

die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club



foto: Dorit Günter, Nadja Hannaske

ISSN 0930-1054 • Kalte Jahreszeit 2001
€ 2,50 bitteschön
Postvertriebsstück C11301F

#76 

Erfa-Kreise

Hamburg: Lokstedter Weg 72, D-20251 Hamburg, <mail@hamburg.ccc.de> <http://hamburg.ccc.de> Phone: +49 (40) 401 801.0 Fax: +49 (40)401.801.41 Voicemailbox +49 (40) 401801.31. Treffen jeden Dienstag ab ca. 20.00 Uhr in den Clubräumen. Der jeweils erste Dienstag im Monat ist Chaos-Orga-Plenum (intern), an allen anderen Diensten ist jede(r) Interessierte herzlich willkommen. Öffentliche Workshops im Chaos Bildungswerk fast jeden Donnerstag. Termine aktuell unter <http://hamburg.ccc.de/bildungswerk/>.

Berlin: Club Discordia jeden Donnerstag zwischen 17 und 23 Uhr in den Clubräumen in der Marienstr. 11, Vorderhaus in Berlin-Mitte. Nähe U-/S-Friedrichstraße. Tel. (030) 285986-00, Fax. (030) 285986-56. Briefpost CCC Berlin, Postfach 640236, D-10048 Berlin. Aktuelle Termine unter <http://www.ccc.de/berlin>

Köln: Chaos Computer Club Cologne (c4) e.V. Vogelsangerstraße 286 / 50825 Köln 50° 56' 45" N, 6°51'02" O (WGS84) / Tel. 0221-546 3953 / <http://koeln.ccc.de/> <oeffentliche-anfragen@koeln.ccc.de>. Treffen Dienstag 20:20.

Ulm: <http://www.ulm.ccc.de/> Kontakt: Frank Kargl <frank.kargl@ulm.ccc.de> Treffen: Montags ab 19.30h im 'Café Einstein' in der Universität Ulm. Vortrag chaos-seminar: Jeden ersten Montag im Monat im Hörsaal 20 an der Universität Ulm.

Bielefeld: Kontakt Sven Klose Phone: +49 (521) 1365797 Email: mail_bielefeld.ccc.de. Treffen Donnerstags, ab 19.30 Uhr in der Gaststätte 'Pinte', Rohrteichstr. 28, beim Landgericht in Bielefeld. Interessierte sind herzlich eingeladen.

Chaos-Treffs:

Aus Platzgründen können wir die Details aller Chaos-Treffs hier nicht abdrucken. Es gibt in den folgenden Städten Chaos-Treffs, mit Detailinformationen unter <http://www.ccc.de/ChaosTreffs.html>:

Bochum/Essen, Bremen, Burghausen /Obb. und Umgebung, Calw, Dithmarschen/Itzehoe, Dresden, Emden / Ostfriesland, Eisenach, Erlangen /Nürnberg/Fürth, Frankfurt a.M., Freiburg, Freudenstadt, Giessen/Marburg, Hanau, Hannover, Ingolstadt, Karlsruhe, Kassel, Lüneburg, Mannheim /Ludwigshafen/Heidelberg, Mönchengladbach, München, Münster/Rheine/ Coesfeld /Greeven/Osnabrück, Rosenheim /Bad Endorf, Neunkirchen/Saarland, Würzburg, Schweiz /Dreyeckland: Basel, Österreich: Wien

Die Datenschleuder Nr. 76

IV. Quartal, Winter 2001

Herausgeber:

(Abos, Adressen etc.)
Chaos Computer Club e.V.,
Lokstedter Weg 72, D-20251 Hamburg,
Tel. +49 (40) 401801-0, Fax +49 (40) 401801-41,
eMail: office@ccc.de

Redaktion:

(Artikel, Leserbrief etc.)
Redaktion Datenschleuder, Postfach 640236, D-10048
Berlin, Tel +49 (30) 280 974 70
Fax +49 (30) 285 986 56 / eMail: ds@ccc.de

Druck:

Pinguin-Druck, Berlin

Layout und ViSDP dieser Ausgabe:

Tom Lazar <tom>, tom@tomster.org

Redaktion dieser Ausgabe:

Tom Lazar, Andy Müller-Maguhn und Tina Lorenz

Autoren dieser Ausgabe:

Andy Müller-Maguhn, wicked, Henri C., Martin Springer, rude God, Tina Lorenz, Arne Ludorff, Stefan Krecher, Lisa Thalheim und Sebastian Lütger.

Eigentumsvorbehalt:

Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zurhabenahme ist keine persönliche Aushändigung im Sinne des Vorbehalts. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nichtaushändigung in Form eines rechtsmittel-fähigen Bescheides zurückzusenden.

Copyright

Copyright (C) bei den Autoren. Abdruck für nichtgewerbliche Zwecke bei Quellenangabe erlaubt.

Der Jihat und das Netz

oder auch: weltkriegsbedingte Verspätung, frohes neues Jahr..

Liebe LeserInnen und Leser,

mit der letzten Ausgabe der Datenschleuder Anfang August berichteten wir vom Tod von Wau Holland [0], vom bevorstehenden Camp der holländischen Hacker [1] und planten bereits eine Jubiläumsfeier unter dem Titel "XXCCC" zum 20 Jahrestag der Gründung des Chaos Computer Club [2], dem 12.09.2001.

Irgendwie hätte das Jahr 2001 sozusagen auch in geordneten Bahnen weiterlaufen können, hatten wir doch mit der Congresshalle am Alexanderplatz einen tollen Ort für Ausstellung und Feier organisiert. Auch für das danebenstehende und ebenfalls im Rahmen bevorstehender Sanierungsarbeiten leerstehende "Haus des Lehrers" war die Idee entstanden, die vordere Fensterfront (8 Etagen á 18 Fenstern) doch mit Baustrahlern und Relais in eine große Matrix zu verwandeln, um vom Alexanderplatz aus einmal Pong in groß spielen zu können. Am 11.09. war es dann so weit: vormittags hatten wir einen kleinen "Pressevorabtermin" organisiert um die Ausstellung zum Jubiläum der Presse vorzustellen, und am Vormittag hatten wir sozusagen auch noch ein einigermaßen journalistisches Interesse geweckt.

Andere hatten für den 11.09. allerdings andere Pläne, so daß der – nach Mitteleuropäischer Zeit – Nachmittag des 11.09. dann doch irgendwie die nicht schöneren, aber doch besseren Bilder lieferte, so daß unsere Ausstellungseröffnung und die Berichte über das mittlerweile blinkende Haus des Lehrers [3] den Bildern von der Eröffnungszeremonie des heiligen Krieges – oder wie man die einstürzenden Hochhäuser in New York auch immer einordnet – weichen musste. „XXCCC“ war dann eher eine familiäre Veranstaltung, die Menschen, die wir für Netzkultur begeistern wollten, blieben zu Hause vor dem Fernseher..

JIHAT.EXE

hat seit Aufruf nicht nur die Landschaft in New York verändert, die Immanentisierung des Eschatons, "was so viel heißt, wie den Weltuntergang heraufzubeschwören" [4] kommt in seinen Folgen für das Netz einer globalen Machtergreifung durch die Geheimdienste – vielleicht nicht gleich, aber doch nahe.

Der "Krieg gegen den Terror" oder auch: die amerikanische Idee, man könne Terrorismus mit Terrorismus bekämpfen, hält uns seitdem nicht nur mit amerikanischen, sondern ebenauch mit europäischen und deutschen "Anti- Terror" Maßnahmen und Gesetzespaketen in Atem, wobei man sich des Eindrucks nur schwer verschließen kann, die fehlende Definition des Begriffs "Terrorismus" bei der Erstellung bestimmter Gesetze sei weniger ein Versehen, als so eine Art Generalplacebo.

Je nach Netzanbindung kommen einem die Gesetzesentwürfe und Pakete seitdem in unterschiedlicher Geschwindigkeit entgegen. Dabei sind diejenigen, die mit einer hohen Bandbreite angebunden sind, nicht unbedingt besser dran, kommt Ihnen die Scheisse nur schneller entgegen. Weniger stinken tut sie deswegen nicht.

In den letzten Wochen hatten wir - neben dem Versuch, zu verstehen wer eigentlich genau diese Pipeline durch Afghanistan warum bauen will [5] - mit europäischen Terrorgesetzen, einem Innenminister im Ermächtigungswahn, der Cybercrimeconvention, einer europäischen Richtlinie zur Verordnung einer mehrmonatigen Speicherung aller Verbindungsdaten im Internet ("Data Retention"), der deutschen Implementierung der EU- Urheberrechtlichlinie und vielen anderen tollen Dingen zu tun, die uns es erst jetzt ermöglichen, euch eine Doppelausgabe der Datenschleuder für die Quartale 3 und 4 des Jahres 2001 zukommen zu lassen.

Wir hoffen, daß euch diese Ansammlung von Artikeln, Materialien und allerlei bunten Infoschnipseln für das lange warten entschädigt und würden uns freuen, auch im Jahre 2002 mit euch für Frieden auf Erden (auch in den Datenetzen) und eine gute Gesinnung für jederman und -frau tätig zu sein..

andy@ccc.de

[0] <http://www.wauland.de/>

[1] <http://www.hal2001.org/>

[2] <http://www.ccc.de/xxccc/>

[3] <http://www.blinkenlights.de/>

[4] Robert Anton Wilson, Illuminatus, Teil 1, erstes Kapitel

[5] http://www.house.gov/international_relations/105th/ap/wsap212982.htm



Aus der Kommission zur Beobachtung der Regierungen in Abwicklung:

Im zeitlichen Dunstfeld der terroristischen Anschlägen haben es bereits einige Gesetze bis zur Verabschiedung geschafft, die unter anderen Umständen wohl kontrovers diskutiert worden wären:

- die **Cybercrime-Convention**, verabschiedet am 23.11.2001 von den Staaten des Europarat (COE = Council of Europe). In einem größtenteils konspirativen Abstimmungsprozess wurde ein Gesetz zum angeblichen Schutz der Informationsgesellschaft vor sogenannter „Cyberkriminalität“ verabschiedet. Dabei wurden einerseits so sinnvolle Maßnahmen wie das Verbot von Computerviren beschlossen, auf der anderen Seite auch Verletzungen gegen Urheberrechtsbestimmungen und zivilrechtliche Rechtsabkommen mit aufgenommen. Eine Implementierung in D-land steht noch aus. Der vollständigen Text der Cybercrime-Convention findet sich unter

<http://conventions.coe.int/Treaty/EN/>

CadreListeTraites.htm

und eine kleine Materialsammlung des Chaos Hamburg unter

<http://www.hamburg.ccc.de/cybercrime/>

- die **Telekommunikations-Überwachungsverordnung (TKÜV)**, eine bis vor kurzem noch hochumstrittene Ansammlung von Maßnahmen. Dabei hat sich die Provider-Industrie leider darauf konzentriert, die Kostenfrage in den Mittelpunkt zu stellen. Nach dem 11.09. war dieses Argument nicht mehr öffentlichkeitsfähig.

Ohne einstürzende Türme und hysterisch einsetzenden Überwachungswahn hätte es der zuständige Referatsleiter beim Wirtschaftsministerium Herr Wagner vermutlich geschafft, ohne in Kraft getretene TKÜV in den wohlverdienten Ruhestand zu gehen. So gesehen herzlichen Glückwunsch, oder auch: Scheisse, liebe Provider und Wirtschaftsverbände.

Es hätte nicht geschadet wenn die Provider auch mal den immer mehr überwachbaren Internet-Nutzer in den Kernpunkt der Auseinandersetzung gestellt hätten. Jetzt ist der Zug abgefahren und das wird erstens teuer und zweitens nicht schön. Details unter

<http://www.bmw.de/Homepage/Politikfelder/Telekommunikation%20%26%20Post/Telekommunikationspolitik/TKUEV.jsp>

Aus der Berichterstattung über die Simulation einer demokratischen Regierung in der Bundesrepublik:

In Deutschland scheint sich nach vorschneller Assimilation von Gebiet und Bevölkerung der deutschen demokratischen Republik eine zweite Wende abzuzeichnen. Ausschlaggebend ist dabei der offenbar nicht hinreichend im Bezug auf geheimdienstliche Verstrickungen überprüfte derzeitige Innenminister Otto Schily.

Halten ihn die einen für einen Schläfer der CDU/CSU innerhalb der SPD, so werden ihm andererseits geschäftliche Verbindungen mit DDR-Embargohändlern und Regierungsstellen nachgesagt. Eine weitere Fraktion neigt dazu, ihn als langfristig plazierten Perspektivagenten der im Dunstkreis der NATO betriebenen klandestinen Organisationen anzusiedeln.

Mittlerweile redet man selbst in Kreisen der offenen Anstalt Berlin-Mitte angesichts der Schilyschen Konzepte nur noch ehrfürchtig vom ehemaligen „liberalen“ Innenminister Kanther.

Die gesammelten Ideen des Herrn Schily zur Bekämpfung des Terrorismus, auch bekannt als „Otto-Kataloge“ sind trotz mehrfacher Warnungen von Bürgerrechtsorganisationen beider deutscher Staaten wie dem Neuen Forum und der humanistischen Union nunmehr auch vom Bundesrat (20.12.) verabschiedet. Ob die Abgeordneten von Bundestag und Bundesrat sich überhaupt die Zeit genommen haben, die nur sehr zögerlich öffentlich gemachten Dokumente vorher zu lesen, konnte nicht ermittelt werden. Das Konzept des Gesetzes ist bereits aus der Spätzeit der DDR aus der Arbeit des „Ich-liebe-ich-doch-alle“ Ministers für Staatssicherheit Erich Mielke bekannt: Ermächtigungsklauseln, mit denen u.a. alle Telekommunikationsverbindungsdaten den Geheimdiensten BND, Verfassungsschutz und militärischem Abschirmdienst zugänglich gemacht werden sollen. Ausländer dürfen zur Identifizierung auch gleich noch eine Sprachprobe abgeben.

Die in öffentlichen Anhörungen geäußerten Hinweise auf mangelnde Verfassungsverträglichkeit wurden zugunsten von zusätzlichen Verschärfungen der vorgesehenen Regelungen nach Rücksprache mit CDU, CSU und Bundesländern ignoriert.

Weitere Informationen zum Stand der Dinge unter

<http://www.cilip.de/terror/>



Noch mehr Ärger mit den Illuminaten: die EU-Urheberrechtsrichtlinie kommt nach Deutschland

Als den bislang bedrohlichsten Schritt zur Einschränkung der Informationsfreiheit im Netz haben sich die Illuminaten offenbar die EU-Urheberrechtsrichtlinie ausgedacht.

Unter der Anmutenden Bezeichnung „Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft“ möchte die EU uns offenbar die US-amerikanischen Konzepte des Digital Millenium Copyright Act (DMCA) mit Euphemismen wie „Harmonisierung“ überstülpen.

Dabei produzieren diese Gesetzesvorstellungen alles andere als harmonische Zeiten: Waren bisher nicht nur Schutzrechte von Urhebern, sondern eben auch Zugangsrecht für Nutzer festgelegt, so basiert die Zukunft des Zugangs zu „urheberrechtlich geschützten Produkten“ im wesentlichen auf dem Verbot, technische Schutzmechanismen zu umgehen oder Hilfstatbestände zur Umgehung (wie Veröffentlichung) zu leisten. Die eigentliche Bestimmung über Zugangsrechte sollen dann den Herren Murdoch, Kirch und Berlusconi überlassen werden.

Begriffe wie öffentlicher Zugang und Bildungswesen finden sich bestenfalls in kompliziert verklausulierten Paragraphen, die einem wirklich den letzten glauben an den Sinn von gewählten Volksvertretern nehmen können. Wieweit der Spielraum bei der nationalen Umsetzung ausgenutzt wird, ist offen. Immerhin erkennt der zuständige Referatsleiter im Bundesministerium der Justiz an, daß der zugrundeliegende Glaube an durchsetzbare digital rights management systems (DRMS) auch so etwas wie der Versuch sein könnte, einen Pudding an die Wand zu nageln. Wer finanziert eigentlich die Zutaten?

Das Gesetz findet Ihr unter:

<ftp://ftp.ccc.de/pub/crd/copyright/EU-RL200129EG.PDF>



Ein merkwürdiger Absatz aus einem merkwürdigen Buch:

„According to secret and long-hidden documents obtained for Body of Secrets, the Joint Chiefs of Staff drew up and approved plans for what may be the most corrupt plan ever created by the U.S. government.

In the name of anti-communism, they proposed launching a secret and bloody war of terrorism against their own country in order to trick the American public into supporting an ill-conceived war they intended to launch against Cuba.

Codenamed Operation Northwood, the plan, which had the written approval of the Chairman and every member of the Joint Chiefs of Staff, called for innocent people to be shot on American streets; for boats carrying refugees fleeing Cuba to be sunk on the high seas; for a wave of violent terrorism to be launched in Washington, D.C., Miami, and elsewhere.

People would be framed for bombings they did not commit; planes would be hijacked. Using phony evidence, all of it would be blamed on Castro, thus giving Lemnitzer and his cabal the excuse, as well as the public and international backing, they needed to launch their war.“

Bamford, James: "Body of secrets: anatomy of the ultra-secret National Security Agency: from the Cold War through the dawn of a new century."

Doubleday, May 2001. ISBN 0-3854-9907-8. p. 82

Die Realitätsfrage

http://www.house.gov/international_relations/105th/ap/wsap212982.htm

1998 UNOCAL CORPORATION TESTIMONY ON HOUSE COMMITTEE ON INTERNATIONAL RELATIONS:

RE: OIL AND GAS RESOURCES IN THE CENTRAL ASIAN AND CASPIAN REGION TESTIMONY BY JOHN J. MARESCA VICE PRESIDENT, INTERNATIONAL RELATIONS UNOCAL CORPORATION TO HOUSE COMMITTEE ON INTERNATIONAL RELATIONS

SUBCOMMITTEE ON ASIA AND THE PACIFIC

FEBRUARY 12, 1998 - WASHINGTON, D. C.

[...] A second option is to build a pipeline south from Central Asia to the Indian Ocean.

One obvious potential route south would be across Iran. However, this option is foreclosed for American companies because of U.S. sanctions legislation. The only other possible route option is across Afghanistan, which has its own unique challenges.

The country has been involved in bitter warfare for almost two decades. The territory across which the pipeline would extend is controlled by the Taliban, an Islamic movement that is not recognized as a government by most other nations. From the outset, we have made it clear **that construction of our proposed pipeline cannot begin until a recognized government is in place that has the confidence of governments, lenders and our company.**

In spite of this, **a route through Afghanistan appears to be the best option** with the fewest technical obstacles. It is the shortest route to the sea and has relatively favorable terrain for a pipeline. The route through Afghanistan is the one that would bring Central Asian oil closest to Asian markets and thus would be the cheapest in terms of transporting the oil. Unocal envisions the creation of a Central Asian Oil Pipeline Consortium. The pipeline would become an integral part of a regional oil pipeline system that will utilize and gather oil from existing pipeline infrastructure in Turkmenistan, Uzbekistan, Kazakhstan and Russia.[...]

Nach den Einstürzen der beiden Hochhäuser des World-Trade-Center hat sich nicht nur bildlich die Medienlandschaft verändert. Der von der amerikanischen Regierung gestartete „Krieg gegen den Terrorismus“ – wie auch immer man Terrorismus mit Krieg bekämpfen kann – hat zumindest ein Großteil der amerikanischen Medien auf eine mehr oder minder einheitliche Regierungslinie gebracht. Dabei gehen die Auswirkungen weit über die Kriegsberichterstattung in Afghanistan hinaus.

Nicht erst die Kriegsmobilisierung durch den amerikanischen Präsidenten Bush hat eine Selektion der Berichterstattung zur Folge, bei denen im Kern die Aufrechterhaltung eines „moralischen“ Rückhalts der Bevölkerung steht. Insb. die jetzige Konfliktmischung zwischen einem konventionellen Krieg (Afghanistan), terroristischen Anschlägen (USA etc.) und einer diffusen weltweiten Terroristenhatz (nach den sogenannten Schläfern) verläuft die Front der Kriegspropaganda bereits weit in die deutsche Medienlandschaft hinein.

Das „globale“ im Sinne von: inter-nationale Internet hat zwar theoretisch auch Nachrichtenquellen aus der Region Afghanistans und Pakistans und aus dem Kulturkreis des Islam nur ein paar Tasten- oder Mausclicks näher gebracht, aber schon die relative

Bekanntheit von Medienerzeugnissen wie cnn.com oder spiegel.de lassen viele Internernutzer offenbar dort verharren, wenn es darum geht, sich aktuell zu informieren.

Im November hatte ich das fragwürdige Glück, mir vor Ort in Amerika ein „Bild“ von der der Situation der Medienberichterstattung zu machen.

Der Absturz der American Airline Maschine am 12.11. im New Yorker Stadtteil Queens war ja zunächst einmal kein direkt „erstaunlicher“ Vorgang; nach den Vorgängen im September und der nicht besonders deeskalierenden Reaktion der amerikanischen Regierung. Es schien es nur eine Frage der Zeit, bis die nächsten Anschläge in den USA kommen würden.

Die CNN Liveberichterstattung berichtete im Grunde genommen erstmal gar nichts, außer eben, daß eine Maschine der American Airlines abgestürzt sei und offenbar mehrere Wohnhäuser getroffen seien. Dann 30 Minuten Rauch, Feuerwehr und mehr oder minder hysterische Zeugen, die den Eindruck vermittelten, sie könnten psychologische Betreuung gerade besser gebrauchen als eine Fernsehkamera.

Als dann allerdings alternativ zu einer Erklärung von Polizei oder Luftfahrtsbehörde der amerikanische



Verteidigungsminister Herr Rumsfeld die erste Erklärung zur Unfallsache abgab, nämlich, daß es sich wohl um einen Unfall gehandelt habe, empfand ich diese Rollenverteilung schon ein bisschen erstaunlich. Und, daß das in Amerika offenbar schon als „normal“ hingenommen wird. Man stelle sich vergleichsweise vor, der deutsche Verteidigungsminister Herr Scharping würde vor dem Hintergrund des brennenden Reichstages vor der Tagesschaukamera erläutern, das offenbar technisches Versagen der Grund für den Flugzeugabsturz in das Gebäude sei.

In der Situation eines Krieges bekommen eben nicht nur Berichte über Erfolge und Mißerfolge in der Schlacht, Positionen eigener und gegnerischer Truppen „kriegswichtig“ Charakter. Auch die Interpretation von Flugzeugabstürzen, biologischen Waffenangriffen, merkwürdigen Unfällen und verschwundenen biologischen und atomaren Waffenexperten beeinflusst den moralischen Rückhalt, den eine kriegsführende Regierung von ihrer Bevölkerung bekommt und wird deswegen „kriegswichtig“. Wenn – um bei diesem Beispiel zu bleiben – also etwaige Terroristen durchaus die Möglichkeiten haben, weitere amerikanische Zivilmaschinen in Amerika z.B. mit einer panzerbrechenden Waffe auf dem Flughafengelände letztlich zum Absturz in eine Wohngegend zu bewegen, so könnte dies den Rückhalt der amerikanischen Bevölkerung gegenüber ihrer Regierung beim Krieg gegen die mutmaßlichen Terroristen in Afghanistan schwächen.

Das eigentlich neue an dieser ganzen Auseinandersetzung, insbesondere für die Amerikaner ist ja der „Homeland“-Attack, den man in den USA bislang so nicht erlebt hat. Bisher waren Kriege weit weg.

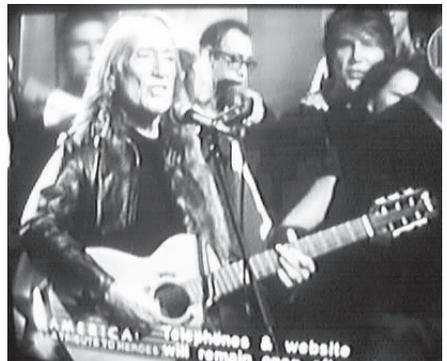
Realität?

Dabei entstehen derzeit höchst seltsame Gesamtrealitäten, in denen nicht einmal mehr versucht wird, die diversen – mitunter sich widersprechenden – virtuellen Realitäten unter einen Hut zu kriegen, also zum Beispiel die „offizielle“ US (CNN/USG) Realität, die Realität der Taliban, der Al Quiada, der afghanischen Zivilbevölkerung und so weiter.. Trotzdem ist genau diese „Realität“ - bestehend aus einer möglichst hohen Anzahl von Quellenlagen derzeit ein Stückweit wohl der anzustrebende Idealzustand. Eine kleine Zusammenstellung von regionalen Quellen findet sich hier zu unter <http://www.contramotion.com/sources/countries>

Die nicht nur im Bezug auf den Krieg gegen die afghanische Bevölkerung, sondern auch auf die Randkonflikte (Indien/Pakistan). Angereichert um die einschlägigen US- und sonstigen Militärnachrichtendienste und strategischen Analysedienste gibt es das ganze auch noch als Quellsammlung zum Vorgang unter <http://www.contramotion.com/sources/events/usawar/> Einen interessanten Hinweis zur derzeitigen Realitätskonstruktion entnahm ich in diesem Zusammenhang einer kleinen amerikanischen Mailingliste von kritischen Geistern, die es merkwürdig fanden, daß immer wenn gerade eine besonders unappetitive Situation im Krieg in Afghanistan eintrat (hunderte bis tausende von Toten Zivilisten) die US-Regierung irgendeine Meldung zu „Cyberterrorismus“ mit einer großen Warnung herausbrachte. So kann man die Öffentliche Aufmerksamkeit natürlich auch ablenken.

Als wir Ende Oktober die Chaosradio Sendung 66 zum Thema Gegenöffentlichkeit in Krisenzeiten, wollten wir während der Sendung eigentlich noch einmal über das Konzept des Filmes „Wag the Dog“ sprechen. Szenario: der Beraterstab des amerikanischen Präsidenten zettelt angesichts einer drohenden Klage gegen den Präsidenten wegen sexueller Belästigung einen Krieg an. Noch während der Sendung erledigte sich das: CNN zeigte Bilder eines Benefizkonzert für die Opfer der Anschläge in New York mit *genau* dem Sänger, der schon im Film „Wag the Dog“ einen emotionalisierenden Beitrag zur Einstimmung der Bevölkerung bringt. Wag the Dog ist Wirklichkeit.

Andy Müller-Maguhn, andy@ccc.de

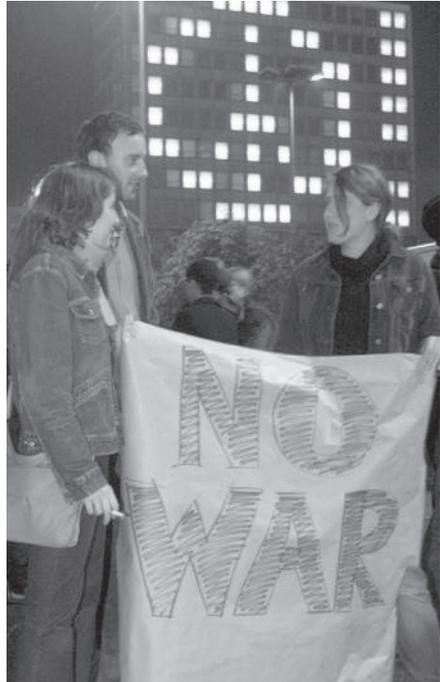


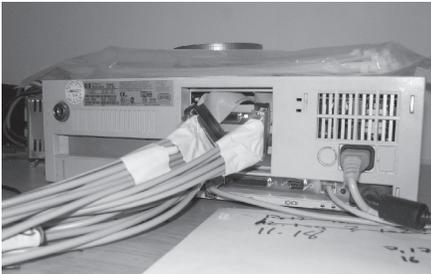
Head-Up-Display



„You can create art & beauty with a computer“
Steven Levy

Zum 20 jährigen Jubiläum des Chaos Computer Clubs wurde auf dem "Haus des Lehrers" am Alexanderplatz in Berlin eine besondere Lichtinstallation in Betrieb genommen: Blinkenlights. Es handelt sich hierbei um 144 einzeln geregelte Baustrahler, die die Fenster der oberen acht Etagen des Hauses erleuchten lassen. Daraus entsteht eine monochrome Matrix mit 8x18 Pixeln, mit der sich so einiges darstellen lässt: Die ganze Nacht über werden Animationen angezeigt, die auch jeder selbst erstellen kann, und über ein Mobiltelefon kann man Pong spielen und seine Liebesbriefe laufen lassen. Blinkenlights wird voraussichtlich noch bis Ende Februar 2002 in Betrieb sein. Weitere Informationen gibt es unter <http://www.blinkenlights.de>. -jmk





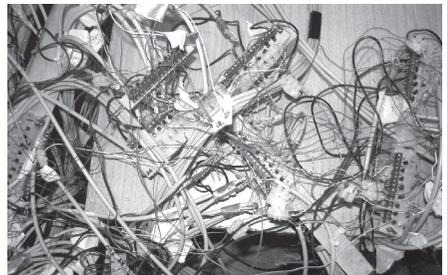
oben: der Steuerungsrechner, der die Lampen schaltet wird selbst nochmal von einer zweiten Maschine gesteuert, die die blinkenlights-Filme in konkrete ein/aus Zustände für einzelne Lampen umwandelt.



ganz oben: Helden (nach) der Arbeit – Papillon & Andreas geht's hier gerade so richtig gut...

oben: Blick vom Fernsehturm auf blinkenlights

unten: insgesamt annähernd sechs Kilometer Kabel wurden verlegt und verschaltet...



Datenreise: PKZ der DDR

© Henri C. 10/2001, Henri-C@web.de

Ein guter Freund empfahl mir kürzlich, mich doch einmal mit der PKZ (Personenkennzahl) der verblichenen DDR auseinanderzusetzen. Nun, da gäbe es im Netz... Schauen wir mal.

Bis dato hatte ich mich mit solcher Thematik eher am Rande befasst. Mir seien darob einige einleitenden Überlegungen gestattet, bevor ich mich den Eigentümlichkeiten der DDR-PKZ widme.

Kennziffern wie Telefonnummern, Kontonummern, Artikelnummern etc. sind Zeichenfolgen. Sie sollen einen Telefonanschluss, ein Konto, einen Artikel etc., also ein Objekt oder eine Person eindeutig kennzeichnen, bezeichnen. Eineindeutig meint, daß die Zuordnung in beiden Richtungen eindeutig ist. Zu einem Objekt gibt es genau eine Kennziffer und eine Kennziffer betrifft genau ein Objekt.

Aufbau und Struktur von kennzeichnenden Zeichenfolgen folgen nun nicht nur der Prämisse der Eindeutigkeit. Diverse Kriterien werden je nach Aufgabenstellung berücksichtigt. Darunter:

1.) Darstellungsökonomie und Datenraum

Ziffern können mit einem Zeichen 10 verschiedene Zustände darstellen (von 0 bis 9)

Buchstaben können mit einem Zeichen 26 verschiedene Zustände darstellen (von A bis Z)

ASCII-Zeichen können 256 Zustände darstellen (je nach Norm)

Je grösser der Datenraum eines Zeichens, desto kürzer kann die Zeichenfolge sein.

2.) Verarbeitungsökonomie

Während des Cyberpaläolithikums (ante DOS) beherrschte Knappheit alle Überlegungen. Speicherplatz war knapp, Rechenkapazität war knapp. Besonders in EDV-befreiten Regionen. Grossen Aufwand (für damalige Verhältnisse) erforderte das Umformatieren von Buchstaben in Zahlen. Das lässt sich vermeiden, wenn von vornherein nur Zahlen verwendet werden.

3.) Merkbarkeit

Zeichenfolgen werden nicht nur mit dem Computer verarbeitet; Mensch muss sie eingeben, auf Plausibilität prüfen und sie sich gelegentlich merken. Gerne benutzt man deshalb "sprechende" Abbildungsverfahren wie geläufige Abkürzungen etc. Generell kann unter "sprechend" jedes Abbildungsverfahren verstanden werden, dessen Verschlüsselung einfach und allgemein zugänglich ist. Dem gegenüber stehen die anonymen Verfahren, deren Codierung geheim oder rein zufällig sind.



4.) Skalierbarkeit

Aufbau und Einrichtung eines Kennzeichnungssystems erfordert großen Aufwand und dauert. Das lohnt nur, wenn das System hinreichend lange in Gebrauch bleibt. Die Konstrukteure werden also zukünftigen Dateninput einkalkulieren.

Historisches

Beschlossen 1969, eingeführt am 01.01.1970 sollte die PKZ zur flächendeckenden Erfassung und Kontrolle der DDR-Bürger dienen. Aber erst 1984 erreichte die damit beauftragte Behörde, die Zentrale Personen-Datenbank in Berlin-Biesdorf die volle Funktionsfähigkeit.

Aufbau und Struktur

Die im Netz von mir gefundenen Informationen und Hinweise zur DDR-PKZ sind in Details nicht einheitlich, insbesondere was die 11. Ziffer und den Prüfalgorithmus betrifft. Ich habe mich jeweils für die plausibelste und mir glaubhafteste Version entschieden. Eine Garantie für historische Wahrheit gibt das aber nicht.

Die Personenkennzahl der DDR besteht aus 12 Ziffern.

Die ersten 6 Ziffern bezeichnen den Geburtstag formatiert wie folgt:

TT MM JJ (Tag, Monat und Jahr jeweils zweistellig; Jahresangabe unter Wegfall des Jahrhunderts).

Die 7. Ziffer bezeichnet das Geschlecht und das Jahrhundert der Geburt:

- 2 bedeutet männlich/19. Jahrhundert
- 3 bedeutet weiblich/19. Jahrhundert
- 4 bedeutet männlich/20. Jahrhundert
- 5 bedeutet weiblich/20. Jahrhundert

Die 8. bis 10. Ziffer bezeichnet die Meldestelle bzw. das Melderegister. Dort waren die zugehörigen hardcopies gesammelt; diese Dienststelle vergab auch die PKZ. Angeblich kamen zur Bezeichnung der Meldestelle nur Zahlen von 001 bis 320 zum Einsatz.

Die 11. Ziffer war eine laufende Nummer. Sie diente zur Unterscheidung derer, die in den ersten 10 Ziffern übereinstimmen. Auch diese laufende Nummer wurde von der Meldestelle vergeben. Dabei gibt es eine Besonderheit; siehe weiter unten.

Die 12. Ziffer ist eine Prüfziffer zur Plausibilitätskontrolle.

Mit der DDR-PKZ haben wir also ein bis zur 10. Ziffer sprechendes Kennzeichen. Nur die 11. und 12. Ziffer sind anonym.

Prüfziffer

Prüfziffern sollen der Datensicherheit dienen. Hoert sich toll an, aber was heißt das konkret? Unter Datensicherheit wird hierbei hauptsächlich Übermittlungssicherheit verstanden. Das betrifft vor allem Eingabefehler, wobei eine oder mehrere Ziffern falsch gelesen oder eingegeben werden. Auch systematische Übertragungsfehler, bei deren Auftreten alle übertragenen Ziffern mit einem konstanten Faktor variiert werden, gehören dazu. Bei nicht korrekter Prüfziffer muss die Eingabe/die Übermittlung wiederholt werden. Eine Prüfziffer übernimmt damit die Funktion einer Protokollnotiz, wie sie ähnlich heute im Datenverkehr üblich ist. Mehr an "Datensicherheit" ist nicht drin, deshalb spricht man auch besser von Plausibilitätskontrolle. Schuld daran hat der geringe Umfang des Datenraumes, den eine Prüfziffer einnehmen kann. In etwa entspricht das einem pin mit einer Stelle, einer Art Kindersicherung also.

Die Berechnung der Prüfziffer m der PKZ erfolgt nach folgendem Algorithmus:

PKZ: a b c d e f g h i k l m

- 1.) $4a + 2b + c + 6d + 3e + 7f + 9g + 10h + 5i + 8k + 4l = x$
- 2.) $x : 11 = n ; \text{Rest} = y$
- 3.) $5y + 5 = z$
- 4.) $z : 11 = p ; \text{Rest} = m$ ist die Prüfziffer

Nachdem die Prüfziffer so ermittelt worden ist, wird sie mit dem Faktor 2 multipliziert (mit dem Gewicht 2 beschwert wie es auch heißt) und damit die Formel 1.) ergänzt. Dann wird ähnlich wie vor verfahren:

- 1.) $4a + 2b + c + 6d + 3e + 7f + 9g + 10h + 5i + 8k + 4l + 2m = x$
- 2.) $x : 11 = n ; \text{Rest} = 10$ bei richtiger Prüfziffer

Nun kommt die Überraschung: Ergab die Prüfung einen anderen Rest als 10 (etwa 0), hatte die vergebende Meldestelle eine andere laufende Nummer in der 11. Stelle (entspricht Buchstabe l in den Formeln) zu wählen.

OK, ich weiss sehr trockener Stoff, fast Essig. - Mut machen: Der zur Anwendung gelangte mathematische Apparat liegt ja nun durchaus im



fussläufigen Bereich. Nix Wurzel, nicht mal Quadrate, geschweige den Kommata, keine negativen, nur natürliche Zahlen! Na, das kriegen wir doch hin. Also wozu soll das nun dienen?

Beschränken wir uns erstmal auf den Prüfalgorithmus: Der erste Schritt ergibt eine relativ große Zahl, die mit dem zweiten Schritt wieder auf eine relativ kleine Zahl zurückgeführt wird. Das ist auch zwingend, denn im Ergebnis wollen wir wieder eine einstellige Zahl, eine Ziffer erhalten. Während des "Aufblähens" werden eine Reihe von Faktoren gebraucht (die "Gewichte"). Beim Reduzieren findet ein Teiler, hier die 11 Verwendung. Dem geneigten Betrachter fällt zweierlei auf. Nach Faktorenzersetzung liegt das kleinste gemeinsame Vielfache der Gewichte und des Teilers mit 27720 weit über dem für x zu erwartenden Wert, der unter 400 liegen dürfte. Das heißt für den Datenraum von x gibt es keinen gemeinsamen Teiler für das Aufbläh- und Reduzierverfahren. Genau das ist der Sinn der Übung, denn nur so lässt sich ein triviales Rückrechnen des Algorithmus vermeiden. Zum zweiten:

Das Restwertverfahren bei Gebrauch des Teilers 11 hinterlässt uns erstmal etwas ratlos, generiert es doch 11 verschiedene Werte (von 0 bis 10). Eine Abbildung dieses Datenraumes auf eine Ziffer wäre nun nicht mehr trivial. Die Konstrukteure des Algorithmus wählten nun einen sehr osteuropäisch anmutenden Weg: Was nicht passt wird passend gemacht! Knirscht zwar, aber funktioniert. Eine durchaus robuste Methode und äusserst praxisnah. Und garantiert nicht rückrechenbar!

Eigenschaften

Nach Aufbau und Struktur kennzeichnet die DDR-PKZ tatsächlich eindeutig Personen und nicht etwa nur Ausweise o.A..

Diese Kennzeichnung bedient sich zwar weitgehend "sprechender" Anteile, verzichtet aber vollständig auf die Verwendung des Namens oder Vornamens der zu kennzeichnenden Person. Mag das auch überwiegend der Verarbeitungsoekonomie geschuldet sein, kam es der Sozialismus-typischen Geheimniskrämerei/Paranoia sehr entgegen. Die Kopplung der PKZ mit dem Namen der Person erfolgte offenbar nur einmal, an einer Stelle, nämlich in der Pappkartei der vergebenden Meldestelle. Das war das Original, die ZPDB (Zentrale Personen-Datenbank Berlin-Biesdorf) nahm in ihren files im Sinne einer Kopie nur Bezug darauf.

Die DDR-PKZ wurde vermutlich - nach Etablierung des Systems - schon kurz nach der Geburt zugeteilt. Bisher (das wird dank Schily sicher so nicht bleiben) begann die Datenkarriere eines unbescholtenen (was immer das auch meint) Bundesbürgers erst mit der Ausstellung des Personalausweises (16. Lebensjahr) oder anlässlich der ersten sozialversicherungspflichtigen Beschäftigung.

Damit liegen ausreichend Informationen über die Struktur und den Aufbau der PKZ vor, dass ich mich an die Beantwortung einiger Fragen wage.

Reichte der Datenraum der 11. Ziffer überhaupt aus?

Die 11. Ziffer dient zur Unterscheidung zwischen denjenigen, die in den vorangehenden Stellen übereinstimmende PKZs haben. Auf Grund des gewählten Prüfverfahrens stehen worst case nur 9 Ziffern zur Verfügung. Die in's Auge gefasste Geburtenrate dürfte 30 Geburten pro 1000 Einwohnern und Jahr wohl kaum überstiegen haben (die tatsächliche Rate blieb meist darunter). Angenommen, die Geburten verteilen sich gleichmässig über's Jahr und die Meldestellen verwalten jeweils annähernd gleich viele Bürger, so rechne ich mal blauäugig hoch. Bei 17 Millionen Bürgern würde danach pro Meldestelle und Tag rund 4,4 Neuzugänge zu erwarten sein. Grob passt das. Vorsicht! Einige Parameter dieser Betrachtung streuten vermutlich stark. Das wird dann zum Problem, wenn Maximalwerte kumulieren. Aber genau das dürfte eingetreten sein. Plattenbausiedlungen hatten in der Aufbauphase oft nur junge Familien als Bewohner. Hier wurde es vielleicht schon eng. (Gar nicht auszudenken wenn in einem derartigen Wohngebiet dann auch noch Vollmond, Lohntütenball, Foehn und Parteitagsberichterstattung im DFF zusammenfielen). Fazit: In der Regel wird der Datenraum der 11. Ziffer sicher ausgereicht haben. Für nicht ausschließbare Spitzenwerte jedoch wäre mir das zu knapp. Ich wage nun noch eine Annahme: Bei den Konstrukteuren des Verfahrens haben wir es mit deutsch-gründlichen pedantischen Beamtenseelen zu tun. Dieser Wert dürfte nicht gestreut haben. Von solchen Charakteren Geschaffenes ist in der Regel schußfest, vandalensicher, überschwemmungsresistent und für die nächsten 500 Jahre angelegt (mindestens). Also bleibt ein dickes Fragezeichen!



Wäre die PKZ-Struktur Y2K-compatible?

In ihrer oben beschriebenen Struktur endet der Datenraum der PKZ am 31.12.1999. Die 7. Ziffer hat jedoch noch Luft. Denkbar wäre eine 6 für männlich und eine 7 für weibliche Geborene des 21. Jahrhunderts.

Konnte die PKZ manipuliert (gefälscht) werden?

Als die DDR dem Politbüro noch nicht abhandengekommen war, gab es ein Sicherungsinstrument, an dem fast alle denkbaren Manipulationsversuche scheitern mussten: Die Zentrale Personen-Datenbank. Angenommen, man hätte eine in sich schlüssige PKZ erfunden. Im Falle einer Kontrolle hätte die ZPDB entweder rückgemeldet, daß diese PKZ gar nicht vergeben wurde oder den Namen der Person, der sie rechtmässig zugeordnet war. Der letztere Fall wäre der wahrscheinlichere gewesen. (s.o. betr. 11. Ziffer)

Seitdem die ZPDB nicht mehr existiert oder im Zugriff ist, stellt sich die Situation anders da. Manches liegt nahe und vieles lässt sich denken. An dieser Stelle moechte ich aber nur einen Teilaspekt beleuchten, nämlich: Koennen zur Verschleierung der Identität einzelne Bestandteile der PKZ variiert werden, ohne daß die anderen Teile der Pkz einschliesslich der Prüfziffer verändert werden?

Ich nehme mir die Gleichung 1.) in ihrer zweiten Ausfertigung (mit Prüfziffer) vor. Eine erste Idee geht dahin , zwei oder mehrere Variablen auf der linken Seite derart zu variieren, daß die Zwischensumme x unverändert bleibt. Das führt zu einem System linearer Gleichungen, bei dem sich sicherlich einzelne Loesungen isolieren lassen. Mein Instinkt sagt mir dennoch, daß da noch mehr moeglich ist. Im späteren

Verlauf des Algorithmus wird die Zwischensumme x durch 11 geteilt; und nur mit dem ganzzahligen Rest wird weiter verfahren. Dieser Rest bleibt nun auch dann unverändert, wenn zu x beliebige ganzzahlige Vielfache von 11 (also 11, 22, 33, etc.) addiert werden. Was für x gilt, gilt auch für die andere Seite der Gleichung und dort natürlich auch für Teilsummen oder einzelne Variablen. Analog bietet sich an, in einer Art Umkehrschluß das Augenmerk direkt auf den Teilerrest zu richten. Ich behaupte mal frech, solange der ganzzahlige Rest nach Teilung durch 11 von einer Gruppe von Variablen erhalten bleibt, obwohl diese selbst variiert werden, bleibt es auch bei der selben Prüfziffer. Wer unbedingt moechte, sei hiermit eingeladen dieses explizit zu beweisen. Ich habe mich darauf beschränkt das an Hand einer kleinen Tabellenskalkulation zu überprüfen. Die eingangs gestellte Frage kann ich uneingeschränkt bejahen.

Umwege erhöhen die Ortskenntnis:

etwas zur Historie:

<http://www.fu-berlin.de/jura/netlaw/publikationen/beitraege/ws97-krawieckio3.html>

streng geheim!:

<http://www.nierenspen.de/pkz.htm>

let's calculate:

<http://www.garlipp.de/pkz>

"Volkes Stimme":

http://www.mbn-extra.de/ddr/info_5.htm

die hier und nicht in Wall Street?:

<http://bundesbank.de/>

"Zahlungsverkehr

"Prüfzifferberechnung (hier gibt's ne hübsche pdf-Datei; siehe Methode 52)

Keine Haftung für externe links!



Der Rundfunk dreht am Rad

Martin Springer, swann@camorra.org

"Schwarzsehen ist unsozial und schädigt den ehrlichen Bürger", verkündete Bayerns Medienminister Erwin Huber unlängst in der Süddeutschen Zeitung. Um dieses Problem zu regeln hat der CSU Politiker eine einfache Lösung auf Lager. Da ohnehin fast alle Haushalte fernsehen, kehrt er die Beweislast einfach um – nur wer der Einzugszentrale versichert, kein Empfangsgerät zu besitzen, wird von der allgemeinen Gebührenpflicht entbunden.

"Was ficht's mich an", fragt sich der ehrliche Hacker, der seinen Informationsbedarf sowieso lieber durch die Datenschleuder, die Tagespresse oder die Mailinglisten seiner Wahl stillt. Der Fernseher, der allenfalls zum Anschauen von Videocassetten oder zum Programmieren des Commodore 64 diente, ist längst entsorgt. Leute, die in Zeiten von MP3, DivX ;-) und Flatrate monatlich 31,58 Mark an die GEZ abdrücken, entlocken uns ein müdes Lächeln.

Der Rundfunkgebührenstaatsvertrag schreibt vor, dass schon der Besitz eines Rundfunkempfangsgeräts zum Gebührenzahlen verpflichtet. Zwar sind Rechner, die Rundfunkprogramme ausschließlich über Angebote aus dem Internet wiedergeben können, nach diesem Vertrag bis Ende 2004 von der Gebührenpflicht ausgenommen. Geht es nach Huber, müssen wir uns aber ab Januar 2005 auf eine Zwangsabgabe gefasst machen, ob wir den Rundfunk empfangen wollen oder nicht. Vielleicht sollten wir uns also einnal mit einer Institution beschäftigen, die uns – ignorieren oder nicht – spätestens in drei Jahren einholen wird?

Rundfunk gibt es in Deutschland genau wie Schulen, Universitäten oder Hallenbäder. In den Landesrundfunkgesetzen ist die Aufgabe des öffentlich rechtlichen Rundfunks beschrieben: allen Bürgerinnen und Bürgern den individuellen, jederzeit möglichen Zugriff zu Informationen garantieren, Orientierung bieten und damit Medienkompetenz vermitteln. Zugangs-

barrieren sollen beseitigt werden, damit der Wandel zur Informations- und Wissensgesellschaft alle gesellschaftlichen Gruppen und Bereiche erfasse. Der öffentlich-rechtliche Rundfunk habe den Auftrag, die in einer Demokratie unerlässliche Informationsvielfalt und Meinungsfreiheit zu gewährleisten.

Auch die Hackerethik fordert, dass der Zugang zu Computern jederzeit möglich und Informationen frei sein müssen. Autoritäten zu misstrauen und Dezentralisierung zu fördern gewährleistet Meinungsfreiheit und Informationsvielfalt. Einen monatlichen Beitrag, um diese Ziele zu fördern, würden wir also durchaus akzeptieren, beschliche uns nicht immer wieder das dumme Gefühl, dass die Rundfunkveranstalter unsere Gebühren für ganz andere Zwecke einsetzen.

Dass der Intendant des MDR Udo Reiter rund 2,6 Millionen Mark an Gebührgeldern verbrannt hat, weil seine Anleihen auf die ecuadorianische Währung Sucre plötzlich nichts mehr wert waren, mag ja noch als Entwicklungshilfe durchgehen. Schliesslich muss ein Sender wirtschaften und dass Ecuador genauso riskant ist wie der neue Markt, kann ja keiner wissen.

Aber dass ARD und ZDF für die Übertragung von ein paar Fussballspielen der WM 2002 in Japan und Südkorea 250 Millionen Mark an den Rechtenhaber Leo Kirch zahlen, geht uns entschieden zu weit. Diese Entscheidung zeugt weder von Medienkompetenz noch



von grosser Fussballkompetenz – auch wenn CSU Medienminister Huber darauf wettet, dass die bayerischen Spieler Deutschland doch noch qualifizieren.

Sei's drum, eigentlich ist das alles schon in Ordnung. Schliesslich spiegeln das Fernsehprogramm nur den Geschmack des Volkes und die Quoten den Zustand unserer Republik wider. Die Intendanten der Sender werden aufgrund ihrer Verbundenheit mit einer der beiden grossen Volksparteien vorgeschlagen, sind also praktisch vom Volk gewählt. Neben viel Dünnpfiff gibt es auch gute Sendungen (z.B. Chaoradio auf ORB). Ausserdem ist die Zukunft des Fernsehens digital und dafür zahlen wir ab 2005 doch gerne.

Schon 1997 (ein Jahr nach Leo Kirch's Alleingang mit DF1) haben Bund und Länder begonnen, die Digitalisierung des öffentlich rechtlichen Rundfunks loszutreten. Herausgekommen ist dabei erwartungsgemäss erstmal eine Menge Papier und eine grosse Unsicherheit darüber, welchen technischen Standards der digitale Rundfunk folgen würde. Wo guter Rat teuer ist, ist der Softwarevertreter nicht weit – die amerikanische Firma OpenTV verkaufte der ARD einen sündhaft teuren digitalen Sender und es dauerte noch einmal ein Jahr, bis die ersten Decoder auf dem Markt waren, die das digitale Zusatzangebot der ARD nutzen konnten, sofern ihr Besitzer über eine Satellitenschüssel verfügte.

Trotz massiver Lobbyarbeit konnte sich das proprietäre OpenTV bis heute nicht als digitaler Fernsehstandard durchsetzen, ebenso wenig wie das Konkurrenzprodukt MicrosoftTV. Schuld daran ist ein internationaler Standard namens MHP (Multimedia Home Platform), der vom Digital Video Broadcast Project (DVB) entwickelt und von der ETSI (TS 101 812) heruntergeladen werden kann.

MHP ist so etwas wie eine gemeinsame API für Software, die über Kabel, Satellit oder terrestrisch auf den Fernseher draufgeladen wird. MHP Applikationen sind Java Xlets und hier kommt Bill Gates' Erzrivale SUN Microsystems ins Spiel, die den MHP Standard so mit Lizenzen absicherten, dass alle Gerätehersteller eine Abgabe an SUN zahlen und eine Open Source Implementierung de facto unmöglich ist.

Die öffentlich rechtlichen Sender haben sich denn auch zur zügigen Einführung des MHP Standards bekannt und es wird nicht mehr lange dauern, bis die ersten Xlets vom Himmel fallen. Spass an den Empfangsgeräten mit digitalem Fernsehen kann man indes auch jetzt schon haben. Die ökonomische (bis 2005 GEZ gebührenfreie) Lösung zum digitalen Fernsehen besteht aus einer DVB-PCI Karte von Siemens, Haupt-

page und Technotrend (Treiber gibts bei linuxtv.org). In einen Rechner gesteckt und mit einer Schüssel verbunden, lassen sich an die 1.000 digitale Programme empfangen, nicht nur ARD und ZDF, sondern zum Beispiel auch der arabische Sender Al Jazeera.

Auf der Festplatte benötigt eine Stunde digitales Fernsehen um die 2 Gbyte Speicherplatz, je nachdem mit welcher Qualität es gesendet wurde. Wem das zu viel ist, dem steht es frei, den MPEG2 Datenstrom in ein handlicheres Format zu konvertieren. Die Killerapplikation des digitalen Fernsehens ist denn auch, ganz wie von den Landesrundfunkanstalten gefordert, der individuelle, jederzeit mögliche Zugriff auf die Informationen unserer Wahl – unabhängig von Sender, Sendezeit oder Kanal. Und wenn die Werbung nervt, schneiden wir sie vor dem Abspielen einfach raus.

WM 2002, du kannst kommen! Unsere selbstgebaute digitalen Videorecorder nehmen die Spiele während wir noch schlafen und am Abend können wir dann mit Freunden, Bier und Beamer darüber fachsimpeln, wer Sieger wird.

Wäre da nicht noch das Problem mit der Verschlüsselung. Für das internationale Geschäft mit den WM Rechten ist es nämlich hinderlich, wenn man zum Beispiel auf Mallorca Fussball via ARD digital umsonst empfängt. Weil Kirch das in seinem Rechtedeal so festgelegt hat, dürfen ARD und ZDF die WM über Satellit nur verschlüsselt ausstrahlen. Wer frühzeitig auf die öffentlich rechtliche und bisher unverschlüsselte Zukunft des Fernsehens gesetzt hat, muss folglich zur WM entweder einen neuen, mit einem Conditional Access Modul ausgestatteten Decoder kaufen, oder er guckt in die digitale Röhre.

Ob dieser zum Himmel schreienden Ungerechtigkeit denkt man bei den Landesmedienanstalten derzeit ernsthaft darüber nach, die Decoder der betroffenen Haushalte kostenlos umzutauschen. Also ab in den Baumarkt, Billig-Decoder geholt und nächstes Jahr gibts dann dafür ein amtliches Gerät mit CAM. Die Smartcards zum Freischalten des digitalen Free-TV werden ehrlichen Bürgern dann vermutlich per Post von der GEZ zugestellt.

"Dummerweise beachtet ein Satellit die Ländergrenzen nicht", hat Norbert Schneider, Direktor einer Landesrundfunkanstalt gesagt. Recht hat er! Und weil deswegen das öffentlich rechtliche Fernsehen verschlüsselt werden muss, werden wir uns 2005 keine Smartcards zum Freischalten holen. Ohne die Möglichkeit zum Entschlüsseln sind unsere Rechner keine Empfangsgeräte und wir sind auch keine "unsozialen Schwarzseher".

Und das soll ein Wurm sein...?

by rude God from da ==- dead kaoz ==-

Die Nachricht, daß wieder mal irgendein VBS-Würmchen unterwegs ist entlockt einem inzwischen nicht mal mehr ein Gähnen. Verschont werden wird man davon in näherer Zukunft zwar nicht, aber es gibt einige interessante Aspekte in Zusammenhang mit Software-Getier, über die es sich nachzudenken lohnt.

Denn auch wenn im Zusammenhang mit beispielsweise dem ILOVEYOU-Virus von "Schaden in Millionenhöhe..." gesprochen wurde: Diejenigen Würmer, die es derzeit in die öffentliche Wahrnehmung schaffen, sind von den Konzepten und der Funktionsweise her vor allen Dingen niedlich.

Es ist einigermaßen schwierig, diese ganzen Viecher sinnvoll einzuteilen: Viren mit Zerstörungsfunktion oder ohne, Würmer, die sich per eMail fortpflanzen und Würmer, deren Autor ein Hamster ist, Trojaner für Linux oder für Windows, Wanzen mit Sternen und solche ohne und so weiter.

Für diesen Artikel sind vor allen Dingen die jeweils zugrunde liegenden Konzepte und deren Implementation wichtig. Wer also eine umfassende Kategorisierung von Malware sucht, der soll woanders hingehen.

Ich bin noch nicht alt genug, um über die guten alten Zeiten zu jammern, als Virenprogrammierer noch richtige Programmierer waren, die versucht haben, auf möglichst wenig Speicherplatz möglichst effizient und raffinierte Schadens-, Infektions- und Tarnroutinen zu implementieren - natürlich in Assembler. Das waren noch richtige Männer! Aber die Viren und Würmer, die derzeit in den Massenmedien soviel Aufmerksamkeit erhalten und "Experten" immer wieder zu Weltuntergangsprognosen veranlassen,

lassen nicht besonders viel Sorgfalt oder Raffinesse erkennen.

Am deutlichsten zu sehen ist das bei vielen der VBS-Viren, wobei der Kournikova-Virus die extremste Ausprägung darstellt: Es wurde ausschließlich mit Hilfe von Vbswg 1.50b erstellt, einem der zahlreichen Virus-Construction-Kits. Viren zum Klicken. Toll. Man sehe sich nur mal den RameN-Wurm an. Die Whitehats sagen dazu: "Ramen.tgz is a UNIX worm written by (an) unknown author(s), who seems to have collected a patchwork of exploit scripts and wrapped them around a modified version of the Synscan vulnerability scanner."

Der Wurm scheint tatsächlich im wesentlichen aus ein paar ExploitZ und einigen Shellsripten zu bestehen, die die Worm Engine darstellen. Wenn man dem Autor nicht direkt Unfähigkeit unterstellen will, dann doch wenigstens Schlampigkeit. Er hat sich offensichtlich nicht besonders viel Mühe damit gegeben.

Allerdings wird es dabei nicht bleiben. Vor allen Dingen wird sich die Art ändern, wie Würmer eingesetzt werden. Die Sichtweise auf Würmer wird sich verändern und damit auch ihre Funktionsweise. Die kursierenden Viren und Würmer lassen den Eindruck von Willkürlichkeit entstehen. Ein System oder tiefere Absichten dahinter sind bisher nicht offensichtlich zu erkennen.



Ich denke aber, dass das Entwickeln von Viren und Würmern professionalisiert werden wird - wenn es das nicht schon ist. Der Nutzen und die Möglichkeiten solcher Software wird Leuten auffallen, die bereit sind, darin Zeit, Geld und Gehirnmasse zu investieren oder investieren zu lassen.

Die Absicht hinter den bisher kursierenden Würmern ist meistens nicht besonders raffiniert: Webseiten defacen, eine Hintertür installieren, sich möglichst weit verbreiten.

Eine Eigenschaft, zB rasend schnelle Verbreitung, die dem Wurm jetzt seinen Schrecken verleiht und ihn in der Berichterstattung der meisten Medien „erfolgreich“ macht, ist aber bei anderen Zielen hinderlich. Denn Würmer bergen ein riesiges Potenzial jenseits von Webseiten defacen und Aufmerksamkeit in der Presse abgreifen.

Hier konvergieren die Techniken, die sich bei Würmern und Viren im Laufe der Zeit als nützlich erwiesen haben und die Bestrebungen auf dem Feld der Exploit Automation. Es ist viel zu gefährlich, stundenlang in einem fremden Firmennetz zu hängen auf der Suche nach interessanten Informationen.

Aber vieles von dieser Arbeit - initialer Angriff, Analyse des Netzwerktraffics, Auskundschaften der Netzwerkstruktur, Finden weiterer anfälliger Hosts in diesem Netz, Durchsuchen von Dateisystemen und Dateien nach bestimmten Schlagwörtern - sind auch automatisierbar. Es wird Einiges an Aufwand und Zeit kosten, diese Ansätze sauber zu implementieren, aber die Vorteile liegen auf der Hand:

Ein Programm kann bei automatisierten Abläufen sehr viel schneller und sauberer agieren als ein Mensch. Der Geschwindigkeitsvorteil ist in der Tat von grosser Bedeutung. Auf einen cleveren, automatisierten Angriff kann man ebenfalls nur automatisiert reagieren. Ich möchte behaupten, dass die Angreifer derzeit den Verteidigern immer um einen Schritt voraus sind.

Kombiniert man eine gute Worm Engine dann noch mit einem ebensovollen Cartridge-Mechanismus, der es ermöglicht, neue Exploits unmittelbar nach ihrer Veröffentlichung zu integrieren, dann dürfte man den verantwortlichen Administratoren schon ordentlich den Tag versauen.

Hier tun sich zwar noch einige Probleme in der praktischen Umsetzung auf, aber die Lösung dieser Probleme ist nur eine Frage der Zeit und der Infrastruktur. Weiterhin ist ein Wurm, der einmal ausge-

setzt ist, schwer zum Aussetzenden zurückzuverfolgen, schwerer jedenfalls als ein menschlicher Angreifer der stundenlang eine Verbindung ins Zielnetzwerk offenhält - zumindest wenn der Aussetzende sich nicht völlig dämlich angestellt hat.

Zwar muss nach wie vor ein Informationsfluss zwischen dem Wurm und dem Aussetzenden bestehen, aber dieser wird auf ein Minimum reduziert.

Ein Wurm kann ausserdem auf völlig unvorhergesehenen Wegen von einem Intranet ins andere in Netze gelangen, in die ein normaler Angreifer nie gekommen wäre, weil er oft nicht die Ruhe und nicht die Gelegenheit hat, alles sehr gründlich abzusuchen. Würmer haben natürlich den entscheidenden Nachteil, dass sie nur bis zu einer gewissen Grenze "intelligent" sind. Allerdings kann der Wurm dann immer noch wertvolle Informationen liefern darüber, wo es sich lohnt, doch selbst Hand anzulegen.

Was den Intelligenzgrad und die Autonomie einer solchen Software angeht: Es sind zum Einen Grenzen gesetzt weil es mit der Künstlichen Intelligenz einfach noch nicht so weit her ist, zum Anderen weil man beim Schreiben eines solchen Wurms immer abwägen muss zwischen der Grösse des Programms und den Features.

Man wird nicht alle Features implementieren können, einfach weil ein 20 Megabyte grosser Wurm Gefahr läuft, schnell aufzufallen. Aber genau das will man vermeiden. Der Wurm soll heimlich, still und leise sein Arbeit tun und möglichst lange unentdeckt bleiben.

Der "Erfolg" zB von CodeRed, dass er sich sehr schnell sehr weit verbreitet ist uU gar nicht erwünscht. Ein Wurm ist hier eher als eine punktuelle Massnahme anzusehen.

Wegen der Sicherheit will ich jetzt nicht auf Details eingehen, wie man bestimmte Probleme bezüglich der Exploit Automation oder der Stealth-Techniken löst. Ich bin sicher, dass die entsprechenden Leute schon lange an solcher Software arbeiten und dass noch entsprechendere Leute sowas schon längst in der Schublade, wenn nicht gar im Umlauf haben. "Writing Internet worms for fun and profit" ist immerhin von 1999.

Aber ich will ja hier niemandem zuarbeiten, der nicht von alleine auch auf die passenden Ideen gekommen wäre.

Lange kann es jedenfalls nicht mehr dauern...



Hacking the City

von Tina <tina@haecksen.org>

Urban Hacking ist ein Begriff, der sich seit Anfang der Neunziger Jahre in der Welt ausbreitet. Der Ausdruck selbst ist relativ schwammig und kann eine Menge Aktivitäten beinhalten. Dieser Artikel präzisiert die Angelegenheit etwas.

Motivation für Urban Hacking kann sowohl ein gewünschtes politisches oder soziales Statement sein, als auch Neugier auf die Dinge hinter der Fassade und der Spass am Ausprobieren kreativer Möglichkeiten. Die Frage, wie man die Ressourcen einer Stadt für sich nutzbar macht, steht dabei im Mittelpunkt. Nicht selten vor allem, weil die Probleme, gegen die Urban Hacker kämpfen, genau durch stadtspezifische Verordnungen, Angewohnheiten oder Gegebenheiten verursacht wurden. Hacktivismus als Protest, der Spass macht.

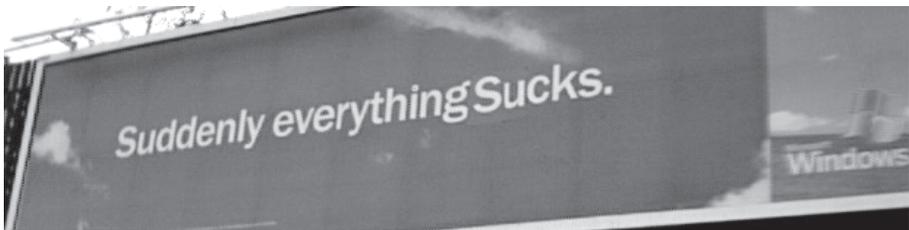
In Amerika sind Hacktivist*innen um einiges sichtbarer als in Europa, was sicherlich auch daran liegt, dass Europa im Vergleich zur USA noch relativ entspannt ist, was bürgerliche Freiheiten angeht. Eine der grössten Hacktivismusgruppen in Amerika sind die Adbusters [1], die mit ihren Aktionen teilweise sogar bis nach Europa rüberschwappen. Am bekanntesten sind die Adbusters für ihre Kampagnen gegen die grossen amerikanischen Konzerne, gegen die Medienkonglomerate und gegen das allgemeine Konsumverhalten ihrer Mitbürger. Und natürlich für ihre ablehnende Haltung der massiven Werbeflut gegenüber, die sich über alle Bereiche des täglichen Lebens ergiesst.

Unter anderem organisieren die Adbusters Aktionen wie die "TV Turnoff Week". Sie motiviert Menschen in ganz Amerika, eine Woche lang den Fernseher auszulassen, um darüber zu reflektieren wie ihr Zeit-

management so aussieht ohne die tägliche Berieselung. Jetzt mag der vorurteilsbehaftete Nerd sagen, dass die Menschen in Amerika ja sowieso nicht denken, und diese Aktion damit eh nur die Leute erreicht, die dafür schon vorher empfänglich waren, aber man sollte niemals die Macht von Mund-zu-Mund Propaganda unterschätzen. Diese Art der Realitätserweiterung führt zwar in der Regel nicht dazu, dass sich Menschen plötzlich eines völlig anderen besinnen, anfangen Bäume zu pflanzen und nie wieder fernsehen, aber immerhin scheinen sich mehr und mehr Leute in Amerika diesen Kampagnen zu öffnen und erleben so eine andere Art, ihren Alltag zu organisieren.

Radikaler sind da die Leute von Whitedot [2], die sich gleich ganz gegen das Medium Fernsehen wenden, und das auch eindrucksvoll demonstrieren. Sie bedienen sich geschickter Sozialmanipulation, um die Befürworterfront interaktiven Fernsehens zu unterwandern (siehe letzte DS).

Hacktivismus zielt allerdings auch auf andere Teile der Tunnelrealitäten ab, zum Beispiel auf das leidige Kamera- und Überwachungsproblem auf öffentlichen Plätzen, welches in Amerika und England schon lange zum Alltag gehört, und auch in Deutschland immer mehr zum Faktum wird. Während allerdings deutsche Projekte wie die Aktuelle Kamera [4] in Bremen oder Chaos Circuit Television in Köln auf Bürgeraufklärung





Eines von vielen Plakatwänden, wie sie diesen Spätsommer in Berlin anzutreffen waren.

setzen, versuchen amerikanische Hacktivistinnen mit einer eher ungewöhnlichen Kampagne, sowohl Passanten und Bürger, als auch die Menschen hinter den Kameras zu erreichen. Die Surveillance Camera Players (SCP) [5] studieren kurze, oft nur minutenlange Stücke ein, mit Dialogen oder Erläuterungen auf Papptafeln, und führen diese Stücke dann auf öffentlichen Plätzen, direkt unter den Überwachungskameras, auf. Klassiker sind dabei natürlich 1984 in der Zweieinhalb-Minuten-Version, und Warten auf Godot, ebenfalls radikal gekürzt. Das Konzept dieser Gruppe hat sich mittlerweile auch in anderen Ländern durchgesetzt, und die SCP geben häufig Gastspiele, unter anderem auch in der Londoner U-Bahn. Geplant ist, möglichst viele Ableger dieser ungewöhnlichen Schauspielgruppe zu gründen. Das Konzept der SCP, mit irrwitzigen Aktionen auf das Problem der Überwachung aufmerksam zu machen, scheint aufgegangen zu sein, sieht man sich die Massen von Menschen an, die bei diesen 'Aufführungen' stehenbleiben und zuzucken.

Es gibt allerdings auch Urban Hacking Gruppen, die sich auf das altbewährte Guerilla-Spiel einlassen und am Randbereich der Legalität agieren. Die Billboard Liberators [6] haben sich der kreativen Umgestaltung von städtischen Werbeflächen verschrieben, ganz nach dem Motto: 'Wir sind die Stadt, und der Stadt gehört die Werbefläche'. Auf der aktionsbegleitenden Webseite erfährt man, wie man Farbeier präpariert,

und kann Erfahrungsberichte vergangener Aktionen nachlesen. Der Schwerpunkt der Billboard Liberators liegt in der Message, die das Plakat hinterher vermitteln soll. Da die Bewegung schon seit Ende der Siebziger Jahre existiert, haben sie eine bewundernswerte Historie an veränderten Plakatwänden; immer mit einer Portion Humor neben der Medienkritik, die ja auch ein Ziel hat: möglichst viele Menschen erreichen.

Beispielgebend für die Spass Seite des Hacktivismus sind die Junx und Mädels von Infiltration [7], einer kanadischen Gruppe, deren Hobby es ist, dorthin zu gehen, wo noch nie ein Nerd zuvor war. Die Innereien von Krankenhäusern, U-Bahntunneln, verfallenen Gebäuden, Schiffen im Hafen stehen auf dem Besichtigungsplan. Aber auch die 'Infiltrators' haben eine Hacker Ethik: nichts zerstören, kein Chaos hinterlassen, nichts stehlen. Insofern lassen sich auch Urban Hacker in das grosse Geflecht der Hackerkultur einbinden. Und das ist auch gut so.

[1] <http://www.adbusters.org/>

[2] <http://www.whitedot.org/>

[3] http://www.whitedot.org/issue/iss_story.asp?slug=privacyattheyaleclub

[4] <http://www.aktuelle-kamera.org/>

[5] <http://www.notbored.org/the-scp.html>

[6] <http://www.billboardliberation.com/>

[7] <http://www.infiltration.org/>



XSLT-Handler für Apache

von Arne

XML und XSLT waren der Hype des vergangenen Jahres. Was allerdings fehlte, war das Bindeglied, der passende Handler, um einen XSLT-Parser in einen Webserver einzubinden. Mit etwas Aufwand schreibt man einen XSLT-Handler selbst, der, zusammen mit einem Webserver und einem XSLT-Parser, eine vollwertige XML-Publishing-Lösung bietet. Übrigens: Das ist auch der Handler, der auf www.ccc.de zum Einsatz kommt.

XML ist ein äusserst flexibles, aber auch beliebiges Datenformat.[1] XSLT ist die passende Stilsprache, um XML-Quellen auf den verschiedensten Ausgabegeräten darstellen zu können.[2] Da XSLT in Client-Applikationen aber nur sehr schlecht implementiert ist, sollte der XML/XSLT-Transformationsprozess server-seitig stattfinden.

Die Voraussetzung für eine XML/XSLT-Transformation ist ein XSLT-Parser, der in das XSLT-Handler-Modul eingebunden wird. Unterschiedliche XSLT-Parser sind verfügbar: Xalan-J, Xalan-C++, XT, Sablotron, Saxon und andere, die die entsprechenden Standards, XSLT und XPath, unterschiedlich weit und in unterschiedlichen Sprachen, Java und C++, implementiert haben. Auch ein XSL-Formatting-Objects-Prozessor lässt sich in den Handler einbinden, damit können PDF-Dateien aus XML-Quellen angeboten werden.

Die bisher verfügbaren XSLT-Handler kamen aus verschiedenen Gründen nicht in Betracht. Sie waren zu unflexibel oder zu kompliziert in den Webserver einzubinden. Also wurde ein passender XSLT-Handler selbst geschrieben: "less code, more flexibility[tm]". Der Vorteil dieser Arbeit ist bedeutend. Das XSLT-Handler-Modul ist einfach anzupassen und zu erweitern und ermöglicht eine erheblich bessere Kontrolle über weite Teile des Publikationsprozesses.

Obwohl das hier beschriebene Modul ausschliesslich mit einem Apache-Webserver getestet wurde, ist das Konzept so universell, dass es sich in jeden anderen Webserver integrieren lässt.

Apache-Konfiguration

Der XSLT-Handler bestimmt anhand der Anfrage-URL die XML-Quelle, das Ausgabeformat und welche XSL-Vorlage zu verwenden ist. Dann startet das Modul einen XSLT-Parser, setzt die Ausgabe zusammen und übergibt diese an den Webserver, der sie dann an den Client liefert.

Das XSLT-Handler-Modul ist in Perl geschrieben, allerdings ist dafür genausogut jede andere Sprache denkbar. Im folgenden skizzieren wir nur den Ablauf, der gesamte Perl-Code ist online abrufbar.[3]

Im Einzelnen

Zuerst wird die Anfrage-URL, d.h. die Apache-Umgebungsvariable REQUEST_URI in einzelne Komponenten zerlegt: \$document_location, \$document_name und ggf. \$type.

```
$requested_url = "/path/to/requested/  
document.html" $document_location = substr "$  
path/to/requested" $document_name = substr  
"document"
```



Das Ausgabeformat \$type richtet sich entweder nach der angefragten URL, d.h. nach der MIME-Endung. foo.html liefert eine HTML-Version, foo.wml die WML-Version usw. ...

`$document_type = suffix of $requested_url`

... oder nach dem Browserprogramm des Abfragenden, d.h. der Apache-Umgebungsvariable HTTP_USER_AGENT.

```
if $http_user_agent contains "MSIE", then
$type = "explorer"
if $http_user_agent contains "Java", then
$type = "java"
if $http_user_agent contains "Lynx", then
$type = "lynx"
if $http_user_agent contains "Nokia-WAP-Toolkit", then
$type = "wml"
if $http_user_agent contains "Mozilla", then
$type = "netscape"
```

Wer Netscape Navigator und Internet Explorer voneinander unterscheiden möchte, sollte bei dem Teilstring Mozilla aufpassen, da sich die meisten Browser als Mozilla ausgeben. Es hat sich bewährt, zuerst nach dem Teilstring MSIE zu suchen und die Abfrage nach Mozilla an das Ende zu setzen. Genauso schwierig ist es, mittels des HTTP_USER_AGENT die

WAP-Browser zu erfassen. Dafür bietet sich die Kombination mit der MIME-Endung an.

Als nächstes wird die XML-Quelle bestimmt. Hier wird von einer Datei ausgegangen, aber auch eine Datenbankanfrage ist möglich.

`$xml_file = $document_root$document_location/$document_name.xml`

Sollte diese Datei nicht existieren, wird ein 404-Fehler angezeigt.

```
if $xml_file does not exist, then print
"error 404" and exit
```

Anhand des Ausgabeformats wird eine XSL-Vorlage ausgewählt - dafür gibt es mehrere Möglichkeiten. Es folgt einem bestimmten, festzulegenden Muster, z.B. gibt es globale XSL-Vorlagen für alle XML-Dateien...

`$xsl_template = /global_style.xsl`

... oder die Silvorlagen haben einen Namen, der sich aus dem Namen der XML-Datei und dem Ausgabeformat zusammensetzt...

`$xsl_template = xml_file-type.xsl`



... oder anhand der `<?xml-stylesheet ...>`-Anweisung in der XML-Datei.

open `$xml_file` and search for lines containing xml-stylesheet tags `$xml_template = URL` mentioned inside the `xml-stylesheet` tag

Allerdings müssen dann alle XML-Dateien eine solche Zeile beinhalten. So kann auch ein evtl. vorhandenes Media-Attribut ausgewertet werden:

open `$xml_file` and search for lines containing xml-stylesheet tags if one of these lines contains "media=\$type", then choose it otherwise choose the first/last `xml-stylesheet` tag `$xml_template = URL` mentioned inside the `xml-stylesheet` tag

Es können auch beide Möglichkeiten kombiniert werden. Z.B. hat die `<?xml-stylesheet ...>`-Anweisung Priorität, ansonsten wird eine globale Stilvorlage verwendet.

Sollte die XSL-Vorlage nicht existieren, wird ein 404-Fehler angezeigt, der auf die existierende XML-Version hinweist.

if `$xml_template` does not exist, then print "error 404 but xml exists" and exit

Mit der XML-Datei und der XSL-Vorlage wird der XSLT-Parser gestartet

execute `/path/to/xsltparser` with arguments: `$xml_file` and `$xml_template` `$output = result`

Die Ausgabe wird dann an den Client übergeben.

```
print "Content-type: $mime_type($type)\n\n$output"
```

An dieser Stelle haben wir einen funktionierenden XSLT-Handler für unseren Webserver, der sich den meisten Erfordernissen anpassen lässt und in alle Richtungen erweiterbar ist. Auf zwei Erweiterungen möchten wir im folgenden näher eingehen: Caching und dynamische Seiten.

Caching

Der XML/XSLT-Output wird gespeichert. Bei der nächsten Anfrage wird statt einer erneuten Transformation lediglich der zuletzt gespeicherte Output gelesen und weitergegeben. Dazu muss der Inhalt des Caches mit der XML-Quelle verglichen werden, ob der Inhalt noch aktuell ist oder die XML-Datei zwischenzeitlich geändert wurde.

Nachdem die XML-Quelle und das Ausgabeformat bestimmt wurden sowie die Existenz der XML-Datei bestätigt ist, gibt es drei Möglichkeiten. (Den Sonderfall, dass eine HTML-Datei existiert und eine XML-Datei nicht, lassen wir ausser Acht. Stattdessen gehen wir für jede Ausgabe immer von einem XML-Master aus.)

- * 1. Die HTML-Datei existiert, die HTML-Datei ist neuer.
- * 2. Die HTML-Datei existiert, die XML-Datei ist neuer.
- * 3. Die HTML-Datei existiert nicht.

Im ersten Fall liegt eine gecachte HTML-Version vor, diese wird einfach als `$output_file` gelesen und an den Client weitergegeben. In den letzten beiden Fällen wird eine neue Transformation angestoßen, und dann das Ergebnis in einem Verzeichnis abgelegt. Natürlich muss dieses Verzeichnis für das Modul beschreibbar sein. Im zweiten Fall wird die bereits existierende HTML-Datei überschrieben.

Es wird also geprüft, ob zum einen eine HTML-Version vorliegt und ob zum anderen diese neuer ist als die ursprüngliche XML-Datei. Das obige Skript wird um folgende Zeilen erweitert:

```
if $output_file exists and $output_file is newer than $xml_file, then deliver $output_file else run the above script and save the output to disk
```

Der vollständige Perl-Code für das XSLT-Handler-Modul mit Caching ist ebenfalls online abrufbar.[4]

Performance

Ausreichende Leistung, d.h. eine schnelle Lieferung der angefragten Seiten, ist ein wichtiger Faktor für ein funktionierendes Internetangebot. Obwohl heutige Systeme über weit mehr Leistung verfügen als sie für durchschnittliche Aufgaben tatsächlich benötigen, kann eine XML/XSLT-Transformation einige Zeit dauern. Insbesondere dann, wenn ein Java-XSLT-Parser zum Einsatz kommt. Das Starten und Kompilieren eines CGI-Skripts nimmt zusätzliche Zeit in Anspruch.

Im Falle von Perl lässt sich mit dem Einsatz von `mod_perl` ein erheblicher Performanzgewinn erreichen. Falls dann noch das Modul als Apache-Perl-Modul umgesetzt wird, erreicht es eine Performanz die sich mit statischen Seiten messen kann. Die folgenden Zahlen geben einen Überblick über die Geschwindigkeit des Moduls (getestet mit OpenBSD auf einem Pentium 200, Apache Webserver und Sablotron-XSLT-Parser).



Ohne Caching:

- * cgi-bin/perl 7 hits/sec
- * mod_perl/registry 10 hits/sec
- * mod_perl/apache::pm 14 hits/sec

Mit Caching:

- * cgi-bin/perl 11 hits/sec
- * mod_perl/registry 75 hits/sec
- * mod_perl/apache::pm 105 hits/sec

zum Vergleich statische Seite:

- * default-handler 180 hits/sec
- * mod_include 140 hits/sec
- * mod_php 90 hits/sec

Die Caching-Erweiterung, es sind nur wenige Zeilen, beschleunigt die Ausgabe von XML/XSLT-Transformationen erheblich.

Dynamische Seiten

Die aktuelle Apache-Version 1.3.x erlaubt nicht die Benutzung mehrerer Response-Handler gleichzeitig. Die XML/XSLT-Ausgabe kann also nicht an mod_include oder mod_php weitergegeben und serverseitig geparsed werden. (Obwohl ein Kaskadieren mittels Apache-Sub-Requests möglich ist. In diesem Fall wird aber ein vollständiger Request-Response-Zyklus durchlaufen. Auch können einzelnen Module das simulieren, z.B. das Apache-Perl-Modul OutputChain.) Erst mit der neuen Apache-Version 2.x ist Input-/Output-Filtering möglich, sodass die Ausgabe der XML/XSLT-Transformation an ein nächstes Modul weitergegeben werden kann.

Vor der Ausgabe an den Client lassen sich einige Zeilen schreiben, die das generierte HTML nach besonderen Befehlen absuchen, diese Befehle ausführen und das Resultat einsetzen. Wird das

Modul in z.B. Perl geschrieben, dann sind auch die serverseitigen Skriptelemente in dieser Sprache:

```
take $input_html and search for a
<plsp:scriptlet> tag
insert substring before the tag into $output_
html
execute <plsp:scriptlet>some code</
plsp:scriptlet> and insert the result into
$output_html
take the rest of the string and parse it
again
if there is no more tag, then insert the rest
of the string into $output_html
Selbstredend kann dieser Teil auch zwischen dem
Einlesen der XML-Quelle und der Transformation
stehen. Vorsicht: Fast jeder Code wird ausgeführt.
Dieser Teil sollte also mit Bedacht programmiert
werden und ggf. nur vorher bestimmte
Skriptelemente zulassen.
```

Fazit

Mit dem hier beschriebenen Aufwand bekommt man eine Publishing-Lösung, die erheblich flexibler, schneller und skalierbarer ist als die sonst verfügbaren.

[1] <http://www.xml.com>

[2] <http://www.w3.org/Style/XSL>

[3] <http://www.lirium.de/webdev/xslthandler/xslt-handler.pl.txt>

[4] <http://www.lirium.de/webdev/xslthandler/xslt-handler-cache.pl.txt>

Former heavyweight boxing champ Muhammad Ali visited the ruins of the World Trade Center on Thursday. When reporters asked how he felt about the suspects sharing his Islamic faith, Ali responded pleasantly, "How do you feel about Hitler sharing yours?"

<http://lists.elistx.com/archives/interesting-people/20010/msg00356.html>



Kaliber 3,5 Zoll – hack 'em from the hip

von Stefan Krecher

Die sogenannte 3.5 Zoll Diskette - sie hat noch lange nicht ausgedient. Auch wenn der Datenaustausch heutzutage i.d.R. über andere Medien stattfindet, hat die Diskette immer noch ihre Daseinsberechtigung. Gerade für Hacker bedeutet sie genügend Platz zum spielen und forschen oder fungiert als knallharte Waffe.

Überall dort wo man physischen Zugriff auf einen PC mit Diskettenlauf hat, kann man Bootdisketten aus vielen Gründen einsetzen.

Ob man seine Arbeitsumgebung auf einer oder mehrerer Disketten immer bei sich hat, um unabhängig vom auf dem jeweiligen PC installierten OS seine Arbeit zu tun oder ob man einen Rechner in einem Netzwerk in eine Passwort-Logging-Station verwandeln möchte.

Muss man einen PC mit gecrashter Platte so gut es irgend geht in Betrieb nehmen oder untersuchen oder ist man genötigt Netzwerkdiagnose zu Betreiben, was u.U. mit dem vorinstallierten Systemen nicht möglich ist.

Will man einen PC im Netz vorübergehend oder dauerhaft zum Router machen oder hat man einen großangelegten Hack auf ein Netzwerk vor - in allen Fällen tun Linux-Minidistributionen auf Disketten ihren Dienst.

Und dann gibt es natürlich Leute, die gegen den Größenwahn der Hard- und Softwareindustrie ankämpfen wollen und beweisen, das man mit relativ wenig Ressourcen bereits eine Menge machen kann.

Es gibt viele verschiedene Minidistributionen, die teilweise angepasst und erweitert werden können. Ich

werde hier nur eine kleine Auswahl beschreiben, eine Übersicht über gängige Distributionen gibt es z.B. unter [1].

Doch zunächst zum technischen Hintergrund der Diskettendistributionen.

In den meisten Fällen handelt es sich um Bootdisketten.

Im Bootsektor der Diskette befindet sich ein Bootmanager, z.B. Lilo, der einen Kernel laden kann, oder es wird direkt der Kernel ausgeführt. Wenn der möglichst abgespeckte Kernel geladen ist und die nötigen Peripherie-Treiber initialisiert sind, wird eine RAM-Disk angelegt, in die dann von Diskette das gepackte root-filessystem geladen und entzippt und schließlich gemountet wird. Wenn soweit alles funktioniert hat, wird nun der sogenannte Init-Prozess gestartet, der die restlichen Initialisierungen vornimmt und letztendlich zum "login:" führt.

Obwohl man Kernel, root-Filesystem und evtl. weitere Filesysteme mit Tools auf verschiedenen Disketten unterbringen kann, ist es nicht unüblich, alles auf eine Diskette zu packen.

Zum Erstellen des Filesystems kann man sich recht elegant eines loopback-device bedienen: es wird mit
`dd if=/dev/zero of=/tmp/fstest bs=1k`



count=4096

ein block-file generiert und ausgefüllt. Dann wird in diesem block-file ein Filesystem angelegt

```
mke2fs -m 0 -i 2000 /tmp/fstest
```

und mit

```
mount -o loop -t ext2 /tmp/fst/est /mnt
```

gemountet.

Dann beginnt die eigentliche Arbeit: das Filesystem mit Leben zu befüllen.

Die Datei /tmp/fstest wird dann noch gezippt, damit sie auf die Diskette passt.

Zu guterletzt wird, wenn man ohne Lilo arbeiten möchte, der Kernel mit dd auf die Diskette gebracht, mit rdev das sog. "ramdisk word" gesetzt (um dem Kernel mitzuteilen, wo er das root-filessystem findet) und dann ebenfalls mit dd, das gezippte filesystem hinter den Kernel auf die Diskette geschrieben.

Auf diese Weise lassen sich, auf den ersten Blick recht trivial, einfache Minidistributionen erstellen. Der Teufel sitzt allerdings im Detail, es ist auf alle Fälle ein langwieriges Unterfangen, dafür aber auch überaus lehrreich.

Nähere Informationen zum Erstellen von Bootdisketten finden sich unter [2].

Im Folgenden sollen bereits fertige Minidistributionen kurz beschrieben werden.

Da nicht alle Vorhandenen erfasst werden können, werden hier nur drei recht verschiedene Varianten mit ganz unterschiedlichen Zielsetzungen betrachtet.

muLinux

muLinux [3] ist eine italienische Distribution, die gut an eigene Bedürfnisse angepasst und in vielen Kontexten sinnvoll verwendet werden kann. Sie basiert auf einem 2.0.36er Kernel.

Es gibt verschiedene "plug-and-play addons" auf Disketten, mit denen das Leistungsspektrum der Basiskonfiguration erheblich erweitert werden kann. Das "SRV"-Addon richtet sich z.B. an Anwender, die spontan verschiedene Server-Dienste anbieten wollen. Auf der Diskette sind u.a. ein Web-, FTP-, Telnet-Server sowie die Samba Suite enthalten.

Das "WKS"-Addon ermöglicht es die einfachen, täglichen Aufgaben zu erledigen. So sind u.a. Lynx, Mutt, PGP, ssh und ein FTP-client enthalten.

Weitere Addons ermöglichen den Einsatz von X Windows Systemen mit verschiedenen Windowmanagern oder beinhalten Softwareentwicklungswerkzeuge wie gcc, tcl oder perl.

Die Entwicklung von eigenen Addons ist ohne Weiteres möglich und gut dokumentiert.

Die Installation der Basisdiskette(n) erfolgt menügesteuert und bietet verschiedene Varianten, von BOOT, ROOT und USR filesystem auf getrennten Disketten oder auf einer Einzigen, auf 1722K "hochformatierten" Disk. Letzteres ist die Standardeinstellung.

Die Basisdiskette an sich beinhaltet schon eine beeindruckende Menge an Software und reicht für viele Einsatzbereiche völlig aus: einfache mail-, irc- und ftp-clients, umfangreiche Dokumentationen und menügesteuerte Setuptools, sogar ein Paketsniffer und ein Portscanner sind enthalten, um nur einige Features zu nennen.

Gängige Hardware wird unterstützt und teilweise automatisch erkannt.

Im Großen und Ganzen, eine beeindruckend umfangreiche und einfach zu handhabende Distribution mit hohem Fun-Faktor.

TomsrTbt [4]

Dieser kryptische Name bedeutet laut FAQ: "Tom's floppy which has a root filesystem and is also bootable."

TomsrTbt basiert wie muLinux in der aktuellen Version auf dem 2.0.36er Kernel.

Der Haupteinsatz dieser Distribution liegt eher im Recovery-Bereich. Dank der umfangreichen Hardwareunterstützung werden auch Netzwerkkarten erkannt. Die Konfiguration von Netzwerkkadapter, Routen, DNS usw. muss allerdings per Hand erfolgen, dann hat man aber wenigstens mit Tools wie telnet oder snarf Zugriff nach draussen.

Die Software zum reparieren, untersuchen und erstellen von Filesystemen ist recht umfangreich, somit ist TomsrTbt ein gutes und schlankes Rescue- und Recovering-System zum "immer-dabei-haben".



Die Installation erfolgt unkompliziert per shell-script, letztendlich wird aber auch nur mit dd das rund 1.7MB große image auf Diskette geschrieben.

Trinux [5]

Für Netzwerkd Diagnose, bzw. um Fehleranalyse zu betreiben oder zum Hacken und Schabernack machen ist Trinux sicher die geeignetste Distribution.

Sie basiert auf einem 2.4.5er Kernel und erkennt Hardware gut und weitgehend automatisch.

Es gibt verschiedene gezippte Images, mit unterschiedlichen Hardwareausrichtungen, z.B. ein Image für gängige ISA/PCI Netzwerkkarten oder eins speziell für Notebooks mit PCMCIA Unterstützung. Die Installation funktioniert problemlos, indem mit dd, das Image auf die Diskette geschrieben wird.

Obwohl zusätzliche Software per Diskette nachinstalliert werden kann, liegt der Clou dieser Distribution in der vollautomatischen Installation via Netzwerk, was sich z.B. in einem bandbreit angeschlossenen Internetcafe gut macht.

Nach dem Booten, wird versucht die Netzwerkkarte per DHCP zu konfigurieren, wenn das erfolgreich war, werden von einem entfernten HTTP-Server mit snarf und dem mitgelieferten Script "getpkg" Tools und benötigte Bibliotheken gezogen und installiert. Die Liste der Software ist selbstverständlich konfigurierbar, der Server von dem geladen wird auswechselbar. Eigene Pakete können auf einem eigenen Server

bereitgestellt und separat nachgeladen werden. Bei so einer Vorgehensweise ist man in seinem Tun natürlich nahezu uneingeschränkt.

Die Auswahl der Software alleine auf dem Trinux-Server ist hauptsächlich auf Netzwerktools beschränkt, läßt aber in dem Bereich kaum Wünsche offen. Sniffer, Password-Logger, Hijacker, Tunneling-Software, Bruteforce-Tools, Vulnerability-Scanner, Portscanner – alles ist zu haben.

Linux-Minidistributionen machen nicht nur Sinn, sie machen auch Spass. Das Erstellen einer eigenen Distribution kann sehr viel Erkenntnisse über die Funktionsweise von Linux liefern und hat zudem noch eine Menge Hack-Value.

Vorhandene Distributionen zu benutzen und zu erweitern kann die eigene Lebensqualität in einer weitgehend windowsverseuchten Welt entscheidend verbessern.

- [1] <http://ldl.8m.com/mini/> (Linux Distribution List [Mini-distribution])
- [2] <http://www.linuxdoc.org/HOWTO/Bootdisk-HOWTO/> (The Linux Bootdisk HOWTO)
- [3] <http://sunsite.dk/mulinux/> (muLinux Project Home Page)
- [4] <http://www.toms.net/rb/home.html> (tomstrbt home page)
- [5] <http://www.trinux.org/> (Trinux: A Linux Security Toolkit)



"Thank you for your recent E-mail. I appreciate your concern. However, I am, at this time, completely satisfied with the size of my penis."



The Humane Interface

von Jef Raskin

"We are oppressed by our electronic servants.
This book is dedicated to our liberation."

Diese zwei Zeilen stammen aus dem Buch "The Humane Interface" von Jef Raskin, verantwortlich u.a. für die One-Button-Mouse, das Macintosh-Projekt bei Apple, SwyftWare und Canons Cat.

Wenn man sich noch nicht näher mit User Interfaces auseinandergesetzt hat, kann dieses Buch eine wahre Erleuchtung sein: User Interfaces müssen gar nicht Scheiße und unbenutzbar sein! Nein, es gibt sogar Menschen, die sich Gedanken machen, wie man ein User Interface am besten gestaltet, damit die Benutzer nicht wahnsinnig werden (dafür sorgt nämlich in den meisten Fällen schon die unterliegende Software).

In vielen Software-Projekten (besonders denen, die 'hobbymäßig' entstehen) gehört das User Interface in eine ähnliche Kategorie wie Dokumentation: langweilig, notwendiges Übel, "muss ich mal schnell noch machen".

Dabei kann ein übelriechendes User Interface die gesamte Software versauen, weil niemand Lust hat, sich durch die krude Bedienung zu schlagen, um an die eigentliche Funktionalität der Software zu kommen.

Jef Raskin hat mit seinem Buch seine Erfahrungen und Erkenntnisse bezüglich des Designs von User Interfaces durchaus verständlich zusammengefasst.

Zum Einen geht er immer wieder ein auf die Bedeutung von "guten" User Interfaces, zum Anderen erläutert er verschiedene Methoden und Aspekte, die ein User Interface "gut" oder eben "schlecht" machen. "User Interface" ist dabei zu verstehen als UI eines bestimmten Programms, des Betriebssystems oder auch die Beschaffenheit von Eingabegeräten - besonders der Tastatur als meistgebrauchtem solchen.

Obwohl er in seinen Beispielen vorwiegend auf den Otto-Normal-Benutzer eingeht (von dem sich die meisten Freaks eifrig distanzieren), lässt er keinen

Zweifel daran, dass besser durchdachte User Interfaces sämtlichen Nutzern eine Menge Ärger und Frust ersparen würden.

Ich selber bin sowieso eine überzeugte Verfechterin der Ansicht, dass gute User Interfaces die Welt retten könnten, aber ich würde das Buch prinzipiell allen empfehlen, die mal in die Verlegenheit kommen sollten, selber ein UI bauen zu müssen – aus einer sehr egoistischen Motivation heraus, versteht sich.

Jef Raskin streift zunächst die theoretischen Hintergründe: Wie funktioniert die menschliche Wahrnehmung? Mit diesen Erkenntnissen geht er ein auf diverse übliche Unarten beim Design von UIs. Als Beispiel seien hier Modi genannt... was für ein tolles Argument dafür, dass vi stinkt!

Es folgt ein eher langweiliges Kapitel über Methoden, mit denen man die Effizienz von User Interfaces messen kann. Das habe ich übersprungen, müßt ihr selber lesen.

In dem darauffolgenden Kapitel stellt Raskin einige ebenso interessante wie radikale Alternativen zu den heute gängigen UIs vor. Er weitet die durch das Buch hinweg formulierten Gedanken dann ausserdem aus auf Bereiche ausserhalb von UI-Design, z.B. die Konstruktion von Programmiersprachen oder die Gestaltung von Kabeln. (Ja, Kabel.)

Ich bin mir noch nicht sicher, ob es nun gut war dieses Buch zu lesen oder nicht, weil ich seit kurzer Zeit deutlich genervter bin von den schlechten UIs die mich überall anspringen. Andererseits: Wenn sich die Konzepte die Raskin da beschreibt in den Köpfen vieler Leute - besonders Programmierer - festsetzen, besteht ja doch noch Hoffnung, dass man diese Computer irgendwann mal benutzen kann ohne immer einen Beißknochen bereithalten zu müssen.

"We must bend the machine to work the way we do rather than change our language conventions to suit what is easiest to program."

"The Humane Interface" von Jef Raskin, Addison-Wesley, 2000, ISBN 0-201-37937-6, \$24.95

Kurzbiographie Jef Raskins <http://www.oac.cdlib.org/dynaweb/ead/stanford/mss/m1147/>

Lisa Thalheim



deleuze.net not found

von Sebastian Lütgert

Von Zeit zu Zeit wirft die Geschichte ihre leeren Flaschen aus dem Fenster, und es gibt tausend gute Gründe, das Ende des dotcom-Booms, das Verschwinden der digitalen Shopping Malls und das Verstummen des sie begleitenden Geschwätzes mit Schadenfreude zu quittieren.

Dass gerade den Kommerzialisierungsgegnern und Netzkritikern der ersten Stunde jedoch kein einziger dieser Gründe mehr einfallen mag, liegt weniger an ihrer legendär kurzen Aufmerksamkeitsspanne, als vielmehr an einer verborgenen und zugleich umso offensichtlicheren ideologischen Verwandtschaft zwischen den Visionären einer alternativ-autonom-anarchischen Netzkultur und den Apologeten der neuen digitalen Ökonomien und Märkte. Denn wenn es sich beim Zusammenbruch des e-Commerce um das Platzen einer "Spekulationsblase" gehandelt hat, dann war die grundlegende Hypothese, der schlagartig alle heiße Luft entwichen ist, vor allem die Wette, in den digitalen Netzen liesse sich der Kapitalismus an seine Grenze treiben, und das Internet werde eines Tages deleuzianisch gewesen sein. Eine Archäologie des vermeintlichen Wissens, das unter den Trümmern der Startups von gestern und in den Ruinen der Netzkritik von vorgestern begraben liegt, würde in beiden Fällen auf die gleichen Bruchstücke einer hoffnungslos euphorischen Verwendung jener Begriffe stossen, in denen Deleuze und Guattari Ende der 60er bis Ende der 70er den Kapitalismus zu denken versucht haben. Doch während jeder, der heute noch den Versuch unternähme, mit einem farbigen Badge am Revers und einem Businessplan in der Tasche ein paar Millionen Risikokapital zu akquirieren, mit schallendem Gelächter zu rechnen hätte, rennt zeitgleich eine ganze Generation selbstgemachter Netztheoretiker mit nicht viel mehr als jeweils einem ungelesenen Exemplar der Tausend Plateaus unterm Arm bei Kunstinstitutionen, Zeitungsredaktionen und Universitäten offene Türen ein. Dass mit letzteren die Rede vom Internet als rhizomatische Wunschmaschine, die entlang ihrer Fluchtlinien und Deterritorialisierungsvektoren harte Identitäten und feste Kapitalanlagen gleichermaßen verflüssige, in eine neue Runde zu gehen droht, ist vor allem deshalb so verheerend, weil die dritte Phase des Internet, deren Anfänge schon vor dem vielzitierten 11. September liegen, die erste zu werden scheint, die nicht mehr von der sozialen und

ökonomischen Romantik der frühen 70er angerieben worden sein wird, sondern von den globalen Kontrollphantasien jener Militärstrategen, die die Architektur des Netzes in den 60ern erfunden haben.

Wer heute den konjunkturellen Verlauf der Mesalliance von Neodeleuzianismus und Netzeuphorie nachzuzeichnen versucht, wird auf einen ersten Boom-Zyklus stossen, der etwa 1992 zunächst verhalten beginnt, nach einer Serie sprunghafter Anstiege 1995 seinen Gipfelpunkt erreicht und anderthalb Jahre später derart abrupt zu Ende geht, dass sich das nicht allein mit den diskursiven Gewinnmitnahmen erklären lässt, zu denen es immer kommt, wenn auf einmal sehr viele Leute das gleiche reden. Die verbliebenen Zeitzeugen verlegen diese erste Hochphase der digitalen Deleuzianer gern in eine mythische Vorgeschichte, für deren legendenumranktes goldenes Zeitalter sie den Begriff "The Short Summer of the Internet" durchgesetzt haben: sagenhafter Aufstieg und plötzlicher Fall einer theoretischen Strömung, die das Netz als hypertextuelles, antihierarchisches, graswurzelhaftes und tendenziell organloses Medium benutzt und gefeiert hat. Ein unvoreingenommener Rückblick hätte nicht nur zu zeigen, warum all diese Behauptungen sich schon bald als völliger Unsinn erwiesen haben würden, sondern auch ihren spezifischen Umschlagspunkt zu benennen: als den Moment, an dem die begriffliche Lebenswelt einer bis dahin nur quantitativ anwachsenden Minderheit so sehr an Trennschärfe verliert, dass sie qualitativ ins Mehrheitsfähige kippt. Wir haben es also eher mit einem feuchtwarmen Spätsommer der Netzkritik zu tun, zu dessen Zeit die entsprechenden Buzzwords längst überreif von den Bäumen hingen – und auch das nur, wenn man unbedingt der Mode folgen will, auf historische Entwicklungen ausgerechnet den Lauf der Natur zu projizieren.

Tatsächlich konnte man Mitte der 90er ganzen literaturwissenschaftlichen Fakultäten dabei zusehen, wie sie, verückt von der Idee des World Wide Web als



einer wild wuchernden Verweismaschine, riesige Gärten hypertextueller Theorie auf ihren Universitäts-Servern anlegten, während einen Flur weiter die Kollegen von der BWL bereits breite Schneisen durch den Info-Dschungel schlugen. Das Wort von der Datenautobahn machte die Runde, einer drohenden Stratifizierung, der weniger aus politischen als vielmehr aus ökologisch-ästhetischen Gründen die Rückkehr zur labyrinthischen Landschaftsarchitektur des Rokoko vorzuziehen sei. Diese Hoffnung auf das Entstehen gewissenhaft gepflegter netzliterarischer Hypertext-Rhizome hat sich von all den Verheissungen des deleuzianischen Internet am schnellsten erledigt, zumal die entsprechenden Versuche sich schon aus strukturellen Gründen jeder Lektüre entzogen und letztlich nur bewiesen, dass gerade nichtlineare Bewegungen zwischen Plateaus sich rein technisch nicht nachbilden lassen, sondern auf die lineare Organisation ihrer faktischen medialen Grundlagen angewiesen sind – und schon die nicht minder interaktiven Irrgärten des späten Barock haben schlechter "funktioniert" und waren weitaus weniger populär, als man gemeinhin annimmt.

Etwa zur selben Zeit ging auf einem benachbarten Feld, das sich damals gern als "kulturwissenschaftlich" bezeichnete, die Theorie vom Internet als Immanenzebene um, deren Protagonisten einen Sommer lang bis spät in die Nacht und früh in den Morgen verkehrtsgegendlich in den Chatrooms herumhingen und über die anti-identitären Verheissungen subjektloser Kommunikation – gefolgt vom virtuellen Ende ihrer vermeintlichen Körper – spekulierten. Auch in diesem Fall genügte ein Blick über die Grenze der eigenen Disziplin, um die Doktoranden der Juristerei dabei zu beobachten, wie sie die handfest transzendentalen Pfeiler von Online-Recht und Ordnung in den Cyberspace einzogen, was die Immanenzverfechter jedoch weder auf die Barrikaden noch zurück zur Kritik sondern nur umso tiefer in das Beharren auf der Gültigkeit der eigenen Erfahrung trieb. Der Irrglauben aber, die Schleier der bürgerlichen Subjektivierung würden sich lüften und die Grenzen des männlichen Körpers verschwimmen, begleitet seit dem 19. Jahrhundert die Einführung eines jeden neuen Mediums: die Einführung des Kabelfernsehens in den 80ern fand ihr Echo in den elegant gescheiterten medientheoretischen Manifesten und Meditationen der Agentur Bilwet, die Kinos der 20er stürzten ihre Besucher in kollektive Delirien, die heute ihrerseits Kopfschütteln auslösen, und als 1835 bei der Eröffnung der Eisenbahnstrecke zwischen Nürnberg und Fürth die ersten deutschen Hippies aktenkundig wurden, waren das weniger die Kritiker, die warnten, ab 30 km/h werde man verrückt, als vielmehr die-

jenigen Passagiere, die darauf bestanden, tatsächlich Farben zu sehen.

Hartnäckiger als im akademischen Milieu hat sich die Rede vom deleuzianischen Internet an seinen Rändern gehalten, in den sogenannten illegalen Wissenschaften, insbesondere der autonomen Medien- und "Pop"-Theorie, von wo aus die entsprechenden Lesarten und Begrifflichkeiten mittlerweile überall dort wieder massiv in die Institutionen zurückströmen, wo nur noch die spekulative Verzinsung vermeintlich subkulturellen Kapitals betrieben wird. Die zentrale Figur, auf die die ausserakademischen Netzforscher seit jeher ihre Hoffnungen projizieren, ist die des digitalen Nomaden, der ihrer Vorstellung nach ziel-, richtungs- und widerstandslos durch die elektronischen Netze wandert und von jeder physischen Territorialität befreit per Telefon, Kabel und Satellit von Kontinent zu Kontinent driftet. Doch während der Hypertext-Hype immerhin noch Grundkenntnisse von HTML zu popularisieren half und die Immanenz-Euphorie zumindest indirekt die Bilwetsche Figur des Datendandy hervorgebracht hat (der wenigstens noch so sehr Punk – also Materialist – war, um zu wissen, dass es allem anti-identitären Eigentlichkeitsgeschwätz zum Trotz die Techniken sind, die die Delirien bestimmen), bearbeitete die rhizomatisch-romantische Rede vom Netz-Nomaden als neuem Subjekt der Geschichte ihr Feld so gründlich, dass dort auf absehbare Zeit kein Gras mehr wachsen wird.

Die theoretischen Verheerungen, die die Verschiebung des Deleuzeschen Nomadismus-Konzepts ins Digitale hinterlassen hat, kommen insbesondere in der landläufigen Überzeugung zum Ausdruck, der Nomade sei von einem wie auch immer gearteten Wunsch nach Bewegung getrieben, obwohl doch selbst die Tausend Plateaus mehrfach explizit darauf hinweisen, dass es sich beim Nomaden gerade um jene Gestalt handelt, die bis zuletzt versuchen wird, ihren Ort zu halten, die sich nur im äussersten Notfall von der Stelle bewegt, der angesichts der drohenden Segmentierungen ihres lokalen Territoriums jeder Gedanke an das Gleiten auf globalen Oberflächen fremd ist und deren Konzept von Raum das genaue Gegenteil dessen darstellt, was wir gemeinhin als "Mobilität" bezeichnen. Und doch beharren seine Fans auf dem obszönen Irrglauben, ausgerechnet in den Surfern der digitalen Netze und elektronischen Wellen fände der Nomade seine aktuelle Entsprechung – obwohl letzterer doch gerade deshalb Wüsten und Steppen bewohnt, weil man dort, wenn überhaupt, am langsamsten vorankommt, und die Eigenheiten des Geländes ihn zudem davor bewahren, von den Protagonisten der neuen (vom späten Deleuze zurecht als genuin kontrollgesell-



schaftlich gedinsten) Sportarten – Springern, Gleitern und eben Surfern – heimgesucht zu werden. Ein Blick in die Geschichte zeigt, dass der Nomade zwar immer wieder auf unvorhergesehene Weise von mächtigen, zum Teil weit überlegenen Feinden in die Flucht geschlagen, nie zuvor jedoch so schlamlos durch die Gegend gezerrt wurde wie in den Deleuzianischen Neunzigern des Internets, deren Ende noch immer nicht in Sicht ist, so dass man den Nomaden weiterhin vor allem vor seinen Freunden in Schutz nehmen muss.

Nun herrscht allerdings auch bei Leuten, die nicht gleich jede begriffliche Verwirrung und jedes konzeptuelle Knäuel als potentielles Rhizom feiern, die Ansicht vor, all diese hippiesk-esoterischen Ausläufer der mythischen Vorgeschichte des Internet hätten sich, wenn nicht erledigt, so doch angesichts der weitgehenden Kommerzialisierung, Stratifizierung und Zensurermächtigung des World Wide Web so weit zurückgezogen, dass aus dieser Richtung keine ernsthafte Gefahr mehr drohe. Der Deterritorialisierungssommer, so ihre These, sei in den naturgesetzlich notwendigen Herbst der Reterritorialisierung umgeschlagen, und der abrupte konjunkturliche Einbruch der Netzkritik erkläre sich schlicht aus dem im selben Moment umso plötzlicher einsetzenden Boom des Neuen Marktes. Dabei verkennen sie jedoch völlig, dass auch das ideologische Gepäck der Startup-Gründer, e-Entrepreneure und Risikokapitalisten, die zwischen 1996 und 1997 die diskursive Vorherrschaft im Internet übernahmen, zu einem nicht geringen Teil aus ähnlichen Versatzstücken eilig quergelesener – primärer wie sekundärer – Deleuze/Guattari-Texte bestand, die jetzt jedoch auf eine derart irre Weise zu ökonomischen Modellen und Businessapplikationen kurzgeschlossen wurden, dass sich daneben noch die windigsten Theorien von der neoural-nomadischen Zukunft des Cyberspace wie harte Wissenschaften ausnahmen.

In ihrem grundlegenden, hierzulande weitgehend ignorierten Aufsatz "The Californian Ideology" haben Richard Barbrook und Andy Cameron schon 1995 nicht nur das bizarre theoretische Patchwork beschrieben, auf dessen Grundlage die Apologeten des Online-Business schon bald ihren gleichermassen kurzen wie triumphalen Siegeszug antreten sollten, sondern auch die kulturellen Herkunftslinien der neuen unternehmerischen Strategien und Tugenden zurückverfolgt, die bis heute die Management-Seminare beherrschen: absurde Fusionen von Slackertum und Technikoptimismus, die allerdings – im Gegensatz zur deutschen Ideologie (Netzkultur als völkische Einheit von "Laptop und Lederhose") – ohne reaktionären Ballast auskamen. Die Internet-Revolution des

e-Commerce war gerade nicht die konservative Gegenrevolution einer Wirtschaftselite, die die Abenteuerspielplätze des Netzanarchismus abräumte, sondern die Fortsetzung dieses Anarchismus mit anderen Mitteln: der späte Triumph einer in der Hippiebewegung der amerikanischen Westküste verwurzelten politischen Strömung, die seit den 60ern für einen radikalen Liberalismus eingetreten war, der sich als Option auf "analogen" sozialen Fortschritt zwar spätestens mit den 80ern erledigt hatte, als grundlegende Ideologie einer neuen digitalen Sozialutopie jedoch schon seit den frühen 90ern eine ungeahnte Renaissance erlebte. Die vor allem in Wired, dem Zentralorgan der Bewegung, lancierte Wette lautete, dass die Idee von der radikalen Freiheit der Individuen, die sich als soziale Forderung nicht hatte durchsetzen lassen, im Zeitalter der globalen Vernetzung sich als zwangsläufige Folge des technischen Fortschritts ganz von selbst realisieren würde.

Was den umherschweifenden Unternehmern des digitalen Kapitalismus – die sich in ihrer Hochphase, 1999, sogar unwidersprochen nachsagen ließen, in Wirklichkeit an der Errichtung des globalen Cyberkommunismus zu arbeiten – an Deleuze gefiel, war neben der grob verkürzten Theorie, die Funktion des Kapitals bestehe hauptsächlich darin, fortwährend Grenzen zu verschieben und niederzureissen, vor allem der (bei Deleuze vor allem von Nietzsche her in den Text strömende) Vitalismus, der sich in Richtung einer biologischen Über-Metaphorik verschieben liess, in deren Begriffen fortan das Funktionieren ökonomischer und sozialer Systeme beschrieben werden sollte. In Reinform liess sich dieses Denken in "Out of Control", dem Hauptwerk des ehemaligen Wired-Herausgebers Kevin Kelly, bestaunen, wo Kapital als Natur, Kapitalismus als Biosphäre und das Zirkulieren von Geld, Menschen und Ideen um den Globus als natürliches Flottieren von Schwärmen, Herden und Wellen im organischen Ganzen eines ökologisch selbstregulierten Freien Marktes gedeutet wurde – mit dem Treppenwitz, dass noch das Platzen der "Spekulationsblase" sich als finale Ankunft des organlosen Körpers hätte interpretieren lassen. Kellys Nachfolger bei Wired, die ansonsten vor allem damit beschäftigt waren, ihre vulgär-schizoanalytische Kapitalismustheorie – Geldströme (Venture Capital) gegen Scheissströme (Content) – als Businessmodell anzupreisen und das nahende Ende der Lohnarbeit auszurufen, verkündeten bald darauf, das Internet lebe tatsächlich, und entwarfen mit spürbarer Verzückung bereits das Szenario pervasiv gewordener, sich real in die Natur auflösender Netze, deren kleinste organische Knoten wahlweise von Biotech-Startups in den menschlichen Körper versenkt oder von AT&T-



Helikoptern flächendeckend über den Metropolen abgeworfen würden.

Einzig die europäische Linke, die das Studium amerikanischer Internetzeitschriften in den 90ern fast vollständig versäumt hat, hielt solche Phantasien noch zu einem Zeitpunkt für irrelevant-amüsante Auswüchse kalifornischer Science-Fiction, als die IT-Industrie bereits derart astronomische Werbebudgets in das ohnehin schon achtfarbig gedruckte Magazin pumpte, dass dieses auf das Format eines mittleren Telefonbuchs anschwell und zugleich in völlig neue Regionen des Risikojournalismus vorsties: Der Dow Jones, so verkündete die Prawda des digitalen Hippietums 1999, werde bis 2008 die 40.000-Punkte-Grenze durchbrechen, um sich Mitte des 21. Jahrhunderts zwischen 250.000 und 400.000 einzupegeln – und spätestens dann würden sich die Ungerechtigkeiten der Vergangenheit (insbesondere Race, Class und Gender) von selbst erledigen. Gerade angesichts des offensichtlichen Irrsinns einer solchen Deterritorialisierungshypothese reicht es nicht aus, von einer bloss ideologischen Blase zu sprechen, wurden doch auf der Grundlage von Prognosen wie dieser in den USA binnen weniger Jahre die letzten Reste staatlicher Wirtschafts- und Sozialpolitik beseitigt und die materiellen Grundlagen für jene Ordnung geschaffen, in der sich der militärisch-unterhaltungsindustrielle Komplex seine Politik mittlerweile ungestört selber macht. Die europäische Linke, die heute in Hardts und Negris Abgesang auf die starken Staaten und fetten Regierungen einstimmt, bleibt dringend eingeladen, in Thomas Franks "One Market under God" nachzulesen, in welchem Ausmass sich in den USA der Wired-Ära die Ansicht durchgesetzt hat, Demokratie und Bürgerrechte seien Errungenschaften, die von den heroischen Anführern des Freien Marktes permanent gegen die Vertreter von Regierung und Parlament durchgesetzt werden müssten (sic, sic und nochmal sic).

Das spektakuläre Scheitern auch der zweiten Welle der Netzeuphorie – wengleich die Chefrhizomatiker von von America Online, denen heute nicht nur Net-scape und Compuserve, sondern auch die Filmstudios der Warner Brothers, die Labels Columbia und Elektra, die Zeitschriften Time, Life, Fortune und Money sowie der Fernsehsender CNN gehören, zurecht darauf bestehen dürften, Scheitern sehe anders aus – hat sich zwar bis in den letzten Winkel des Globus herumgesprochen, gerade auf Seiten der europäischen Netz-intelligenz aber doch bloss zu Ratlosigkeit geführt. Während eine rapide schrumpfende Zahl rapide wachsender Konzerne im Kampf gegen die angeblichen Verbrechen von Software-, Musik- und Biopiraterie digitale Urheber- und "geistige" Eigentums-

rechte durchsetzt, mit denen sich nicht nur sämtliche nichtkommerziellen Formen des Datenaustauschs präventiv kriminalisieren, sondern auch die natürlichen und sozialen Ressourcen ganzer Kontinente enteignen lassen, und zugleich amerikanische wie europäische Regierungsfirmen die technischen Standards einer elektronischen Sicherheitsarchitektur etablieren, neben der die Überwachungsmethoden des 20. Jahrhunderts dilettantisch wirken, fegen die Veteranen der Netzkritik unentgeltlich die entvölkerten Flure der digitalen Shopping Malls und führen in ihrer reich bemessenen Freizeit auf den einschlägigen Mailinglisten ihre tragischen Niederlagen von einst als Farce wieder auf – in diesem Herbst, indem sie die Geschäftsbedingungen des befreundeten New Yorker Netzkunst-Startups Rhizome.org als kasinokapitalistisch dekonstruieren – na pfui, wie geht denn das zusammen, wer hätte das gedacht! Da passt es ins Bild, dass die Zeitschrift Konkret ihren Lesern ausgerechnet Telepolis als Startportal für Netzlinke empfiehlt, was ähnlich viel Sinn macht, als würde De:Bug ihren Abonnenten zum Einstieg in die Kapitalismuskritik das Verbrauchermagazin WiSo ans Herz legen.

Das Internet ist heute auf dem besten Weg, die neuen Formen elektronischer Arbeit und Freizeit restlos miteinander zu vernetzen und computerisierte Freude, Verschwendung, Knappheit, Sklaverei und Paranoia zu einem weltweiten vierundzwanzigstündigen Arbeitstag zusammenzusetzen: zu jenem digitalen Kontinuum, das vielen von uns zumindest spielerisch bereits vertraut ist als die sich vollendende Einheit von Spass und Terror der Neuen Ökonomie. Zur gleichen Zeit wirft die Geschichte ihre leeren Flaschen aus dem Fenster: Das Internet wird nicht deleuzianisch gewesen sein, sondern – read my lips, make no mistake – das erste Massenmedium der Kontrollgesellschaften. Deren Wappentier wird nicht die Schlange gewesen sein, sondern der Linux-Pinguin. Die globale Vernetzung autonomer Produzenten wird kein Rhizom gewesen sein, sondern der Produktionsmodus der vertikalsten Wirtschaftsordnung, die die Welt je gesehen hat. Die Grenze des Kapitalismus wird kein Ort gewesen sein, an dem sich eine hübsche Aussicht auf sein mögliches Jenseits eröffnet, sondern gerade jener Bereich, in dem die herrschenden Verhältnisse am härtesten um ihr Fortdauern kämpfen. Und eine Linke, die Morpheus für einen Filmhelden und PHP für ein Verschlüsselungsverfahren hält (und auch ansonsten glaubt, ihr gemeinsamer Boden bestünde aus geteilten Meinungen statt aus geteilten Methoden) wird selbst, wenn sie den mittleren Deleuze endlich mal durch den späteren ersetzt haben wird, keine Linke gewesen sein, sondern bloss eine Rechte unter vielen.



Verwirrspiel um den Echelon-Lauschposten in Bad Aibling

von Stefan Krecher

In der letzten Ausgabe der Datenschleuder berichteten wir von der bevorstehenden Schließung der Abhörstation in Bad Aibling – Ende Oktober verkündete dann das US-Verteidigungsministerium, daß in Bayern, erstmal bis zum Jahre 2004, weitergelauscht wird. Die Begründung mutet etwas fadenscheinig an: im Wesentlichen scheint man sich auf die veränderte sicherheitspolitische Lage zu berufen.

Das hin und her um Bad Aibling ist schon fast grotesk, keiner kann genau sagen, was dort passiert und wer belauscht wird. Vor ein paar Monaten wurde behauptet, das die Kapazität im englischen Mega-Ohr in Menwith Hill den Standort in Bad Aiblingen überflüssig mache, und plötzlich ist der deutsche Echelon-Ableger so wichtig.

Aber halten wir uns erstmal ein paar Fakten und eine grobe Timeline vor Augen:

Seit dem Ende des zweiten Weltkrieges wird in Bad Aiblingen von amerikanischen Militärs und Geheimdiensten (in wechselnden Konstellationen) eine Abhörstation betrieben. Diese Abhörstation ist Teil eines globalen Netzwerkes, dessen Grundlage das "UK-USA Security Agreement" (UKUSA) ist, und dem sich später noch Australien, Kanada und Neuseeland anschließen. Deutschland als Nato-Partner hat auf die auspionierten Daten lediglich Zugriff als "Drittverwerter" und befindet sich in einer ständigen "Bettelrolle".

Die rechtliche Grundlage für die lauschenden Amerikaner in Bad Aibling ist das Nato-Truppenstatut, welches militärische Aufklärung erlaubt und ihnen quasi Hoheitsrechte auf dem Gelände zugesteht. Eine Begehung durch deutsche Behörden ist eingeschränkt möglich, beschränkt sich dann aber nur auf nicht sicherheits-/ geheimhaltungsrelevante Bereiche ...

Interessanterweise taucht erst im Januar 2000 ein Dokument der "Air Intelligence Agency" aus dem Jahr 1995 auf, aus dem über Umwege abgeleitet werden kann, das Bad Aibling eine "Echelon Unit" ist und gibt den Spekulationen um das sagenumwobene Echelon-System neuen Auftrieb.

Im Juli des selben Jahres wird schließlich vom europäischen Parlament ein Untersuchungsausschuß eingesetzt. Stimmen werden laut, die vermuten, daß die Amerikaner das Echelon-System auch zur Wirtschafts- und Industriespionage nutzen.

Im November erfährt die Presse, daß die USA Gelder bereitstellen wollen, um den Horchposten Bad Aibling weiter auszubauen.

Im ersten Quartal 2001 werden die Spekulationen um Echelon und Bad Aibling immer wilder, hinzukommt, das erste Erkenntnisse des Untersuchungsausschusses die Öffentlichkeit erreichen. Es werden mehrere Klagen abgewiesen, in denen die Bundesregierung bezichtigt wird ein Abhörsystem u.a. zur Wirtschaftsspionage zu dulden. Begründungen für die abgewiesenen Klagen sind Mangel an Beweisen und die Versicherung der USA, das in Bad Aibling ausschließlich militärisch aufgeklärt würde. Eine nichtmilitärische Nutzung wäre nicht vorschriftsgemäß und ist somit ja auszuschließen – so der Standpunkt der Staatsanwaltschaften.



Im Mai stellt der Untersuchungsausschuss bei einer Geländebegehung fest, daß alle Antennen nach Osteuropa ausgerichtet sind.

Später scheinen sich Beweise für Wirtschaftsspionage zu häufen, der Ausschuss kommt zu dem Schluss, das evtl. Verstöße gegen die europäische Menschenrechtskonvention vorliegen.

Am 31.5. schließlich wird bekanntgegeben, das die Abhörstation Bad Aibling geschlossen werden soll.

Am 3.7. wird der Echelon-Abschlussbericht vom Untersuchungsausschuss verabschiedet und am 5.9. vom europäischen Parlament ebenso.

Der Abschlussbericht weist unter anderem darauf hin, daß das Echelon-System durchaus geeignet ist, Wirtschaftsspionage zu betreiben. Namentlich werden Deutschland und England dazu aufgefordert, US-Überwachungsaktivitäten auf ihrem Territorium davon abhängig zu machen, ob diese gegen die europäische Menschenrechtscharta verstossen.

Für die Bundesrepublik besteht also zunächst kein Handlungsbedarf, da man noch davon ausgeht, das Bad Aibling geschlossen wird.

Am 11.9. verändert sich die Lage radikal – als Folge der Terroranschläge in den USA wird den US-Geheimdiensten vorgeworfen versagt zu haben. Die USA befinden sich im Zugzwang und greifen zunächst einmal Afghanistan an.

Nachdem im Oktober dann der deutsche Bundeskanzler per cron-job unaufhörlich seine uneingeschränkte Solidarität zu den USA verkündet, gibt ein Sprecher des US-Verteidigungsministeriums bekannt, das in Bad Aibling weitergelauscht werden soll.

Was ist da nun passiert? Eine mögliches Szenario könnte so aussehen: die Bundesregierung gerät unter Druck, einmal wegen der Vorwürfe aus der Bevölkerung US-Wirtschaftsspionage und massenhaft unkontrolliertes Abhören zu dulden und zum anderen wegen der Forderungen des Echelon-Abschlussberichtes. Die Bundesregierung versucht an mehr Informationen darüber zu kommen, was wirklich in Bad Aibling passiert und vor allem möchte sie teilhaben an den Abhörergebnissen. Vielleicht wird sogar damit gedroht, das Nato-Truppenstatut enger auszulegen und einer nichtmilitärischen Nutzung durch u.a. Geländebegehung auf die Schliche zu kommen. Laut Untersuchungsausschuss gibt es ja angeblich auch Beweise für die nichtmilitärische Nutzung.

Da die US-Regierung nicht gewillt ist die ersehnten Informationen zu teilen und unter Umständen weitere Enthüllungen befürchtet, zieht sie die Lauscher aus Bad Aibling ab. Seit dem 11.9. herrscht die Situation vor, das den Amerikanern schlecht etwas abgeschlagen werden kann, was diese natürlich ausnutzen und bekannt geben, weiter in Bad Aibling Stellung zu halten.

Wenn sie, wie sie immer behaupten, nur militärische Aufklärung betreiben, hätten sie den Standort Bad Aibling gar nicht erst aufzugeben brauchen – wer gibt schon gerne "quasi Hoheitsgebiet" freiwillig ab? Es liegt doch auf der Hand, das hier auch andere, als militärische Interessen im Spiel sind. Auch die Vorwürfe des Untersuchungsausschusses bzgl. des Verstoßes gegen die EU-Menschenrechtskonvention stehen noch im Raum.

Eine Klärung ist aber ersteinmal nicht in Sicht.



Jeder browst jeden

von wicked

Der 5. Internationale Browserday fand in Berlin unter dem Motto "Mobile Minded" statt. Dreißig Projekte zum Thema "Mobile Browsing" wurden in jeweils 3 Minuten vorgestellt.

Die vorgestellten Konzepte hatten dabei kaum noch was mit traditionellen Webbrowsern zu tun, es ging dabei vielmehr darum Leute und Maschinen sich gegenseitig browsen zu lassen.

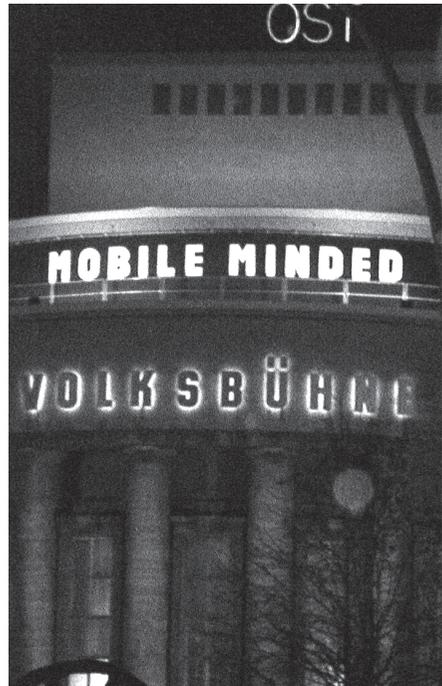
So sollen Geräte sich fremder Personen untereinander ueber Bluetooth oder GSM austauschen, um ihre Besitzer zu verkuppeln, Musik miteinander auszutauschen oder sogar eine eigene Gemeinschaft aufzubauen.

Auch zur Navigation in der realen Welt sollen sich mobile Geräte einsetzen lassen, um diese bei Bedarf an individuelle Vorlieben anzupassen. Der Schutz der Privatsphaere der Benutzer nimmt bei den meisten vorgestellten Konzepten einen recht niedrigen Stellenwert ein, der Wunsch nach möglichst umfassenden Datenaustausch scheint größer zu sein.

Die Zuschauer schienen nicht so technikgläubig zu sein, der Publikumspreis ging an eine Lowtech Variante des mobilen browsens, dem "Instant Mobile Offline Networking Frame" [1], ein Browserfenster zum ausdrucken. Die Jury entschied sich fuer "datenamort" [2], ein Projekt das sich mit der integration von Webinterfaces und Architektur beschäftigt.

[1] <http://www.imon.de>

[2] <http://www.datenamort.de>



BESTELLFETZEN

Bestellungen, Mitgliedsanträge und Adressänderungen bitte senden an:

CCC e.V., Lokstedter Weg 72, D-20251 Hamburg

Adressänderungen und Rückfragen auch per E-Mail an: office@ccc.de

- Satzung + Mitgliedsantrag
€ 2,60
- Datenschleuder-Abonnement, 8 Ausgaben
Normalpreis € 32,00
Ermäßigter Preis € 16,00
Gewerblicher Preis € 50,00 (Wir schicken eine Rechnung)
- Alte Ausgaben der Datenschleuder auf Anfrage
- Chaos CD blue, alles zwischen 1982 und 1999
€ 23 + € 2,60 Portopauschale

Die Kohle

- liegt als Verrechnungsscheck bei
- wurde überwiesen am _____.____.____ an
Chaos Computer Club e.V., Konto 59 90 90-201
Postbank Hamburg, BLZ 200 100 20

Name: _____

Strasse: _____

PLZ, Ort: _____

Tel., Fax: _____

E-Mail: _____

Ort, Datum: _____

Unterschrift: _____



hacking is not a crime

27./28./29.12.2001 / BERLIN - GERMANY