Was ist und zu welchem Ende betreiben wir Social Engineering?

Spiegel Online (ein Link zur Quelle, o Wunder!) fantasiert wieder wahllos herum: „Denn Bronk hackte sich in deren E-Mail-Konten…“ Das hätte die Taz auch nicht schlechter formulieren können. Wie zum Teufel, „hackt“ man sich in E-Mail-Konten? Etwa mit einer real gar nicht existierenden „Online-Durchsuchung“?

Nein, der Kerl war kein echter „Hacker“, sonder jemand, der sich des guten alten Social Engineering bediente: „Ausgestattet mit dem derart zusammengetragenen Hintergrundwissen ging er daran, die E-Mail-Passwörter seiner Opfer zu ändern. Dazu machte er sich nicht etwa die Mühe, zuerst deren Passwort herauszufinden. Stattdessen gab er sich deren E-Mail-Providern gegenüber als Inhaber des jeweiligen Accounts aus und beantragte, mit der Begründung, er habe sein Passwort vergessen, online ein neues. Weil viele Provider immer noch Standardabfragen, beispielsweise nach dem Mädchennamen der Mutter, verwenden, um in solchen Fällen die Identität des Antragstellers zu überprüfen, fiel es Bronk nicht schwer, die E-Mail-Konten zu übernehmen.“

„Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Daten oder Dinge zu gelangen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um Dinge wie geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von Social Hacking.“

Also bitte keine Computermythologie, Technik-Schamanismus oder anderen Regenzauber: Man kann sich nicht einfach so irgendwo „reinhacken“.

Totalüberwachtes Lob des Kommunismus

Er ist vernünftig, jeder versteht ihn. Er ist leicht.
Du bist doch kein Ausbeuter, du kannst ihn begreifen.
Er ist gut für dich, erkundige dich nach ihm.
Die Dummköpfe nennen ihn dumm, und die Schmutzigen nennen ihn schmutzig.
Er ist gegen den Schmutz und gegen die Dummheit.
Die Ausbeuter nennen ihn ein Verbrechen.
Aber wir wissen:

Er ist das Ende der Verbrechen.
Er ist keine Tollheit, sondern
Das Ende der Tollheit.
Er ist nicht das Chaos
Sondern die Ordnung.
Er ist das Einfache
Das schwer zu machen ist.

Bertolt Brecht

Ich fordere aus gegebenem Anlass, diese volksverhetzenden, empörenden und vor allem total jugendgefährdenden Inhalte aus dem Schulunterricht und auch aus Museen zu verbannen. Lehrer, die es dennoch wagen, Brecht im Deutschunterricht zu erwähnen, sollten total mit Berufsverbot belegt oder mindestens totalüberwacht werden.

Dieses Verb gab es zwar bisher nicht im Deutschen, die deutsche Sprache sollte aber den Belangen der total wahren Totalitarismus-Doktrin – der einzig erlaubten Sicht auf die deutsche Geschichte – totalangepasst werden. Zumindest sollte ein Vermerk in jedes Buch und jede Internet-Veröffentlichung, dass der „Dichter" Brecht seine total antifreiheitlichdemokratischen Zeilen in einem Zustand geistiger Totalumnachtung verfasst hat.

Es kann nicht sein, dass die Freiheit der Rede missbraucht wird, um den Jugendschutz zu unterhöhlen und Kinder und Herwachsenden total hilflos mit diesem Schmutz und Schund allein zu lassen. Allein schon wegen Brecht brauchen wir die Vorratsdatenspeicherung jetzt und total sofort. Auch sollte die Polizei jederzeit auf alle Computer zugreifen können, um kontrollieren zu können, ob sich dort jugendgefährdende Inhalte befinden – wie etwas Bertold Brecht und anderen Formen von Kinderpornografie. Das will auch die total große Mehrheit der Deutschen.

Schützt endlich unsere Kinder vor total undeutschen Dichtern!

Auch hier lesen: „10 Gründe, warum der Kommunismus schlecht für uns wäre".

Internet-Quiz

Wie steht es um Ihre Internet-Grundkenntnisse? Sie kennen sich mit dem Internet schon aus? Aha. Dann beantworten Sie schnell die folgenden Quiz-Fragen:

☐ja
☐nein Ich kenne den Unterschied zwischen dem Internet und dem World Wide Web.

☐ja
☐nein Ich kenne die Boolesche Algebra einer Suchmaschine.

☐ja
☐nein Ich benutze PGP bzw GnuPG. weil ich nicht nur elektronische Postkarten verschicken will und weil ich keine Webcam im Schlafzimmer habe

☐ja
☐nein Ich benutze einen Newsreader, um abonnierte Newsgroups zu lesen.

☐ja
☐nein Ich weiß, wie man im Usenet ein Userprofil erstellt.

☐ja
☐nein Ich weiß, welche Software man für IRC benutzt und kann verschlüsselt und unbeobachtet chatten.

☐ja
☐nein Ich weiß, warum man einen TOR-Schlüssel nicht beim Hausmeister abgeben muss.

☐ja
☐nein Ich kann die IP-Adresse eines SMTP- oder News-Servers einer Firma zuordnen.

☐ja
☐nein Ich weiß, wie man Javascript ausschaltet und wofür das gut ist.

☐ja
☐nein Ich weiß, was ein „Thread“ ist.

☐ja
☐nein Ich benutze nicht Webmail, sondern einen vernünftigen MUA. SCNR

☐ja
☐nein Ich kann einem DAU erklären, warum man für „Phishing“ keinen Angelschein braucht.

Antworten:
„Ja“ 12 mal: Sie sind Mitglied in der „German Privacy

Foundation“ und inkognito hier.
„Ja“ 9-11 mal: Sie sollten vielleicht eher einen technischen Beruf ergreifen – der wird besser bezahlt. Bewerben Sie sich als Sysop (was ist das?) beim Innenministerium!
„Ja“ 6-8 mal: Sie sind nicht unbedarft, aber können noch etwas dazulernen.
„Ja“ 3-5 mal: Rudimentäre Vorkenntnisse sind vorhanden, aber ausbaufähig.
„Ja“ 0-3 mal: Sie haben keinen blassen Schimmer vom Internet, behaupten aber vermutlich das Gegenteil. Sie sind wahrscheinlich ein Journalist mit Facebook-Account, der über „Online-Durchsuchungen“ Artikel schreibt.

[vgl. Heise: „Studie: Wachsende Sorge um ‚digitale Außenseiter‘ – …sind 63 Prozent der Gesellschaft nicht oder wenig souverän im Umgang mit der digitalen Technik“. Ich halte den Wert von 90 Prozent für wahrscheinlicher.]

[Bitte selbst ausfüllen] fordert [bitte selbst ausfüllen]

„Für kommendes Jahr wird ein Gesetzentwurf der US-Regierung erwartet, durch das Internet-Telefonate einfacher abgehört und verschlüsselte E-Mails sowie Chat-Nachrichten besser überwacht werden sollen“, berichten Heise und netzpolitik.org.

Wie will man verschlüsselte Nachrichten „überwachen“? Von einem journalistischem Text erwarte ich, dass derartige sinnfreie Textbausteine zerhauen und der Unfug, der sich in ihnen verborgt, dem Publikum deutlich gemacht werden. Auch IRC-Nachrichten kann man nicht „überwachen“; ja, man kann

sogar verschlüsselt chatten.

„Das wirklich fürchterliche bei derart dummen Vorschlägen ist daher leider, dass helle Köpfe kostbare Zeit dafür opfern müssen, sich zu diesem Unsinn zu äußern“, steht bei netzpolitik.org. Full ack. Aber was das heisst, wissen die DAUs auch wieder nicht.

Verschwörungstherorien leben davon, dass sie immer und immer wiederholt werden. Wie heute leider auch bei Heise anlässlich eines dummdreisten Rülpsers des sattsamm bekannten Schünemann, der aus irgendwelchen Gründen „Innenminister“ in Niedersachsen ist. (Für die Nachgeborenen: wir hatten diesen Herrn hier schon vor fünf Jahren durchgenommen.)

„Weiter drängt der Innenminister auf neue Befugnisse für die Länderpolizeien wie Online-Durchsuchungen von IT-Systemen oder ‚präventive Überwachungen von Telefonaten und E-Mails‘. Bisher ist die Einsatzmöglichkeit entsprechender Spionagesoftware dem Bundeskriminalamt (BKA) vorbehalten, das davon bis zum Frühjahr nach eigenen Angaben aber noch keinen Gebrauch gemacht hatte“, schreibt Krempl und erwähnt mit keinem Wort, dass es eine derartige Software weder jemals gegeben hat noch dass es sie geben könnte. Ohne Beweise glaube ich sowieso kein Wort. Krempls suggestive Formulierungen nenne ich unseriös. Ich warte darauf, dass jemand „präsentiv“ meine E-Mails überwacht. Probiert es doch!

„If crypto is outlawed, only outlaws will have crypto.“ Yeah.

Online Erotica and Cyberporn:

on a screen near you

Jeder Mensch, der bei der Zeichenkette „Kinderpornorgrafie im Internet“ nicht gleich den Kopf zum Gebet abnimmt, weiß, dass dieser populistische Kampfbegriff den Zensur-Lobbyisten nur dazu dient, das Internet technisch zu überwachen und/oder reaktionäre gesellschaftlichspolitische Ideen durchzupeitschen. Das was von Anfang an so. Ich schrieb im September 2003 auf meinen Blog:

Gesellschaftliche Regeln Tabus besitzen eine quasi-religiöse Konsistenz: sie grenzen ein, was gesagt und gedacht werden kann, sie stiften die Identität einer Gruppe und ritualisieren den öffentlichen Diskurs darüber. In den siebziger Jahren diskutierte die Öffentlichkeit in der alten Bundesrepublik das Thema „Drogen“, hysterisch, ohne Rücksicht auf die Fakten und mit einer puritanischen Attitude als Konsens, die heute nur noch lächerlich wirkte. Niemand würde heute die Medien auf sich aufmerksam machen, warnte man davor, im „Internet“ gebe es Informationen darüber, welche Cannabis-Sorten in Holland gerade besonders günstig zu erwerben wären. Experten durften damals ungestraft in medizinische Fachbücher schreiben, Opiate wie Heroin bewirkten Hirnschäden oder Haschisch machte süchtig. Beide Thesen sind gleichmassen grober Unfug. (…)

Dieser Hype zum Thema Kinderpornografie im Internet setzte voraus, dass die Selbstkontrolle der Medien völlig versagte, weil niemand die Fakten nachprüfen wollte. Die quotenträchtige, weil angstbesetzte Schlagzeilen wie „immer mehr (Kinder)Pornografie im Netz“ versprachen offenbar mehr Wohlwollen der Rezipienten als die unbequeme Recherche, die diese Behauptung schnell ad absurdum geführt hätte. Die Berichte in den Zeitungen und Fernsehsendern der letzten fünf Jahre zu diesem Thema, die versuchen, sich der Realität anzunähern und nicht nur Presseerklärungen bestimmter Lobby-Gruppen unkommentiert übernahmen, kann man an einer Hand abzählen.

Franz Wegener schrieb 1996 in einem Artikel „Cyberpornographie: Chronologie einer Hexenjagd“ – für die mittlerweile nicht mehr existierende Zeitschrift „Intro“ des Kulturfördervereins Ruhrgebiet e.V. – : „Kaum zu glauben: Der momentane Medien-Hype über Pornogaphie im Internet, der nun auch die 200 von Compuserve gesperrten Usenet-Gruppen zum Opfer gefallen sind, basiert in erster Linie auf einem schlampig geschriebenen Artikel von Time-Autor Philip Elmer-Dewitt über die Studie „Marketing Pornography on the Information Superhighway“ von Martin Rimm…, der die Untersuchungsergebnisse einer Studie, die sich auch mit Pornographie im Internet befaßt, stark verzerrt wiedergegeben hat. Der Artikel…hatte schlicht und ergreifend keine faktische Grundlage.“

Das hinderte aber die Mehrzahl der Journalisten in Deutschland nicht daran, den Artikel als ernst zu nehmende Quelle einfach zu übernehmen. Die Nachwirkungen sind noch heute zu spüren: Wer es wagt, sich dem irrationalen Mainstream des Diskurses entgegenzustemmen, wird scheel angesehen, als sympathisiere er mit Kinderschändern. (…)

Grundlage für den berühmt-berüchtigten Artikel der Time war Martin Rimms Studie „Marketing Pornography on the Information Superhighway“ von der Carnegie Mellon Universität in

Pittsburgh. In dieser Publikation geht es um Pornography on Computer Network? – also nicht primär um das Intenet, sondern um vernetzte Computer allgemein. Die Studie beschäftigt sich vornehmlich mit rund siebzig privaten Mailboxen (Bulletin Board System, abgekürzt BBS), die in technischer Hinsicht mit dem Internet nicht verbunden und auch kein Teil dessen sind. Am Rande widmete sich Rimm drei Dutzenden Diskussionsforen im Usenet – die wiederum haben mit dem World Wide Web nichts zu tun. Im WWW analysierte der Autor circa zehntausend Seiten, er fand (im Jahr 1995) nur auf neun Webseiten harte Pornografie – Kinderpornografie überhaupt nicht.

Die Studie Rimms wurde aber als „the first systematic study of pornography on the Information Superhighway", kategorisiert, als zöge man eine Expertise der Bundesbahn über den Gleisbau zur Konzeption neuer Autobahnen heran. Im Unterschied zu Grafiken im Internet kann der Nutzer eine Mailbox nicht sehen, welche Inhalte auf ihnen zu finden sind, er muss sich nach bestimmten Schlüsselbegriffen orientieren, bevor er eine Datei auf seinen Rechner kopiert. Die Studie Rimms beschränkte sich im wesentlichen auf Mailboxen, die ihre Inhalte selbst als „commercial" oder gar „adult" anpriesen – kein Wunder, dass dort Pornografie zu finden war. Das war ihr eigentlicher Zweck.

Man kann die Geschichte dieses Hypes nicht rational diskutieren. Das scheitert in der Regel daran, dass Zensur-Lautsprecher wie Bosbach, Volksverdummer wie der BKA-Präsdident Ziercke oder die Jugendschutzwarte gar nicht wissen, was eine Mailbox ist. Sie werden daher auch nicht begreifen, dass „Cyberporn" schon immer viel Lärm um nichts Wichtiges war.

Auf Zeit Online lesen wir heute das aktuelle Update des Hypes. „Cyberporn" wurde im lauf der Jahre ersetzt durch die Sprechblase „Kinderpornografie". Die Parole „Löschen statt sperren" ist nur deshalb erfunden worden, um den Befürwortern der Sperrlisten und sinnfreien Stoppschildern den Wind aus den

Segeln zu nehmen. Leider haben auch die Guten diese Parole aufgegriffen, weil man froh sein muss, dass der gesellschaftliche Konsens der Komitess für die unmoralischen Umtriebe im Internet nicht die einstweilige Erschießung von Leuten wie mir durchgesetzt haben. In Wahrheit ist „Löschen statt sperren" genau so ein Quatsch wie Sperrlisten – es gibt nicht zu sperren, was des Sperrens würdig wäre.

Schauen wir uns doch die Liste der Websites an, auf die das BKA ein virtuelles Auge geworfen hat. Kein einziges deutschen Medium hat erwähnt, dass die US-amerikanische gesetzliche Grundlage, was „Kinderpornografie" sei, eine andere ist als die deutsche und dass deutsche Behörden weder das Recht noch die geringste Chance haben zu fordern, dass die dortigen Provider „einschlägiges" Material löschen. Und natürlich kann jeder in zehn Sekunden herausfinden (das ist *keine* Website mit Kipo, Herr Internet-Blockwart!), welche Firma welchen Server hostet – und das nicht nur in den USA, sondern weltweilt. Wer diese beiden wesentlichen Fakten unterschlägt, ist ebenfalls ein Volksverdummer.

„Von Erfolg oder Misserfolg der Löschbestrebungen hängt ab, wie es mit dem sogenannten Zugangserschwerungsgesetz weitergeht", schreibt Zeit online affirmativ. Wer das Orwellsche Neusprech der Zensur-Lobby übernimmt und statt Zensurgesetz „Zugangserschwernisgesetz" sagt, outed sich selbst als jemand, der nicht weiß, was Journalismus sein könnte.

Der Artikel auf zeit Online nennt auch keinen Autor. Das liegt vermtulich daran, dass man bei moraltheologischen Themen wie Drogen, Rechtsextremismus und Kinderpornograpfie im internet auch die Volontäre ranlassen kann. Recherche (*Wo, verdammt noch mal, gibt es öffentliche zugängliche Kinderpornografie im World Wide Web? Nicht zu vergessen: World Wide Web bekanntlich kein Synonym für Internet.*) ist nicht erwünscht und man weiß ja eh, was bei dem Artikel herauskommt.

Liebe wohlwollende Leserin und lieber geneigter Leser! Sie werden verstehen, dass mich das Thema nur noch ankotzt und ich keine Lust habe, darüber auch nur ein Wort zu verlieren. Man ist nur noch von einem Haufen Irrer umgeben.

Skype: Heimlich auf den Rechner spielen

Auf Law blog wird eine Vorausmeldung von Spiegel offline erwähnt: „Zoll hört auch Skype-Telefonate mit“ – „Für die Bundesregierung handelt es sich um einen Fall zulässiger Quellen-Überwachung. Es würden nur laufenden Telekommunikationsvorgänge überwacht. Das kann man allerdings auch anders sehen. Jedenfalls dürften nach der Infiltration des genutzten Computers keine sonderlich großen Hürden bestehen, um das gesamte System auszuspähen.“..

Da schlägt natürlich sofort die Stunde der Verschwörungstheoretiker, die gepflegtes Halbwissen, fehlende Recherche, urbane Märchen und das geheimnisvolle, aber unsubstantiierte Geraune, „sie“ seien schon „drin, wir wüssten

das nur nicht, zusammenmischen, bis man endlich „Online-Durchsuchung“ drüber schreiben kann.

Ganz besonders dämlich formuliert Spiegel Offline: „Nach SPIEGEL-Informationen spielen die Ermittler auf die Computer von Verdächtigen heimlich ein Programm zum Mitlauschen auf. (…) Diese Überwachung beziehe sich ‚ausschließlich auf Daten aus laufenden Kommunikationsvorgängen‘ und stehe damit im Einklang mit dem Urteil des Bundesverfassungsgerichts zur sogenannten Online-Durchsuchung.“

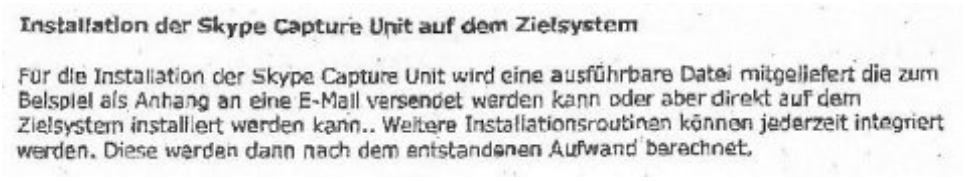
Dieser Quatsch ist gleich mehrfach zu beanstanden. Zum einen ist es kein Journalismus, wenn man zu bestimmten Themen ausschließlich „innenpolitische Sprecher“ und andere Lobbyisten zu Wort kommen lässt. Es geht nicht darum, wie politische Parteien die Welt sehen wollen, sondern darum, wie sie ist. Ein Journalist sollte den Ehrgeiz haben, die Leserinnen und Leser aufzuklären. Wenn das nicht geschieht, handelt es sich um Propaganda oder um das Verbreiten von Gerüchten.

Bei Compliance-Magazin.de lesen wir zum Beispiel: „Auf die Frage der Liberalen, wodurch sich die Quellen-TKÜ von der Online-Durchsuchung unterscheide, verweist die Regierung darauf, dass bei diesen beiden Maßnahmen ‚lediglich die Technik der Vorgehensweise ähnlich‘ sei. Durch programmtechnische Vorrichtungen bei der Quellen-TKÜ sei von vornherein sichergestellt, dass eine ‚über den Überwachungszweck hinausgehende Online-Durchsuchung nicht möglich ist‘.

Auch davon ist jedes Wort gelogen. Wenn man das suggestive Bürokraten-Neusprech unkritisch übernimmt, wird die Realität eben nur vernebelt. Deswegen sind diese Wortungetüme wie „Quellen-Telekommunikationsüberwachung“ übernommen worden – niemand sollen wissen oder gar begreifen können, um was es sich eigentlich handelt. Das Abhören von Telefonaten ist in der TKÜV geregelt; das ist eine ganz andere gesetzliche

Grundlage als, die für den heimlichen behördlichen Zugriff auf fremde Rechner benötigt würde. Wer beides vermischt, hat entweder nichts begriffen oder will bewusst verwirren.

Udo Vetter scheint vergessen zu haben, dass er zum Thema Skype schon am 17.8.2010 gebloggt hat. Er verwies damals auf den Wikipedia-Eintrag zu Skype, wo man lesen kann, worum es eigentlich geht. Natürlich kann man Skype anhören, aber nicht mit Methoden, die der real gar nicht existierenden „Online-Durchsuchung" irgendwie ähneln. Man kann also mitnichten, wie Spiegel offline suggiert, einfach so „heimlich" ein Programm auf fremde Computer „spielen." Nein, das kann man nur, wenn man den physikalischen Zugriff hat und Software installieren darf (der Besitzer des Rechner muss also ein Dau sein.)



Installation der Skype Capture Unit auf dem Zielsystem

Für die Installation der Skype Capture Unit wird eine ausführbare Datei mitgeliefert die zum Beispiel als Anhang an eine E-Mail versendet werden kann oder aber direkt auf dem Zielsystem installiert werden kann.. Weitere Installationsroutinen können jederzeit integriert werden. Diese werden dann nach dem entstandenen Aufwand berechnet.

auf der Website der Piratenpartei Bayern kann man im Detail nachlesen, wie die sich Fall von Skype vorstellen.

Eine ausführbare Datei, die per E-Mail-Anhang verschickt werden kann? Da lachen ja die Hühner!. Und die installiert das Zielobjekt nichtsahnend? Und der Verdächtige hat auch weder einen Mac noch Linux? Ich zitiere mich selbst vom 27.08.2009:

In der Heise-Meldung von gestern heisst es: „Ein Schweizer Software-Entwickler hat auf seinen Seiten den Quelltext zu einem Programm veröffentlicht, das verschlüsselte Kommunikation über Skype heimlich belauschen kann. Das Programm ist dazu vorgesehen, als Trojanisches Pferd auf einem PC eingeschmuggelt zu werden. Dort klinkt es sich nach Angaben des Autors in den laufenden Skype-Prozess ein, schneidet die Audio-Daten der Gespräche heimlich mit und lädt sie dann als MP3-Dateien auf einen externen Server."

Ds habe ich mir genauer angesehen. Das Trojanische Pferd ist

mitnichten ein „Bundestrojaner“, den es bekanntlich nicht gibt, sondern das Programm Minipanzer: „Minipanzer is a trojan horse that disguises as any kind of file type and when executed on a victims system it collects all sensitive data like account information etc. and sends it to an email address owned by the attacker. It is a one-shot-trojan. It doesn’t install on a target system but only executes its payload and removes itself afterwards.“

Im dazugehörigen Blog heisst es: „The code is simple and straightforward. You have know malware development is no rocket science and if you expect big magic you are at the wrong place.“ Am besten hat mir der Kommentar „Giovannis“ gefallen: „Despite what some people say, Skype has never been secure. It is relatively easy to hack skype accounts, skype does not even check if the same user logs in simultaneusly on different machines and what is worst, the second user can get a copy of all the chats. Skype is good for housewifes that want to chat a bit with their kids, but for confidential conversations the use of strong voice encryption is required. In our company we tested many of them, we now keep with PhoneCrypt from securstar as it proved to be very good, stable, and with an excellent voice quality.“

Ich verweise auf mein hiesiges Posting „“Bayerntrojaner” zum Abhören von Internet-Telefonie?“ sowie auf meinen Artikel in der Netzeitung: „Wenn der Laptop zweimal klingelt“.

Auf law blog gab es einen interessanten Kommentar: „@mark: es geht um einen einfachen Audio-Capture-Client mit Streamingfunktion der sich fernwarten lässt. Der Programmieraufwand dafür beträgt ca. 20-30 h. Dazu kommt dann die Sonderfunktionalität für Skype die man noch mal mit der gleichen Zeit veranschlagen kann. Dazu noch Tests sowie der Server. Alles in allem ein Projekt, dass sich mit nur einem Mann-Monat stemmen lässt. Selbst bei einem Stundenpreis von vollkommen utopischen 500€ für den Entwickler reden wir hier von Entwicklungskosten im sehr niedrigen 5stelligen Bereich.

Bei den Preisen muss die Software nur ein einziges Mal zum Einsatz kommen, damit sie sich für die entwickelnde Firma rechnet. Ich bleibe dabei: hier wird über den Tisch gezogen.“

Nach mal langsam zum Mitschreiben: Man kann nichts heimlich auf fremde Rechner spielen, wenn der Besitzer das nicht will. Kapiert?

Massenwahn “Kinderpornografie im Internet”, reloaded

„BKA will Besitz und Verbreitung von Kinderporno-Links kriminalisieren“, berichtet Heise. Dem BKA geht es offenbar gar nicht mehr um rationale Argumente oder um Verfolgung der Täter, sondern ausschließlich um Zensur-Lobbyismus. Das zeigt die „Analysis of a representative example of European blacklists„, die der Arbeitskreis Zensur (AK Zensur) vorgelegt hat:

Results:
•Three domains were found to contain illegal child abuse images.
•Two of these have been on the Danish blacklist since 2008 and were also blocked in Norway, Finland and Sweden. After sending an abuse message to the hosting provider in the USA, the websites were removed in less than 30 minutes. This suggests that the police did nothing to shut these sites down for about two years.
•One domain has been on these blacklists since about spring 2010, in the TLD .in (India), hosted in the Netherlands. The domain was suspended by the Indian domain name registry three hours after a request was sent.

•More than half of the blocked domains (92) were already deleted.
•Many domains (66) were not registered anymore.
•Some domains (6) did not contain any child abuse images or obvious illegal content.

Summary:
The vast majority of the blocked domains are no longer active. Only a few still are.
•164 domains were blocked in Denmark, but offered no illegal material or were not connected at all at the time of our investigation.
•3 of the blocked domains were found to contain child abuse images, even though two of them had been blocked for as long as two years. After 30 minutes and 3 hours of action respectively, they were taken down by their webhoster or registry. This could have been achieved much earlier. All we had to do was to send a few emails.

„‚Das Ergebnis ist eine Blamage für die Strafverfolgungsbehörden‘‚, meint Alvar Freude vom AK Zensur, da von allen untersuchten Links lediglich drei Seiten tatsächlich Inhalte enthielten, ‚die als Kinderpornografie eingestuft werden können‘. (…) Trotzdem habe es offensichtlich ‚keine Versuche von Seiten der Strafverfolgungsbehörden‘ gegeben, diese illegalen Inhalte aus dem Netz zu entfernen.“

Wen wundert das…. Mich wundert auch nicht, dass ausser Heise kein deutsches Medium darüber berichtet. Der Opportunismus der Mainstreamholzmedien ist vergleichbar mit der Zeit der US-amerikanischen McCarthy-Ära: Der Staat braucht die öffentliche Meinung und die Medien nicht zu zensieren. Wenn die vom Massenwahn und der allgemeinen Hysterie schon infiziert sind, funktioniert die Gleichschaltung auch so.

Irgendwie erinnert mich das Krankheitsbild des Massenwahns „Kinderpornografie im Internet“ an einen Roman von Camus, den ich in meiner Schulzeit lesen musste (leider auf französisch –

vieles habe ich damals gar nicht verstanden): „Die Pest„. Thema: „die ständige Revolte gegen die Sinnlosigkeit der Welt“. Man kann gegen die Hysterie und Kritiklosigkeit deutscher Medien nicht argumentieren. Man kann auch gegen andere psychische Krankheiten, etwa Schizophrenie“, nicht argumentieren. Wer Stimmen hört, wird sich von einem Beweis, dass es diese gar nicht gäbe, nicht von seiner Meinung abbringen lassen.

Anthropologen, Ethnologen und Soziologen späterer Epochen werden über die Hysterien und Exorzismen des beginnenden Internet-Zeitalters sowie deren urbane Märchen („Kinderpornografie im Intenet“, „Online-Durchsuchung“) sicher interessante wissenschaftliche Arbeiten verfassen und schmunzelnd den Kopf schütteln, wie wir heute über die Kinderkreuzzüge, – ähnlich wie Elias Canetti in „Masse und Macht“ den „psychischen“ Zustand großer Menschengruppen genial beschrieben hat.

Andreas Pfitzmann ist tot

Heise: „Sicherheitsexperte Andreas Pfitzmann verstorben (…) Letzte Forschungsprojekte waren „anonymes Websurfing“ (JAP), „Privacy and Identity Managment in Europe for Life“ (PrimeLife) und „Steganographie“ (Nachruf der TU Dresden – Fakultät Informatik, Nachruf des CCC).

Wenn auch nur ein Politiker, der über „Online-Durchsuchungen“, Krytografie und über das Internet an sich faselt, einen Bruchteil des Wissens von Andreas Pfitzmann hätte, dann sähe die Welt vermutlich besser aus.

Telekommunikationsüberwachungsverordnungsmaßnamen

Ich musste mich regelrecht prügeln, zum Entenbraten, auch bekannt als der einflussreichste Hoax des Jahrzehnts, auch bekannt als das Märchen von der real gar nicht existierenden und technisch nicht umsetzbaren so genannten „Online-Durchsuchung“ etwas zu verfassen. Wie gewohnt ist die Berichterstattung der ahnungslosen Medien interessanter als das Faktum selbst. Natürlich fordert ein Innenminister immer schärfere Gesetze, ungeachtet seiner Parteizugehörigkeit und seines Charakters, falls vorhanden, hieße er Schily, Schäuble oder de Maiziere. Das Sein bestimmt das Bewusstsein, und ein Innenminister, der sich ausschließlich von opportunistischen Karrieristen, Zensur-Propagandisten, ahnungslosen Dampfplauderern (ja, ich denke an Bosbach) und Lobbyistne des Überwachungsstaats umgibt und qua Amt umgeben muss, der trägt immer den unvermeindlichen Komparativ auf den Lippen: Der Staat muss härter melden, durchführen und verbieten.

Bei Heise las ich die irreführende Überschrift: „De Maizière will heimliche Online-Durchsuchungen auch zur Strafverfolgung“. Der Kollege Krempl ist für merkwürdige und suggestive Formulierungen schon einschlägig bekannt: „Zudem macht sich de Maizière für den Einsatz heimlicher Online-Durchsuchungen zur Strafverfolgung stark. Bisher darf allein das Bundeskriminalamt (BKA) zur Abwehr terroristischer Gefahren verdeckt auf IT-Systeme Verdächtiger zugreifen. Der Innenminister drängt nun auf eine Verwertungsbefugnis für Daten, die mit dem Bundestrojaner gewonnen werden, in der Strafprozessordnung (StPO).“

Kein Wort darüber, dass der „verdeckte Zugriff“, der hier

suggeriert wird, weder bisher ein einziges Mal stattgefunden hat noch jemals so stattfinden wird. Auch ist die Bezeichnung „Bundestrojaner“ Schaumschlägerei, weil es diesen „Trojaner“ (es müsste eigentlich Trojanisches Pferd heissen, die Trojaner standen aussen um den antiken hölzernen Gaul herum) gar nicht gibt. Aber Krempl drückt eben wie der mediale Mainstream die Zahnpaste weiter aus der Tube. Man muss Unfug nur lange genug wiederholen, irgendwann glaubt jeder daran. Aber der Begriff ist eben so sexy, da kann niemand widerstehen.

Welt Offline hat etwas genauer formuliert: „Im Einzelnen will de Maizière dem Verfassungsschutz die Erlaubnis zur sogenannten ‚Quellen-Telekommunikationsüberwachung‘ (Quellen-TKÜ) geben.“ Diese Wort-Ungetüm wird immer dann ins Spiel gebracht, wenn niemand mehr nachfragen soll, was eigentlich gemeint ist. Die fromme Legendenbildung der Überwachungslobby hat bekanntlich zur Sprachregelung geführt: Man muss die Daten der Kriminellen überwachen, bevor sie auf den Knopf zum Verschlüsseln drücken. So stellen die sich das vor. Das Neusprech hat seinen Weg in die Medien auch deshalb gefunden, weil die brav jedwedes Deutsch des Grauens nachplappern, ohne ihrer verdammten Pflicht nachzukommen, dieses gespreizte Bläd- und Furzbürokratendeutsch in kleine und verständliche Teile zu zerhacken. Man geriert sich als Durchblicker, wenn man den Quatsch und jeden Jargon übernimmt. Ich sage nur: Telekommunikationsüberwachungsverordnungsdurchführungsmaßnahmen.

Die so genannten „Quellen-TKÜ“ hat auch mit dem, was bei DAUs und im Volksmund als „Online-Durchsuchung“ bezeichnet wird, gar nichts zu tun, sondern handelt davon, wie man Telefonie und E-Mails belauschen soll.

Ich habe keine Lust, alles immer zu wiederholen. Also zitiere ich mich selbst: *Krempl (..:), hier diese Rezension weiterlesen: „Als nächstes zeigen die Autoren, dass es sich bei der Online-Durchsuchung um ein sich selbst verstärkendes Phänomen handelt, das aus unklaren Definitionen darüber*

herrührte, was mit der Online-Durchsuchung eigentlich gemeint sein soll. Gepaart mit dem Mythos des allmächtigen Hackers schaukelte sich die Darstellung der Online-Durchsuchung in den Medien zu immer größeren Horrorszenarien auf, die man letztlich als nahezu faktenfrei bezeichnen kann. Die einzig gesicherten Fakten waren nur die Berichte in den Medien, nicht deren Inhalt. Aus der vielleicht noch anfangs verwendeten konjunktiven Form ‚könnte' wurden dann konkrete Forderungen von Politikern. Journalisten stellten suggestive Fragen, ob es denn solche Fälle nicht schon längst gegeben habe, und weil man nicht genau wusste, was mit ‚Online-Durchsuchung' gemeint ist (oder was man selbst darunter versteht) und man es mit anderen Verfahren vermischte/verwechselte, ergab sich das Bild, dass schon seit langem dieses Verfahren ohne Rechtsgrundlage abgelaufen ist. Dies Alles, gepaart mit dem fehlenden Sachverstand, führte zu dem schon genannten ‚Medien-Hype'. Beim Lesen dieses Teils des Buches kommt man aus dem Staunen über diese Vorgänge nicht heraus. Steht es so schlecht um den Journalismus in Deutschland?"

Zitat im Zitat: *Ich zitiere mich selbst: „In Wahrheit hat es eine „Online-Durchsuchung" oder gar den „Bundestrojaner", der seit geraumer Zeit durch die Medien geistert und sogar einen eigenen Eintrag bei Wikipedia bekommen hat, nie gegeben – und es wird ihn auch nie geben. Er ist ein Hoax und beruht auf dem mangelnden Sachverstand eines Oberstaatsanwaltes, jeweils einer Falschmeldung der taz und der Süddeutschen und der Tatsache, dass alle deutschen Medien, ohne die Fakten zu recherchieren, voneinander abgeschrieben haben. Nach dem Prinzip ‚Stille Post' steht am Ende der Berichterstattung dann der ‚behördliche' Hacker, vom dem am Anfang nie die Rede war."*

Ceterum censeo: Der Kaiser ist nackt! Es gibt keine ‚Bundestrojaner'!

So zynisch und dumm ist stern.de

Ein Tweet Maik Söhlers machte mich darauf aufmerksam: „Der dümmste Text seit 100 Jahren„. Ja, man kann dem polemisch zustimmen. Es geht um das beliebte und medienkompatible Thema „Amoklauf“ (in Lörrach), wo das herkommt und wo das alles enden wird.

Anlass ist ebenfalls ein Tweet: „Die Amokläuferin von #Lörrach: heterosexuell, verheiratet, katholisch, Juristin. #Bosbach weiß noch nicht so richtig, was er verbieten will.“

Felix Disselhoff („Multimedia-Journalist, 26“) verbreitet auf stern.de eine dumpfe Mischung aus purer Faktenfreiheit, suggestiver Meinung und moraltheologischen Gefasel. Das kann man belegen: Disselhoff hat noch nicht einmal die Grundlagen des Internet begriffen und verwechselt das „Web“ mit dem Internet. Was soll das heißen: „gibt sich das Web recht zynisch“? Was ist mit der Usenet-Gemeinde und der IRC-Gemeinde und der Filesharing-Gemeinde, wenn es eine „Netzgemeinde“ gäbe? Wenn man gar nicht mehr weiß, wo „es“ im Internet steht, dann schreibt man eben „im Netz“. Worüber reden wir hier eigentlich?

Das ist jetzt keine Erbsenzählerei. Wenn ein Verkehrsexperte eine Auto nicht von einer Lokomotive unterscheiden könnte, sich aber anmaßte, über Binnenschifffahrt zu räsonnieren, würde man sicher an seiner Kompetenz zweifeln. Das Internet existiert seit 1969, das World Wide Web aber erst seit 1991 bzw. 1993. Wie sah denn, Herr „Multimedia-Journalist“ Disselhoff, das Internet zwischen 1969 und 1990 aus?

„Ob, wie von ‚Zyneasthesie, [diesen Nutzer gibt es nicht,

stern.de! BS] behauptet, die Täterin verheiratet und heterosexuell war und ob sie katholischen Glaubens ist, stand zum Zeitpunkt des ersten Tweets noch gar nicht fest. Trotzdem verbreiteten sich die 138 Zeichen rasant. Damit wird einmal mehr deutlich, wie Kommunikation über Dienste wie Twitter, Facebook und Co. funktioniert: schnell.“ Das ist erstens nicht wahr und zweitens Deutsch des Grauens. Damit wird einmal mehr deutlich, wie Kommunikation über Holzmedien wie stern.de und Co. funktioniert: dumm und langsam.

„Das Problem ist wie so oft nicht die Nachricht, sondern wie mit ihr umgegangen wird. Während ausgebildete Journalisten darin geschult sind, sensibel mit Daten von Personen umzugehen und Fakten zu recherchieren, steht hingegen bei Twitter die Meinung schnell fest. Der Pressekodex gilt nun einmal nur für die Presse.“

Auch hier eine schlichte Falschmeldung. Auf der Website des Presserats heißt es: „Im Internet ist der Presserat ab dem 1.1.2009 für journalistisch-redaktionelle Beiträge zuständig, sofern es sich nicht um Rundfunk handelt.“ Außerdem, Kollege Disselhoff, ist der Presserat keine Behörde, vor der der Deutsche an sich gleich auf die Knie geht, sondern seine bloße Lobby-Organisation und ein Verein. „Mitglieder sind nur die vier Verbände, die auch den Trägerverein bilden: der Bundesverband Deutscher Zeitungsverleger (BDZV), der Verband Deutscher Zeitschriftenverleger (VDZ), der Deutsche Journalisten-Verband (DJV) und die Fachgruppe Journalismus in Ver.di.“ Also nichts, was man besonders ernst nehmen müsste.

„Die Presse“ sind nach der Rechtsprechung des Bundesverfassungsgerichts auch Medienerzeugnisse von Bürgern, die dem Zweck der demokratischen Willensbildung und der Aufklärung dienen. Darunter fallen heute insbesondere Blogger und immer noch Leute, die einfache Flugblätter verfassen.

Außerdem darf ich als Journalist darauf hinweisen, dass das selbstbeweihräuchernde Geschwätz, „ausgebildete“ Journalisten

würden Fakten recherchieren, bloße Agitprop ist und der Realität nicht mehr entspricht. (Ich will ja nicht schon wieder mit dem einflussreichsten Hoax des Jahrzehnts kommen.)

Das Internet ist laut Disselhoff „ein Medium, welches von vielen fälschlicherweise als die Zukunft des Journalismus betrachtet wird“. Da hat der Kollege aber Meinung und Fakten „sauber“ getrennt! Das kommt davon, wenn man nie über den Suppenteller der Holzmedien, welche von vielen fälschlicherweise als die Zukunft des Journalismus betrachtet wird, hinausgeblickt hat.

„Aus einer einzelnen Meldung wird eine Lawine, die den Wahrheitsgehalt (…) oft unter sich begräbt.“ Mit diesem Satz kann man leben. So war es bei der so genannten „Online-Durchsuchung“, so ist es bei dem vom stern.de mitfinanzierten, aber um so erfolgloseren „Kampf gegen Rechts“ (man soll sich auch mit der „guten Sache“ nicht gemein machen, stern.de!) und auch bei dem moralinschwangerem und Hysterie-kompatiblen Schlagwort „Kinderpornografie im Internet“. Die „Fakten recherchierenden“ Journalisten haben sich wahrlich nicht mit Ruhm bekleckert (nein, die gar nicht existenten Massenvernichtungswaffen im Irak und den Hufeisenplan lassen wir auch weg).

Mal ganz am Rande: Was will uns der Künstler auf stern.de eigentlich sagen? Dass „das Internet“ schlechteren Journalismus bietet als die Holzmedien?

Wie Schopenhauer schon in Die Welt als Wille und Vorstellung schrieb: „In diesem Geiste also arbeitend und während dessen immerfort das Falsche und Schlechte in allgemeiner Geltung, ja, Windbeutelei und Scharlatanerei in höchster Verehrung sehend, habe ich längst auf den Beifall meiner Zeitgenossen verzichtet.“ Das ist auch das Motto dieses kleinen Blogs.

Von E-Mail-Standorten, mythischen Hackern und Kampfjets

Spiegel offline (von DAUs auch Spiegel „Online“ genannt) und Computer und die Berichterstattung dazu – das passt irgendwie nicht zusammen, Als Quelle der Heiterheit ist es jedoch immer gut. Heute, liebe Kinder, nehmen wir den Standort einer E-Mail durch (ja genau, ihr habt richtig gehört und auch im Internet-Unterricht aufgepasst – brav!) und die chinesische Lockheed Martin F-35 (ja, ein Kampfjet und fast genau so schnell wie eine E-Mail!).

„Spott über Polizei wird Bankräuber zum Verhängnis“, heisst es heute bei SpOff. „Nun schrieb der 19-Jährige in Hamburg eine Mail an Zeitungen und Polizei und machte sich über die Fahnder lustig – wohl ohne zu wissen, dass der Standort jedes Computers ermittelt werden kann. Vier Stunden später nahmen ihn Beamte auf der Reeperbahn in einem Internetcafé fest…“

Wissen wir eigentlich, was gemeint ist? Nicht wirklich. Also lesen wir gemeinsam: „E-Mail-Header lesen und verstehen, dort das Kapitel „III. E-Mail-Headerzeilen im einzelnen“, genauer: das Unterkapitel „b) „Received:“-Headerzeilen im einzelnen“.

*Received: from mx3.gmx.example (qmailr@mx3.gmx.example [195.63.104.129]) Hier steht jetzt, von welchem Mailserver die E-Mail empfangen wurde. Das Format dieser Zeile ist leider nicht ganz einheitlich. Immer gilt: die Nummer in (eckigen) Klammern ist die unverwechselbare IP-Nummer des einliefernden Rechners – hier „195.63.104.129“. Außerdem ist angegeben, wie dieser sich vorgestellt hat (die Angabe aus dem HELO) – hier „qmailr@mx3.gmx.example“. Das hat unser Mailserver brav überprüft und festgestellt, daß die IP-Nummer tatsächlich zu „mx3.gmx.example“ gehört. (…) Wenn HELO und Realität übereinstimmen, wird der HELO-Parameter manchmal gar nicht angegeben. Dann findet sich nur die IP-Nummer und der (als richtig festgestellte) Name des einliefernden Servers. Andererseits geben manche MTA nur den (möglicherweise gefälschten) HELO-Parameter und die (echte) IP-Nummer an, ohne den zugehörigen Namen nachzuschauen. Dann ist der angegebene Name gerade *nicht* wahr. Auch ist es möglich, daß die Reihenfolge der Angaben genau umgekehrt ist (zuerst HELO, dann tatsächliche Angabe). Schließlich – und am schlimmsten :-(– gibt es ältere MTAs, die noch an das Gute im Menschen glauben und außer dem (beliebig fälschbaren) HELO überhaupt nichts festhalten.*

Alles klar? Puls und Atmung noch normal? Noch mal zum Mitschreiben: Die IP-Adresse ist *nicht* der *Standort* eines Computers, obwohl diejenigen, die an das Märchen der „Online-Durchsuchung“ glauben, das anders sehen (möchten). Was könnte also passiert sein? Hat der doofe Bankräuber seine Webmail-Adresse (DAU-kompatibel: gmx, yahoo, google mail usw.) benutzt, um eine E-Mail an lka.7011@hamburg.de zu schreiben? („Ihre Nachricht wird nur während der normalen Bürostunden gelesen.“ Bankraub bitte nur während der normalen

Bürostunden?) Nein, hat er nicht, dann müsste man die Pointe anders formulieren. Im Header der E-Mail wird also die IP-Adresse eines SMTP-Server gestanden haben, den man dem Internet-Café zuordnen konnte.

Was aber, wenn er ein Laptop und ein offenes WLAN benutzt hätte? Pustekuchen, mal abgesehen von denen, die wissen, wie man eine anonyme E-Mail schreibt. Der Standort eines jeden Computers kann keinesfalls so ermittelt werden. Der Satz ist schlicht grober Blödsinn.

Und jetzt zu etwas ganz Anderem.

Schön ist heute auch die Bildunterschrift einer Spiegel-Offline-Fotostrecke über die „F-35 „Lightning II“: „2009 stahlen Hacker große Mengen an geheimen Daten über das Flugzeug. In den USA wurde China verdächtigt.“ Immer wenn das Wort „Hacker“ in deutschen Medien auftaucht, muss man zwei Mal hinschauen und fragen: Ist das wirklich wahr? Oder wieder nur ein Hoax, ein modernes Märchen oder bewusste Volksverarschung?

Jetzt wird’s lustig – wo haben die das wieder abgeschrieben, ohne zu recherchieren? Wikipedia: „Im April 2009 kam es gemäß einem Bericht des Wall Street Journal zu einem Hackerangriff auf Daten des F-35 Projekts. Dabei wurden größere Mengen Daten aus Rechnern des US-Verteidigungsministeriums gestohlen. Laut

Pentagon wurden dabei jedoch keine weitreichend sensiblen Daten kopiert."

Die Suche nach dem ursprünglichen Tagesschau-Link führt zu Websites, die Verschwörungstheorien verbreiten, die pöhsen Chinesen stünden hinter allem und jedem Byte, das auf eine krumme Bahn gerät – also ungefähr das Niveau der antichinesischen Agitprop, die hierzulande ungefiltert in den Medien breit getreten wird.

In einem ForumGermanicum wird man fündig – dort steht noch die Tagesschau-Meldung von damals:

Unbekannte Computer-Hacker haben einem US-Zeitungsbericht zufolge das teuerste Waffenprojekt in der Geschichte des Pentagon geknackt. Die Täter hätten große Datenmengen aus den Rechnern des US-Verteidigungsministeriums kopiert, darunter auch Detailpläne des neuen Kampfflugzeugs F-35 Lightning II, berichtete das ‚Wall Street Journal unter Berufung auf Regierungskreise. (…) Im Fall des Kampfjets steht der Zeitung zufolge noch nicht fest, wie groß der sicherheitstechnische und finanzielle Schaden ist. Eingedrungen seien die Cyberspione über Schwachstellen in den Netzwerken von zwei oder drei an dem Projekt beteiligten Unternehmen. Zwar hätten die Internetspione mehrere Terabyte an Daten über Design und Elektronik des Kampfflugzeugs abgegriffen. Das geheimste Material sei allerdings sicher geblieben. Es ist demnach auf Computern gespeichert, die nicht mit dem Internet verbunden sind. (…) Pentagon-Sprecher Bryan Whitman kommentierte den Bericht mit dem Hinweis, dass nach seinem Wissen keine sensiblen Daten geknackt worden seien."

Unter Berufung auf Regierungskreise. Offenbar. Internetspione. Ein seriöses Medium hätte die Quelle verlinkt. „Computer Spies Breach Fighter-Jet Project", titelte das Wall Street Journal (also *nicht* „einem US-Zeitungsbericht zufolge" – die Tageschau verschweigt sogar die Quelle und schämt sich noch nicht mal dafür.).

Die Datendiebe sind also in ein schlecht gesichertes Firmennetzwerk eingedrungen, das mit dem des Pentagon verbunden war. „Former U.S. officials say the attacks appear to have originated in China. However it can be extremely difficult to determine the true origin because it is easy to mask identities online. A Pentagon report issued last month said that the Chinese military has made ’steady progress‘ in developing online-warfare techniques. China hopes its computer skills can help it compensate for an underdeveloped military, the report said.“

Es geht also nur darum, die eigene Schlamperei, das Netzwerk betreffend, als chinesischen „Hacker“-Angriff auszugeben. Nichts Genaues weiß man ohnehin nicht, weil die Journalisten von „ehemaligen“ Angestellten des US-Verteidiungsministeriums gebrieft wurden. Da die Chinesen immer besser und immer böser würden, brauchten die Militärs jetzt mehr Geld – das soll dem Leser suggeriert werden.

Ich glaube wieder mal kein Wort von dem, was in der Zeitung steht, noch nicht mal den Bildunterschriften bei Spiegel offline.

Enten, dreifach gebraten und gewendet, revisited

Die geneigte Leserin und der geneigte Leser werden, ähnlich wie ich, bei der Lektüre dessen, was die Holz- und Mainstream-Medien zum Thema Internet absondern, fragen, ob man nicht stattdessen ganz etwas Anderes schreiben könnte, etwa: „Ἄνδρα μοι ἔννεπε, Μοῦσα, πολύτροπον, ὃς μάλα πολλὰ πλάγχθη, ἐπεὶ Τροίης ἱερὸν πτολίεθρον ἔπερσε“ oder etwa „□□□□□□ □□ □□□ □□□□

□□□□ □□□□□ □□ □□□□□ □□□□□□□ □□□□□ □□□ □□□□□ □□□“. Das würde sich besser anhören und genauso viel oder wenig aussagen – und man fühlte sich auch noch humanistisch-gebildet (Homer!) und moraltheologisch (Talmud!) besser nach der Lektüre… Oder vielleicht einen Psalm.

Was lasen wir vor einigen Tagen bei Spiegel Offline über „Cybercops“ aus Bayern, „die auf höchstem technischen Niveau operieren“? Die werden jetzt dort eingestellt. Der Grund: Die Bösen im Internet werden immer böser. „Die Spione hacken sich meist unbemerkt über sogenannte Trojaner in die Systeme auch kleiner und mittelständischer Unternehmen und saugen Daten ab. ‚Alle zwei Sekunden wird irgendwo auf der Welt eine Schadsoftware ins Netz gestellt‘, so der bayerische LKA-Präsident Peter Dahte.“

Nun, wenn das ein leibhaftiger Präsident sagt, dann muss es ja stimmen und alle Holzmedien müssen es unkritisch nachplappern, allen voran Spiegel Offline. Ich war bisher – offenbar irrig – der Meinung, die Aufgabe von Journalisten sei es, die Öffentlichkeit aufzuklären und hohle Sprechblasen aufzustechen und als das darzustellen, was sie sind – heiße Luft.

Man kurz nachgehakt: Die „Spione“ machen also immer öfter diese berühmt-berüchtigen „Online-Durchsuchungen“, an denen unsere auf höchstem Niveau operierenden Sicherheitskräfte so kläglich scheitern – und nicht nur, weil ihnen das vom Bundesverfassungsgericht ohnehin verboten worden ist? Und dann auch noch mit „Trojanern“? Kann mir mal jemand erklären, wie das zielgerichtet geht? Man schickt allen Mitarbeitern einer Firma eine – natürlich unverschlüsselte! – E-Mail mit einem Attachment, was sich an sämtlichen EDV-Experten vorbeihangelt und sich auch selbst installiert, weil ja bekanntlich alle Menschen mit Admin-Status online sind und auf alles klicken und alles installlieren, was nicht bei drei auf dem nächsten Baum ist? Ganz nebenbei: Woher weiß der Dahte das mit den „alle zwei Sekunden“?

Ich sag euch was: Das ist genau so ein sinnfreies Gefasel und ein Lügenmärchen wie man es gewöhnlich vom Präsidenten Ziercke zur „Online-Durchsuchung“ kennt. Wenn ich nicht so unglaublich höflich wäre, würde ich Dahte einen Dummschwätzer nennen.

Und jetzt zu etwas fast ganz Anderem. „Trojaner spioniert Kreditkarten und Bankdaten aus“ – „Datendiebstahl: Bundesbehörden warnen vor Banking-Trojaner“ – „Internet: BKA warnt vor Trojanern beim Online-Banking“. Undsoweiter. Die Süddeutsche im Original: „Die schädliche Software nistet sich meist beim Besuch einer infizierten Webseite auf dem Computer ein.“

Soso. Sie nistet sich. Man kann es auch ganz anders formulieren, dann wäre es gut, schön und wahr, käme aber ganz ohne die kulturpessimistische Attitude aus, dass das Pöhse überall im Internet lauere und dass man rein gar nichts machen könne ausser zu beten: „Die Nutzer eines bestimmen Betriebssystems, die keinen Gedanken an ihre Sicherheit verschwenden und ihren Browser so einstellen, wie es Bill Gates er gern hätte, und anderen Leuten erlauben, aktive Inhalte ungefragt auf ihren Rechner zu schaufeln, die laufen Gefahr, dass ihnen was passiert.“ Wenn man die Wahrheit schriebe und nicht dummes Zeug wie der Regenzauber „auf jedem Computer sollten außerdem ein aktuelles Virenschutzprogramm und eine Firewall installiert sein“, dann würden sich die Leute natürlich fragen: Muss ich jeden Tag in der Zeitung lesen, dass ich, wenn ich über die Straße gehe, vorher gucken muss, ob ein Auto kommt? Pfeifen, unkritische, wie man das in Bayern grammatikalisch zu sagen pflegt. Ich reg mich wieder auf.

Und jetzt zu etwas noch ganz Anderem. „Hackerangriff Wiederherstellung der KZ-Gedenkstätten-Websites läuft“. – „KZ-Gedenkstätte Rechtsextreme hacken Buchenwald-Website“. – „Neonazis: Internetseite der Gedenkstätte Buchenwald zerstört“. – „Websites von KZ-Gedenkstätten teilweise gelöscht“. – „Entsetzen über neue Dimension rechtsextremer

Aktivitäten“. – „Neonazis manipulieren Buchenwald-Internetseite“.

Ich tu euch nicht den Gefallen. Nein, ich glaube nicht, was in den Medien geschwätzt wird. Ich bin ein kritischer und mündiger Bürger und mache mir selbst ein Bild.

Ich lese die Leserkommentare bei Heise zum Thema. „1. Wie können die was von einer Internetseite löschen? Hat da jemand schlampige CGI/PHP Skripte geschieben? 2. Haben die keine Backups?“ – „Das hier sagt ja wohl alles über die Kompetenz der Ersteller aus: , Diese Website ist optimiert für Internet Explorer und Netscape Navigator ab Version 4. Die Vollversion benötigt das Flash-Plugin.‘ Über so einen Spruch bin ich lange nicht mehr gestolpert.“ (Gut, die Antwort: „Das ist ja auch eine Gedenkstätte“ ist ein bisschen zu zynisch.) „Was passiert ist, die Webmaster der Gedenk-Intenetseite haben beim Thema „IT-Sicherheit“ nicht aufgepasst, und ein paar rechtsradikal veranlagte „möchtegern-Hacker“ haben sie ge-defaced. Dadurch wurde keinerlei Erinnerung ausgelöscht (ausser vielleicht der Log Datei des Servers, wenn die Cracker nicht ganz komplett doof waren) (…) Aber dann solche Pressestatements, und es wird offenbar das die Betreiber des Museums nicht nur von IT-security, sondern vom Web schlechthin keine Ahnung haben. Also hört auf mit dem geheule, sucht lieber nach der Sicherheitslücke, stopft sie, dann setzt den Server neu auf und spielt das letzte Backup wieder ein.“ – „Netcraft Apache/1.3.28 Unix PHP/4.3.4 lief offenbar bis gestern dort. Man betreibt dort offenbar einen eigenen Server und hält sich am Motto ‚Never touch a running System‘. Man hätte jemand fragen sollen der sich mit so etwas auskennt. Oder gleich Webhosting bei einem seriösen Provider buchen (…) Das es kein Backup gibt ist ebenfalls nicht zu entschuld(ig)en. Mögen euch die Hacker treffen.“

Erstaunlich bescheuert berichtet Gulli.com: „Zugang zu den Servern konnten sich die Täter mittels eines Viruses verschaffen der vermutlich schon vor der Attacke eingeschleust

wurde.“ Ein Virus?! „Hacker“ schleusen gezielt (!) einen „Virus“ ein?! Und wie machen die das? Dann sollten das Bundesamt für Sicherheit in der Informationstechnik und das Bundeskriminalamt bei den angeblichen neonazistischen Hackern in die Lehre gehen, wie man „Viren“ unbemerkt und irgendwie einschleust, um anschließend einen Fernwartungs-Zugriff zu haben.

Ich habe keine zwei unabhängigen Quellen für die These, dass irgendwelche kackbraunen Kameraden die Website der Gedenkstätte Buchenwald zerstört hätten. Ich kann mir auch ganz etwas anderes vorstellen. Aber das sage ich besser nicht, ich reg mich schon genug auf.

Meidet die dunklen Ecken des Internet (burks.de)!

Immer wenn man glaubt, dümmer ginge es nimmer, kommt der Bund deutscher Kriminalbeamter daher und legt noch einen drauf. Bei Heise las ich: „Wer zukünftig im Internet einkauft, Geld überweist, Behördengänge erledigt oder andere Geschäft

abwickelt, soll sich nach dem Willen des Bundes Deutscher Kriminalbeamter zuvor bei einer staatlichen Stelle registrieren lassen, sagte der BDK-Vorsitzende Klaus Jansen in einem Interview der Neuen Osnabrücker Zeitung. (…) Zudem solle die Polizei das Recht bekommen, ‚Trojaner, Viren und Schadprogramme von privaten Rechnern entfernen zu dürfen'."

Das Märchen von der real gar nicht existierenden Online-Durchsuchung also. Anscheinend hat dieser Kerl gar nicht gemerkt, dass das Bundesverfassungsgericht den Wunschtraum des behördlichen Zugriffs in Echtzeit auf alle „Internet-Festplatten" schon längst verboten hat, obwohl das Anliegen ohnehin technisch nicht umsetzbar ist. Nach dem Motto „steter Tropfen höhlt den Stein" wird der Unfug einfach immer und immer wieder wiederholt. Politischer Flankenschutz kommt von Leuten wie Uhl (um mal jemand anderen als den unvermeidlichen Bosbach zu nennen), der die chinesische Zensur gern in Deutschland einführen möchte: „Was die Chinesen können, sollten wir auch können. Da bin ich gern obrigkeitsstaatlich".

Die Agitprop der obrigkeitsstaatlichen Internet-Ausdrucker steht ähnlich auch bei RP Online (Rheinische Post). Zeit Online wie auch andere verzichten auf jedwedes kritisches Wort – deutscher „Qualitätsjournalismus" eben.

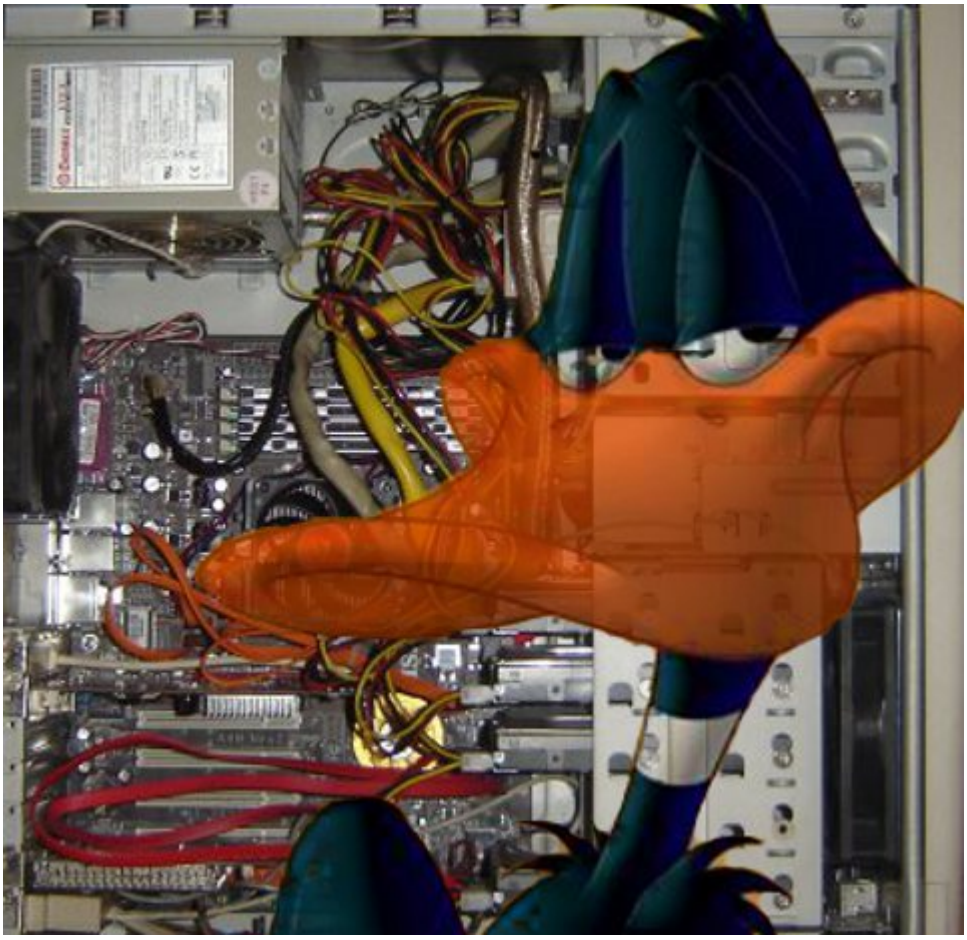
Die Neue Osnabrücker Zeitung titelt: „Kriminalbeamte wollen in sozialen Netzwerken verdeckt ermitteln." Das ist natürlich eine tolle Idee: Wenn jeder, der sich in Partnerbörsen, bei Facebook, StudiVZ oder sonstwo im so genannten Web 2.0 herumtreibt, damit rechnen muss, dass der Gesprächspartner ein verdeckter Ermittler ist, würden vielleicht einige DAUs mit ihren Daten vorsichtiger umgehen.

Im Heise-forum steht schon ein Entwurf der „Internet-Verkehrsordnung", der mir gefallen hat:
§1: Ins Internet darf nur, wer einen Internetführerschein hat.
§2: Für P2P-Protokolle gelten Geschwindigkeitsbegrenzungen.
§3: Staatlichen Paketen, bei denen das Blaue-Blinklicht-Flag

im Header gesetzt ist, ist Vorrang zu gewähren. Zuwiderhandlungen werden mit Internetführerscheinentzug von sechs Monaten bestraft; sollten die Pakete den Bundestrojaner enthalten, kann die Strafe auf ein Jahr erhöht werden.
§4: Teile des Webs dürfen durch Aufstellen entsprechender Verkehrszeichen gesperrt werden.

„Weniger als ein Prozent der 260000 Polizisten in Deutschland" seien „fit fürs Netz". Das merkt man. Jansen ist ein schlagendes Beispiel dafür.

Die sich selbst verstärkende faktenfreie Ente, lau aufgewärmt



„700.000 Euro für eine Ente“ schrieb ich am 25.05.2010 in diesem kleinen onlinedurchsuchungshoaxfeindlichen Blog. Gestern wärmten der Heise-Newsticker („CDU/CSU und SPD halten an heimlichen Online-Durchsuchungen fest“) und die taz („BKA hält sich zurück“) [*was für ein dämlicher Titel!*] die wohl bekannte Ente wieder auf.

Die beiden Artikel enthalten keine Informationen – sie geben nur das sinnfreie Gefasel einiger Politiker zum Thema der real gar nicht existierenden „Online-Durchsuchung“ wieder. „Gerade beim internationalen Terrorismus beobachten wir zunehmend, dass sich Personen modernster Technologien bedienen, um nicht entdeckt zu werden.“ Modernste Technologien – was könnte damit gemeint sein? Terroristen nutzen das Internet? Der Satz wäre ja sinnvoll, weil für unsere Sprechblasen-Absonderer das Internet ultramodern ist (weil ihnen erst gestern ein persönlicher Referent davon erzählt hat).

„Die Rechtsextremen haben die moderne Technik entdeckt“,

raunte Focus 1993. Das ist der Stand der Diskussion: Man häufe ein paar Komparative um ein vermeintliches Bedrohungsszenario, drapiere es mit kulturpessimistischer Attitude („es wird alles immer schlimmer“) und deutschtypischer Hysterie („die Bösen werden immer öfter immer böser“) und tröpfele noch ein wenig Eigenwerbung drauf („der Verfassungsschutz mahn, warnt und ist besorgt“).

Aber ich schweife ab. Mich regen die „Kritiker“ genau so auf: „Der verdeckte Zugriff auf Festplatten sei ‚überflüssig‘ und richte ‚bürgerrechtlichen Flurschaden‘ an, da er nicht einmal an einen festen Tatverdacht geknüpft sei.“ Bevor ich auch nur ein Wort weiterlese, möchte ich wissen: Wie soll der so genannte „verdeckte“ Zugriff auf „Festplatten“ bewerkstelligt werden? Warum, verdammt noch mal, taucht diese doch nicht ganz unwesentliche Frage weder bei Stefan Krempl noch bei dem einschlägig bekannten Dampfplauderer und Nebelkerzenwerfer Christian Rath von der taz auf? Weil die Zahnpasta schon aus der Tube ist und nicht wieder hinein könnte, selbst wenn sie wollte? Wozu habe ich eigentlich das Buch geschrieben? Liest der Rath seine eigene Zeitung nicht?

Krempl und Rath, hier diese Rezension weiterlesen: „Als nächstes zeigen die Autoren, dass es sich bei der Online-Durchsuchung um ein sich selbst verstärkendes Phänomen handelt, das aus unklaren Definitionen darüber herrührte, was mit der Online-Durchsuchung eigentlich gemeint sein soll. Gepaart mit dem Mythos des allmächtigen Hackers schaukelte sich die Darstellung der Online-Durchsuchung in den Medien zu immer größeren Horrorszenarien auf, die man letztlich als nahezu faktenfrei bezeichnen kann. Die einzig gesicherten Fakten waren nur die Berichte in den Medien, nicht deren Inhalt. Aus der vielleicht noch anfangs verwendeten konjunktiven Form ‚könnte‘ wurden dann konkrete Forderungen von Politikern. Journalisten stellten suggestive Fragen, ob es denn solche Fälle nicht schon längst gegeben habe, und weil man nicht genau wusste, was mit ‚Online-Durchsuchung‘ gemeint

ist (oder was man selbst darunter versteht) und man es mit anderen Verfahren vermischte/verwechselte, ergab sich das Bild, dass schon seit langem dieses Verfahren ohne Rechtsgrundlage abgelaufen ist. Dies Alles, gepaart mit dem fehlenden Sachverstand, führte zu dem schon genannten ‚Medien-Hype'. Beim Lesen dieses Teils des Buches kommt man aus dem Staunen über diese Vorgänge nicht heraus. Steht es so schlecht um den Journalismus in Deutschland?"

Ich zitiere mich selbst: „In Wahrheit hat es eine „Online-Durchsuchung" oder gar den „Bundestrojaner", der seit geraumer Zeit durch die Medien geistert und sogar einen eigenen Eintrag bei Wikipedia bekommen hat, nie gegeben – und es wird ihn auch nie geben. Er ist ein Hoax und beruht auf dem mangelnden Sachverstand eines Oberstaatsanwaltes, jeweils einer Falschmeldung der taz und der Süddeutschen und der Tatsache, dass alle deutschen Medien, ohne die Fakten zu recherchieren, voneinander abgeschrieben haben. Nach dem Prinzip ‚Stille Post' steht am Ende der Berichterstattung dann der ‚behördliche' Hacker, vom dem am Anfang nie die Rede war."

Ceterum censeo: Der Kaiser ist nackt! Es gibt keine ‚Bundestrojaner'!

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!

Die Ente nach Schweizer Rezept

Wie sich die Textbausteine der DAUs doch gleichen. „Staat will Zugriff auf Schweizer Festplatten“, formuliert die Basler Zeitung unkritisch und ahnunglos. Natürlich kommt im gesamten Artikel kein Wort darüber vor, ob das überhaupt machbar sei, was das Bundesamt für Justiz dort will. Danach fragt niemand mehr. Es ist wie bei Schopenhauer – die digitale Alpenwelt als Wille und Vorstellung.

„Der Staat will künftig auf die Festplatten verdächtiger Personen zugreifen können. Mithilfe von Trojanern sollen Strafverfolgungsbehörden sich auf den Harddisks umsehen dürfen.“ Mit „Trojanern„? Halt. Bitte jetzt zunächst das Gehirn einschalten. So dämlich ist ja noch nicht einmal Ziercke. („Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht.“) Der möchte mittlerweile schon gern vorher in die Wohnung des Verdächtigen einbrechen lassen, um zu versuchen, ob man physisch auf den Rechner zugreifen kann.

Wie will man erstens die IP-Adresse der Zielperson

herausfinden? Wie will man zweitens einen „Trojaner“ genau auf deren Rechner schleusen, wenn die auch nur einmal die Ratschläge des Bundesamtes für Sicherheit in der Informationstechik beherzigt hat? Das geht nicht.

„Im Falle eines Verdachts sollen dank den Überwachungsprogrammen alle Mails, Fotos und Filme für die Untersuchungsbehörden zugänglich sein.“ Was soll dieser Unfug: Was ist, wenn die Person ihre E-Mail verschlüsselt? Das „Abhören“ digitaler Postkarten ist ja ohnehin leicht möglich. Was also noch? Wie will man von außen einen Keylogger installieren? Und wie will man unbemerkt und beweissicher abgefangene Informationen verschicken?

Basler Zeitung, es interessiert mich nicht die Bohne, was jemand „will“ und was sein „soll“, sondern nur, *wie* das geschehen könnte. Das wisst ihr nicht? Ihr habt noch nicht einmal diese doch nicht unwesentliche Frage gestellt? Dann solltet ihr euer journalistisches Selbstverständnis mal updaten.

„Das Bundesamt für Justiz rechtfertigt diesen Schritt damit, dass im Internet vermehrt über Verschlüsselung kommuniziert werde. Gerade Straffällige würden sich dies zunutze machen. Trojaner, die, einmal installiert, jede Tastatureingabe mitverfolgen können und die Informationen an den Urheber des Überwachungsprogramms schicken, sollen diese Lücke schliessen.“ Also doch Keylogger. Noch mal zum Mitschreiben: Wie wollt ihr den auf die (!) Rechner der Zielperson bekommen? Und gerade „Straffällige“ verschlüsseln? Beweise dafür?

„Oder des Vertriebs von verbotener Pornografie.“ Nun, das ist kein deutscher Satz. Wir versuchen ihn dennoch zu verstehen. Diese suggestive Wortwohl suggeriert uns, dass das Böse (auf dem die menschliche Fortpflanzung beruhgt) in bildlicher Form auf den berüchtigen „Internet-Festplatten“ lauert. Darf ich mich mal kurz selbst zitieren (06.02.2007)? Danke.

„In Wahrheit hat es eine „Online-Durchsuchung“ oder gar den „Bundestrojaner“, der seit geraumer Zeit durch die Medien geistert und sogar einen eigenen Eintrag bei Wikipedia bekommen hat, nie gegeben – und es wird ihn auch nie geben. Er ist ein Hoax und beruht auf dem mangelnden Sachverstand eines Oberstaatsanwaltes, jeweils einer Falschmeldung der taz und der Süddeutschen und der Tatsache, dass alle deutschen Medien, ohne die Fakten zu recherchieren, voneinander abgeschrieben haben. Nach dem Prinzip „Stille Post“ steht am Ende der Berichterstattung dann der „behördliche“ Hacker, vom dem am Anfang nie die Rede war.“

Was mich am meisten aufregt, sind die merkbefreiten „Kritiker“. Sie kritisieren die Verschwörungstheoretiker des Bundesamtes für Justiz nur, anstatt laut zu rufen: „Der Kaiser ist nackt! Es gibt keine ‚Bundestrojaner'“!

700.000 Euro für eine Ente

Die wohlwollenden Leserinnen und Leser ahnen bestimmt schon, was heute unser Thema sein wird. Der Tagessspiegel meldet: „Als wichtiges Instrument im Kampf gegen den internationalen Terrorismus wurde sie gepriesen, doch bisher hat das Bundeskriminalamt (BKA) keine einzige Online-Durchsuchung durchgeführt.“ Heise dazu: „BKA nahm bislang keine Online-Durchsuchung vor“.

Schon klar. Wie ich schon in meinem Buch behauptete: Es hat noch keine gegeben (und wird es auch nicht geben). Wie sollte das auch funktionieren….

„Demnach investierte das BKA bislang knapp 700.000 Euro in Online-Durchsuchungen. Davon entfallen rund 581.000 Euro auf Personalkosten“. Und auf was entfiel die restlichen 119.000

Euro? Auf den Kauf von neuen Computern vermutlich. Die Ente kann man wahrhaftig in reinem Gold aufwiegen.

Nur zur Erinnerung:
– Sueddeutsche.de (07.12.2006): „‚Es gab bereits Einzelfälle in Strafverfahren, bei denen richterlich angeordnet solche Durchsuchungen stattgefunden haben‘, sagt Dietmar Müller, Pressesprecher des BKA in Wiesbaden. Das Verfahren sei relativ neu und erfolge ausschließlich in Abstimmung mit der Staatsanwaltschaft und mit richterlichem Beschluss. Aus ‚ermittlungstechnischen Gründen‘ könne Müller nicht sagen, wie die digitale Spionage technisch funktioniert.“
– Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Petra Pau, Kersten Naumann und der Fraktion Die Linke (22.12.2006, Drucksache 16/3787):
„Seit wann wenden deutsche Sicherheitsbehörden das Instrumentarium des ‚heimlichen Abziehens von Daten auf fremden Computern mittels spezieller Software‘ (Online-Durchsuchung) an?“ – „Der Bundesregierung liegen keine Erkenntnisse über in Ermittlungsverfahren durchgeführte Online-Durchsuchungen vor.“
– Heise Newsticker (25.04.2007): Bundesregierung gibt zu: Online-Durchsuchungen laufen schon.
„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.“
– Tagesschau.de (27.04.2007): „Seit 2005 haben deutsche Geheimdienste nach Angaben des Bundesinnenministeriums knapp ein Dutzend Privatcomputer heimlich via Internet durchsucht.“
– Tagesschau.de (28.04.2007, Wolfgang Wieland im Interview): „Wir gehen auch davon aus, dass das noch nie richtig geklappt hat. Es gab technische Schwierigkeiten. Das Einschleusen hat nicht geklappt…“

– Spiegel Online (09.07.2007, Wolfgang Schäuble im Interview): SPIEGEL: „…wie etwa die heimlichen Online-Durchsuchungen zeigen. Die haben die Sicherheitsbehörden ohne gesetzliche Grundlage jahrelang angewandt. Schäuble: Moment. Es gab einen Anwendungsfall im Inland.“
– Focus Online (05.01.2008): „Reda Seyam klickte laut FOCUS die getarnte E-mail der Verfassungsschützer an und aktivierte so die erste und bislang einzige Online-Durchsuchung in Deutschland.“
– Bundesverfassungsgericht (27.02.2008): „Vereinzelt wurden derartige Maßnahmen durch Bundesbehörden bereits ohne besondere gesetzliche Ermächtigung durchgeführt. Über die Art der praktischen Durchführung der bisherigen ‚Online-Durchsuchungen‘ und deren Erfolge ist wenig bekannt. Die von dem Senat im Rahmen der mündlichen Verhandlung angehörten Präsidenten des Bundeskriminalamts und des Bundesamts für Verfassungsschutz haben mangels einer entsprechenden Aussagegenehmigung keine Ausführungen dazu gemacht.“
– Spiegel Online (01.03.2008): „Die beiden bekannten Fälle von Online-Durchsuchungen wurden gegen den Berliner Islamisten Reda S., der gute internationale Kontakte in die Dschiahd-Szene [sic] unterhält, und einen Iraner geführt, der der Proliferation verdächtigt wurde.“

Noch Fragen zum einflussreichsten Medien-Hoax des Jahrzehnts?

Der Kaiser ist auch in Rheinland-Pfalz nackt

Das Innenministerium in Rheinland-Pfalz ist nicht für besonders ausgeprägte Internet-Affinität bekannt. Deshalb darf man denen auch nicht übelnehmen, dass sie die wohl bekannte Ente aka Hoax „Online-Durchsuchung“ über ihre Website watscheln lassen. Man möchte übrigens auch „verschlüsselte Internet-Telefonie“ überwachen. Wie, das weiß kein Mensch. Aber so ist das eben bei Enten: Die Welt als Wille und Vorstellung. Wehe, es erinnert jemand an die Realität.

„‚Für eine erfolgreiche Gefahrenabwehr ist es unerlässlich, dass die Methoden der Sicherheitsbehörden mit den technischen Möglichkeiten der Terroristen und Kriminellen Schritt halten‘, erklärte Bruch. Allerdings betont Bruch auch, dass das Recht der Bürger auf Privatsphäre auf jeden Fall geschützt werde. Die gesetzlichen Voraussetzungen für die Online-Durchsuchung berücksichtigten selbstverständlich die Rechtsprechung des Bundesverfassungsgerichts. ‚Wegen ihrer besonderen Schwere unterliegen solche Eingriffe daher engen Grenzen und sind auf

die Abwehr erheblicher Gefahren und schwerster Straftaten beschränkt.‘, unterstrich der Minister weiter. Denn nicht nur die gesetzlichen Voraussetzungen seien hoch angesetzt, auch die für eine solche Maßnahme zu treffenden Vorbereitungen seien außerordentlich zeitintensiv und komplex, so dass die Online-Durchsuchung voraussichtlich nur höchst selten zur Anwendung kommen werde.“

Das ist natürlich Kokolores und kompletter Blödsinn. Wie dem Stammpublikum bekannt und wie auch in meinem Buch zum Thema hinreichend erörtert, hat es noch nie eine Online-Durchsuchung gegeben, wie sie der Volksmund versteht, und noch niemand hat sich erkühnt, eine Erfolg versprechende Methode vorzuschlagen, den Rechner eines Vedächtigen zielgenau ohne dessen Wissen zu durchsuchen. Das geht gar nicht. (Meine Artikel in Telepolis zum Thema hat Wikipedia weggelassen – was die Ente stört, lässt man weg. By the way: Der Kaiser ist nackt!)

Hier kann man es zum Beispiel nachlesen: „Eine Online-Durchsuchung wurde – soweit sie dem Projektteam bekannt wurde – lediglich in drei Fällen angedacht und in zwei Verfahren beantragt, aber abgelehnt. In zwei weiteren Fällen wurde die Maßnahme genehmigt, aber nicht durchgeführt.“ Quod erat demonstrandum. Alles andere ist Verschwörungstheorie, und dafür sind die Medien und der Chaos Computer Club zuständig.

Sogar die taz rezensierte – weil es so nett geschrieben ist, hier eine Langfassung:

„Die sogenannte Onlinedurchsuchung ist nicht viel mehr als ein aufgeblasener Medienhype und ein zahnloser Papiertiger obendrein. Mit diesem Instrument lässt sich zwar jede Menge rechtspolitischer Flurschaden an-, aber wenig Effektives gegen den internationalen Terrorismus ausrichten. Dabei liegt der Skandal für die beiden Autoren weniger in der zweifelhaften Technik, als in den Fehlinformationen, die darüber verbreitet werden.

Denn, so die überraschende Ausgangsthese des Buchs: So etwas wie eine ‚Onlinedurchsuchung' gibt es überhaupt nicht, jedenfalls nicht als funktionierendes Instrument in Händen der Ermittlungsbehörden. Die Vorstellung, Polizei und Geheimdienste könnten sich heimlich in jeden PC hacken, und zwar ohne dafür die Wohnung des Betroffenen betreten zu müssen, kann demnach getrost ins Reich der Märchen verwiesen werden – zu hoch sind die technischen Hürden, die dafür überwunden werden müssten. Selbst Laien könnten sich mit einfachsten Mitteln erfolgreich gegen Spitzelprogramme dieser Art wehren; einmal abgesehen davon, dass bislang noch keine Behörde überzeugend dargestellt habe, wie ein solcher staatlich sanktionierter Hackerangriff in der Praxis überhaupt aussehen könnte.

Was den Glauben an den „Bundestrojaner" am Leben erhalte, sei nichts anderes als Ignoranz in Sachen Computertechnik und der Mythos von der Allmacht des ‚Hackers'. Die etablierten Medien hätten allesamt in der Berichterstattung über die Onlinedurchsuchung regelmäßig versagt, so die Kritik der Autoren. Praktisch durchgehend sei nach dem System ‚Stille Post' verfahren worden: Einer schreibt vom anderen ab, und am Ende bestätigen sich Halb- oder Unwahrheiten von selbst. (…) Schröder weist überzeugend nach, dass es entgegen anderslautenden Berichten bis jetzt keinen einzigen erfolgreichen Einsatz eines ‚Bundestrojaners' gegeben hat."

Und was machen die Medien im aktuellen Fall daraus? Kein kritisches Wort, weder bei Heise noch beim SWR. Es wird einfach so getan, als sei so etwas möglich. Recherche? Fehlanzeige.

So perpetuuiert sich die Ente. Oder, wie Albert Einstein 1922 richtig sagte: „Jeder Blödsinn kann dadurch zu Bedeutung gelangen, dass er von Millionen Menschen geglaubt wird."

Screenshot: SWR zum Thema – man kann muss die Sicherheitseinstellungen des Browsers herunterfahren, um einen

Beitrag rezipieren zu können – so werden Surfer zur Dummheit erzogen.

Die Daten der anderen

Bild.de ist heute Sprachrohr und Lobbyist Zierckes: „Datenschutz hilft Kinderschändern“. Natürlich. Und wir sind alle pädophil, wenn wir keine Webcam im Schlafzimmer installiert haben.

„In einem aktuellen Missbrauchsfall konnte ein Kinderschänder laut BKA nur mithilfe ausländischer Dienstellen ermittelt werden.“ Ach ja? Welches andere Land speichert denn auf Vorrat? Und wie ist der Datenaustauch gesetzlich geregelt? Quellen? Fakten? Nicht in deutschen Medien.

Noch einmal Ziercke am 15.11.2007: „Sie können sich die abstrakten Möglichkeiten vorstellen, mit dem man über einen Trojaner, über eine Mail oder über eine Internetseite jemanden aufsucht. Wenn man ihnen erzählt hat, was für eine tolle Website das ist oder eine Seite mit ihren Familienangehörigen, die bei einem Unfall verletzt worden sind, sodass sie dann tatsächlich die Seite anklicken.“

Mir fehlen bei einem solchen Blödsinn einfach die Worte. Mir fehlen auch die Worte, warum ein deutsches Medium einen derartigen Idioten überhaupt unkritisch zu Wort kommen lässt. Oder warum Journalisten nicht in schallendes Gelächter ausbrechen, wenn er den Mund aufmacht. Muss am verinnerlichten Obrigkeitsstaat liegen.

BKA-Lobbyismus: Sperren statt löschen

Leseempfehlung: Netzpolitik.org und RA Stadler über das BKA und dessen Lobbyismus für Zensurgesetze.

Netzpolitik.org: „Während die FDP-Fraktion für den 17.03. zu einer öffentlichen Anhörung "Lösungen und Wege im Kampf gegen die Kinderpornographie" einlädt, plant die CDU-/CSU-Fraktion parallel eine "fraktionsoffene" Informationsveranstaltung zum gleichen Thema. Eingeladen sind u.a. BKA-Chef Ziercke und ‚Innocence in Danger‚."

Jeder lädt nur die ein, deren Meinung die eigene schon bestätigt. Es geht den Zensurbefürwortern nicht um eine rationale Diskussion, sondern um moraltheologisch geprägte Propaganda, der sich, was zu erwarten war, auch die Internet-Ausdruckerin Alice Schwarzer angeschlossen hat.

Mein Rat: Alle Veranstaltungen und Talkshows weiträumig umfahren, bei denen die exakte Zeichenkette „Kinderpornographie" irgendwo auftaucht. Dort heißt es nur „Kopf ab zum Gebet".

By the way: Der Kaiser ist nackt! Im World Wide Web gibt es keine Kinderpornografie, deren (technisch) Verantwortlicher anonym bleiben könnte.