

Ich habe mal ein bisschen gestöbert und bin auf das hübsche Kapitel „proprietäre Elemente“ gestoßen. Hihihi. Wer benutzt heute eigentlich noch *blink*?

Bei *bgsound* musste ich grübeln: „Wird heute, wenn überhaupt noch gewagt, meistens mit Hilfe von Flash realisiert, das über JavaScript mit dem Event-Handler onload gestartet wird.“

Mal abgesehen davon dass es dreist ist, den ahnungslosen Surfer mit Musik zwangsweise zu bedudeln: Ich surfe bekanntlich nicht wie ein DAU, sondern *ohne* Javascript. Wie erzwinge ich denn Hintergrundmusik ohne Flash und Konsorten?

Firesheep oder „Hacken“ für jedermann

Zuerst habe ich mich bei der Lektüre des aktuellen Print-Spiegels geärgert, dass jemand unwidersprochen dummes Zeug über das Internet verbreiten durfte. Der „Strafrechtler und Schufa-Ombudsmann Winfried Hassemer: „Wer zwei Stunden im Internet surft, hinterlässt mehr Spuren als bei der Schufa.“ Nein. Stimmt nicht. Gar nicht wahr. Nur DAUs hinterlassen Spuren und erlauben Cookies und Javascript und HTTP referrer. Aber so ist nun mal leider das Niveau der Diskussion. Es ist zum Heulen.

Unter der reißerischen Überschrift „Hacken für jedermann“ lesen wir auf S. 131 etwas über Firesheep, „a Firefox extension that demonstrates HTTP session hijacking attacks“. Kein Wort darüber in Spiegel Offline, was diese Software macht, sondern nur dumpfe Panikmache: „Automatisch schnüffelt sie nach ungesicherten Verbindungen in der Umgebung, zum Beispiel um auszuspähen, der sich im Café über ein ungeschütztes WLAN bei Facebook angemeldet.“ Vermutlich kann man mit diesem „Hacker-Tool“ auch Verkehrsampeln ausstellen….

Warum sollte man jemanden warnen oder mahnen, der bei Facebook ohnehin die Hosen runterlässt und seine Daten in alle Welt verstreut (was war noch mal das Geschäftsmodell von Facebook?)…. Bruce Schneier hat dazu das Nötige gesagt: „Basically, Facebook authenticates clients with cookies. If someone is using a public WiFi connection, the cookies are sniffable. Firesheep uses wincap to capture and display the authentication information for accounts it sees, allowing you to hijack the connection.(…) Protect yourself by forcing the authentication to happen over TLS. *Or stop logging in to Facebook from public networks*.“

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!

Avanti Facebook Dilettanti

Was ist das Gute an Facebook? Dass sich die deutschen Zensoren darüber aufregen und meinen, am deutschen Wesen müsse die Welt genesen: „Es kam zu einem offenen Brief an Facebook mit der Aufforderung, die Profile der Neonazis zu löschen, oder es komme zu einer Anzeige wegen Volksverhetzung. Am 17. April 2009 stoppte die Deutsche Telekom ihre Werbung auf Facebook mit Hinweis auf ‚rechtsextreme‘ Webseiten auf dem Portal“. Was ist eigentlich daraus geworden? Deutsche Staatsanwälte verklagen Facebook wegen „Volksverhetzung“ – trotz des First Amendment? Zuzutrauen wäre es ihnen. Nur mal zum Erinnern:

„Der 1791 verabschiedete Artikel verbietet dem Kongress, Gesetze zu verabschieden, die die Meinungsfreiheit, Religionsfreiheit, Pressefreiheit, Versammlungsfreiheit oder das Petitionsrecht einschränken.“

So etwas gibt es in Deutschland **nicht**. Der Bundestag **darf** Gesetze erlassen, die die Meinungsfreiheit, die Pressefreiheit und die Versammlungsfreiheit einschränken. Einige Grünen haben jüngst wieder schärfere Zensur-Gesetze gefordert, die Partei „Die Linke“ will das Internet zensieren und das Bundesverfassungsgericht muss immer wieder eingreifen, wenn deutsche Gerichte die Versammlungsfreiheit mit Füßen treten. Aber es ist verschwendete Zeit, den Deutschen erklären zu wollen, was Meinungsfreiheit (auch für die Blösen, die Doofen und die Ekligen) bedeutet. Das ist intellektuell zu anspruchsvoll für Lichterkettenträger.

Ich schweife ab. Zum Thema. In der aktuellen c’t las ich einen interessanten Artikel über soziale Netzwerke. „Facebook hat nach eigenen Angaben mehr als 400 Millionen aktive Benutzer, von denen sich jeder zweite täglich einloggt: Wäre der Dienst ein Staat, so wäre er noch vor den USA der drittbevölkerungsreichste der Welt.“

Bei Wikipedia las ich: „Ebenso überarbeitete Facebook im Dezember 2009 die Kontrolle über die Privatsphäre. Nun kann jeder Nutzer bei der Veröffentlichung von Statusmeldungen, Medien oder Links differenziert festlegen, wer diese sehen darf und wer nicht.“

Ich wollte also einfach mal reinschauen, nur so aus Neugier. Die wohwollenden Leserinnen und geneigten Lesen ahnen schon, was jetzt kommt: Es ist mir nicht gelungen, trotz meines guten Willens, sogar die Standardeinstellungen meines Browsers zu verändern. Für Linux gibt es ohnehin keine „Hilfe“, die diesen Namen verdient, und mein Problem, das ich gern detailliert wüsste, *was* ich an Javacsript, Cookies usw. zulassen muss, damit ich mich registrieren kann, wird nirgendwo beantwortet.

Ich bin *kein* Exot – ich bin *normal*. Ich surfe mit Mozilla/Firefox für Linux und habe die Add-Ois Cookiesafe, NoScript und RefControl in Gebrauch. Sogar wenn ich Javascript und Cookies für Facebook temporär erlaube, kann ich mich nicht registrieren – ich müsste noch zahlreiche andere aktiven Inhalte von Anbietern, die nicht kenne, auf einen Rechner lassen. Warum und wer das ist, wird mir nicht verraten. Und deshalb könnt ihr mich mal kreuzweise, ihr sozialen Netzwerke.

Update: Jetzt habe ich mein Windows-Laptop hervorgekramt…

Seamonkey und Pdfit

Ich habe mir die wunderbare Firefox-Erweiterung pdfit installliert. Pdfit erlaubt, eine Website direkt als Grafik oder als pdf auszudrucken – sehr praktisch. Das konnte ich zuletzt vor Jahren unter Windows mit meinem minderlegalen Acrobat Distiller.

Oft werde ich das Feature aber nicht nutzen. Ich bin jetzt auf den Browser Seamonkey umgestiegen, der Schriften und Grafiken besser anzeigt als Firefox (vielleicht liegt es auch an meiner Grafikkarte). Die Sicherheitseinstellungen sind ähnlich komfortabel: Ich surfe grundsätzlich *ohne* Javascript, und der Seamonkey bietet eine komfortable Verwaltung der Cookies (die ich per default auch verbiete). Auch der JonDo-Client arbeitet einwandfrei.

Unfreiwillige Selbstkontrolle

Zur Zeit wird die „Sau“ Presserat wieder durchs Dorf getrieben. Nun hört sich der pieselige Verein feierlich an, ähnlich wie Zentralrat der Muslime oder Zentralrat der Sinti und Roma. Der „Presserat kontrolliert künftig auch Online-Journalismus“, heißt es bei Heise. Soso. Macht er das? Und was soll uns das sagen? „Unter die Lupe nehmen“, wie die Frankfurter Rundschau und die Tagesschau die Tätigkeit des zahlosen Tigers Presserat sybillinisch nennen, weil ihnen kein anderer Textbaustein einfiel für das genauer Hinsehen als genau, hört sich an wie das ebenso sinnfreie „das Verfassungsschutz beobachtet“.

Das dazu passende Verbum, das einen Gefühlszustand des Vereins suggeriert, bringt Deutschlandradio: „Der Deutsche Presserat zeigt sich besorgt.“ Ja, das Böse nimmt zu, allüberall und schon seit dem Neolithikum. Der Tagesspiegel erwähnt noch etwas Urdeutsches, ohne dass ein Journalist hierzulande noch nicht einmal aus Klo geht: „Gremium wird auch fürs Internet zuständig“. Dann kann ja nichts mehr schiefgehen, wenn die Zuständigkeit eines deutschen Vereins für das digitale Universum definiert worden ist. Am deutschen Presseratswesen soll das Internet genesen.

Jetzt aber im Ernst. Der Presserat ist ein „Tarnfirma“ von vier Verbänden, wie in seiner Selbstdarstellung klar zu sehen ist: Dem Verband Deutscher Zeitschriftenverleger (VDZ, dem Bundesverband Deutscher Zeitungsverlager (BDZV, dem DJV und „ver.di Fachbeerich Medien (dju)“. Der Presserat ist eine Lobby-Organisation von denjenigen Verbänden, die bis noch vor kurzem das Monopol eines real gar nicht existierenden Presseausweises für sich beanspruchten, bis sie von deutschen Gerichten eines Besseren belehrt wurden. Er sei ein Organ der „freiwilligen Selbstkontrolle“, als gäbe es auch eine „unfreiwillige Selbstkontrolle“. Wessen? Derer, die das mitmachen. Für die, die sich nicht freiwillig kontrollieren

wollen, sind die Verlautbarungen des Presserats etwas, womit man den Hobbyraum im Keller tapeziert.

Wenn andere Journalistenverbände auch einen Presserat gründen wären, könnte sie niemand daran hintern. Ich würde den neuen Verein aber *Pressezentralrat* nennen. Das hörte sich noch toller an. Tun könnte der außer dem obligatorischen Mahnen und Warnen gar nichts. Konventionalstrafen für die Missetäter hätte er auch nicht. Lichterkettenträger aller Medien, vereinigt Euch!

SPIEGEL Wissen

…habe ich gerade getestet: Die Suche funktioniert nicht ohne Javascript. Man fasst es nicht. So züchtet man DAUs heran.

Verfassungsfeind Schäuble

Nach einem Bericht der HAZ (bei denen sieht man nichts ohne eingeschaltetes Javascript – Idioten!) wilkl Schäube *alle* abhören. „Jetzt hat Schäuble den Referentenentwurf aber auf erstaunliche Weise ’nachgebessert‘. In der jüngsten Fassung vom 6. Dezember findet sich plötzlich in Paragraf 20u ein neuer Absatz, der den bisher für bestimmte Berufsgruppen vorgesehenen Schutz weitgehend wieder zurücknimmt.“ Wer hätte das von unserem Innenminister gedacht, der uns doch alle liebhat?! Ich nenne Schäuble einen Verfassungsfeind.

24C3 | Gezielte Trojaner-Attacken

Laut Heise hat Maarten Van Horenbeeck eine schöne Geschichte über Chinesen-Trojaner erzählt. Ich glaube das alles nicht so einfach. Natürlich: Wenn man „The Month of Kernel Bugs „(MoKB) archive“ anschaut, überkommt einen das Gruseln. Dennoch: Ich halte die meisten Meldungen, die Chinesen hätten wieder irgendetwas „gehackt“, für reine Propaganda, weil niemand die Faken überprüft. (vgl. spiggel.de, 04.09.2007: „Chinesen greifen das Pentagon an!“ sowie spiggel.de, 26.08.2007: „Die China-Hacker kommen nicht“).

„Laut Van Horenbeeck startete die immer wieder mit China in Verbindung gebrachte Trojaner-Invasion 2005 mit einem unauffällig per E-Mail dahergekommenen Bildschirmschoner-Objekt mit dem Namen dot.scr, das eine ausführbare Datei erhielt.“ So ein Quatsch: Warum soll ein Attachment

„unauffällig“ sein? Und wer installiert Bildschirmschoner von unbekannten Absendern, womöglich aus China? „2006 folgte gemäß

Van Horenbeeck ein nach wie vor aktiver Trojanerangriff mit einer als HuJintao.doc betitelten Word-Datei.“

Ein Hacker-Angriff mit einer Word-Datei? Womöglich mit einem Bambus-Rechner? Soll ich diesen Schwachfug glauben?

Laut Horenbeck sei die Windows-Schwachstelle MS05-035 ausgenutzt worden. Nach Heise befasst sich MS05-035 „… mit einem Fehler in der Font-Behandlung von Word, der sich durch manipulierte DOC-Dateien ausnutzen lässt. Betroffen ist Word aus Office 2000 und XP (2002) sowie die Word-Versionen aus Microsoft Works 2000 bis 2004. Word 2003 hingegen ist laut Microsoft immun.“ Sehr gefährlich hört sich das nicht an, denn es betrifft nur einige Systeme – und die müsste jemand vorher kennen.

„Im April erregte ein ungewöhnlicherweise in einem reinen HTML-Anhang daherkommender Trojaner die Aufmerksamkeit des Belgiers.“ Mir scheint dieser Belgier ein Wichtigtuer zu sein, mit Verlaub. Anhang in HTML! Da lachen ja die Hühner! Wie

sollte man jemanden, der mit seinem MUA vernünftig umgehen kann, damit überlisten können – und dann vielleicht auch noch *ohne* Javascript? Nein, nein, nein, ich glaube weiterhin kein Wort.

Eine wichtige Quelle für die angeblichen Trojaner-Angriffe aus China ist jemand, der keinen Anlass auslässt, um sich zu blamieren: „Die Beamten im Innenministerium haben die angeblich aus China stammenden Trojaner-Angriffe auf Bundesbehörden nachdenklich gemacht. ‚Finstere dritte Mächte' hätten entsprechende Versuche unternommen, weiß Staatssekretär August Hanning. Diese seien aber „erfolgreich abgewehrt worden". (Heise-Newsticker, 05.09.2007)

Vielleicht wäre es an der Zeit, wenn der geschätzte Kollege Krempl, der fast alle die Meldungen bei Heise verfasst hat, die Zeit fände, auch einmal die Fakten zu überprüfen – dann löste sich der Trojaner-Hoax made in VR China vermutlich in Luft oder in Praktikanten auf.