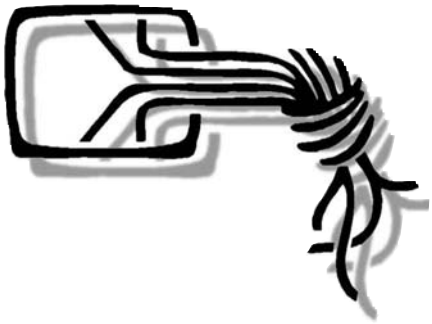
# Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club e.V.




- ActiveX bedroht die Welt
- Homebanking
- Wirtschaftsspionage & Kryptoverbot
- CCC '96 Rückblick

ISSN 0930-1045
März 1997, DM 5,00
Postvertriebsstück C11301F

#58

# Adressen


## Impressum

Die Datenschleuder Nr. 58
Quartal I, März 1997

**Herausgeber:**
Chaos Computer Club e.V.
Schwenckestrasse 85
D-20255 Hamburg
Tel. 040 - 401 801 - 0
Fax. 040 - 491 76 89

**Redaktion: ds@ccc.de,**
Redaktion Datenschleuder
Neue Schönhauser Str. 20
D-10178 Berlin
Tel. 030 - 283 54 87 2
Fax. 030 - 283 54 87 8

**Druck:**
St. Pauli Druckerei, Hamburg

**ViSdP**: Andy Müller-Maguhn
**Mitarbeiter dieser Ausgabe:**
Andy-Müller Maguhn (andy@ccc.de), Steffen Peter (Wau Holland (wau@ccc.de), Frank Rieger (frank@ccc.de), Tim Pritlove (tim@ccc.de), Lutz Donnerhacke (lutz@ccc.de)




**Hamburg:** Treff jeden Dienstag um 20 Uhr in den Clubräumen oder im griechischen Restaurant gegenüber. Schwenckestraße 85, 20255 Hamburg. U-Bahn Osterstraße. Achtung! Neue Rufnummer (040) 401801-0, Fax (040) 4917689, mail: ccchh@ccc.de, http://www.ccc.de

**Berlin:** Treff jeden Dienstag ab ungefähr 20 Uhr in den Clubräumen, Neue Schönhauser Str. 20, 10178 Berlin, im Vorderhaus ganz oben. ÖPnV: Alexanderplatz oder Hackescher Markt. Tel. (030) 28354870, Fax (030) 28354878, cccbln@ccc.de. http://berlin.ccc.de, Chaosradio auf Fritz i.d.R. am letzten Mittwoch im Monat von 22.00-01.00 Uhr.

**Bielefeld:** FoeBud e.V., Treff jeden Dienstag um 19:30 im Cafe Durst in der Heeperstr. 64. Monatliche „Public Domain" Veranstaltung, siehe Mailbox. Briefpost: Foebud e.V., Marktstr. 18, D-33602 Bielefeld, Fax. (0521) 61172, Mailbox (0521) 68000 und Telefon-Hotline Mo-Fr 17-19 Uhr (0521) 175254. Mail zentrale@bionic.zerberus.de

**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, mail: ccc@ews.on-luebeck.de, http://www.on-lübeck.de/bfischer/ccc.html

**Ulm:** Treff jeden Montag um 19 Uhr im Cafe Einstein an der Uni Ulm. Kontakt: frank.kargl@rz.uni-ulm.de
**Stuttgart:** Sücrates - Stuttgarter Computerunde, Kontakt: T. Schuster, Im Feuerhaupt 19, D-70794 Filderstadt, norman@delos.stgt.sub.org
**Frankfurt:** da tut sich auch was, auch wenn es noch keinen Treff in der wirklichen Welt gibt - siehe http://www.rz.uni-frankfurt.de/~katsemi
**Mainz:** demnächst in diesem Theater

**Österreich:** Engagierte ComputerexpertInnen, Postfach 168, A-1015 Wien
**USA:** 2600 (Zeitschrift) mit diversen Treffs an diversen Standorten. Abopreise Overseas: 30$ individual, $65 corporate, Back issues available at $30 per year overseas. Briefpost: 2600, Subscribtion Dept., P.O. Box 752, Middle Island, NY 11953-0752, Tel. +1-516-751-2600, Fax. +1-516-474-2677, http://www.2600.com

## Editorial

Die Arbeit für den Chaos Computer Club kann manchmal ganz schön nerven. Und eine Menge Spaß machen. In letzter Zeit hat es ganz schön genervt und eine Menge Spaß gemacht. Ergebnis: die erste ChaosCD-Beta ist erhältlich für alle Mitglieder und Microsoft dreht am Rad.

Der Patzer, den sich Microsoft mit Ihrer „Internet-Technologie“ ActiveX geleistet hat, zeigt mal wieder aufs feinste wobei es bei diesem ganzen Internationalen Kindergeburtstag namens Internet eigentlich geht: Marktanteile.

Und dafür wird dem Computerbenutzer und -abhängigen schon einiges zugemutet. Waren Viren vor ein paar Jahren noch ein dickes Thema werden Makro-Viren die aus Textdateien gekrochen kommen schon wie normal hingenommen. Getan dagegen wird recht wenig. Abgesehen von ein paar Utility-Herstellern, die sich an den Viren einen goldenen Bauchnabel verdienen.

Mit ActiveX wird dem Computerbenutzer mittlerweile zugemutet, Programme ohne jede inhaltliche Prüfung direkt auf seine allerheiligste Festplatte loszulassen. Der sogenannte „Sicherheitsmechanismus“ in ActiveX ist keiner, taugt auch sonst wenig und mag als früheste Technologie-Beta aller Zeiten in die Geschichte eingehen: „Alle kommerziellen Herausgeber als vertrauenswürdig ansehen“ ist eine der fadenscheinigen Optionen, mit der vertrauenswürdige Kunde seine Computerumgebung konfigurieren kann. Lächerlich!

All das bestätigt nur Microsofts maßlos verzerrte Sicht der Welt. An die Konsequenzen, die ActiveX für seine Kunden hat, scheint Microsoft nicht gedacht zu haben. Die Firma aus Redmond scheint zwar gut zu wissen, wohin heute alle gehen wollen, aber an das Morgen denkt Bill Gates III. anscheinen weniger als es sein biographisches Pamphlet „Der Weg nach vorn“ vermuten ließ.

Also merke: traue keinem Internet-Applet und schon gar nicht allen kommerziellen Herausgebern.

Frohe Ostern
Die Datenschleuder-Redaktion
März 1997

## Index

# Kurzmeldungen

## Falsche Nummern

Aufgrund eines technischen Defektes wurden im amerikanischen SkyTel Funkruf-Netz an mehr als 100000 Kunden falsche Rückruf-Nachrichten gesandt. Das Problem verschlimmerte sich, als einige gewissenhafte Teilnehmer die Nachricht beantworteten und ihre derzeitigen Telefonnummern hinterließen, so daß derjenige, der ihnen die Funkruf-Nachricht geschickt hatte, sie dort erreichen konnte.

Als Folge kam es zu einer 26 Minuten dauernden schwerwiegenden überlastung des Telefonnetzes, da nun Tausende Sky-Tel-Kunden versuchten, diese Nummern zu wählen. Anscheinend hatte das ganze Unglück seinen Anfang genommen, als ein Kunde, der eine neue PIN-Nummer („personal identification number“) angefordert hatte, versehentlich eine geheime PIN-Nummer erhielt, die das Unternehmen normalerweise dazu benutzt, Informationen ihres Dow Jones-Nachrichtendienstes an etwa 100000 Abonnenten zu senden. Die siebenstellige PIN-Nummer, die wie eine Telefonnummer aussieht, wurde dann an alle Dow Jones-Abonnenten übertragen, von denen viele die Nummer als örtliche Telefonnummer ansahen und anzuwählen versuchten. Andere erkannten die Nummer als PIN-Nummer und riefen SkyTel an, um die tatsächliche Telefonnummer des vermeintlichen „Anrufers“ zu erhalten, und verstopften so die Leitungen zu SkyTel. „Zum ersten Mal in der Geschichte unseres bundesweiten Rufdienstes hatten wir eine Unregelmäßigkeit in der Datenbank, die die fehlerhaften Funkmeldungen an unsere Kunden verursachte,“ sagte ein Sprecher von SkyTels Muttergesellschaft MTel, die sich für den Vorfall entschuldigte.

Zitiert aus Wall Street Journal, 10. Januar 1997
frank@ccc.de

## EU plant Umsatzsteuer auf Telekommunikationsdienste

Die Europäische Union plant die Einführung einer Regelung, die es den Mitgliedsländern erlaubt, Umsatzsteuern auf sämtliche Telekommunikationsdienste einzuführen. Dies betrifft auch telefonische Rückruf-Systeme, die entwickelt wurden, um die hohen europäischen Telefongebühren für Auslandsgespräche zu umgehen, indem Europäer einen Rückrufservice in Amerika anrufen.

Der Rückrufservice beendet das Gespräch sofort, ruft zu den wesentlich niedrigeren amerikanischen Telefongebühren zurück und verbindet dann den europäischen Anrufer mit der ursprünglich gewünschten Nummer. Für amerikanische Unternehmen könnte die neue Regelung theoretisch auch bedeuten, daß sie für Waren, die sie über das Internet an europäische Kunden verkaufen, Umsatzsteuer abführen müssen. In manchen EU-Mitgliedsländern beträgt die Umsatzsteuer über 20 Prozent.

New York Times, 11. Januar 1997
frank@ccc.de

## Programmierer bekennt Betrug an AOL

Eine ehemaliger Informatikstudent der Universität Yale hat sich schuldig bekannt, America Online (AOL) betrogen zu haben, und erwartet nun die Höchststrafe von fünf Jahren Gefängnis, 250.000 US-Dollar Geldstrafe und Schadensersatz an AOL,

deren Service ohne Bezahlung in Anspruch genommen wurde. AOL schätzt den Verlust auf 40000 bis 70000 US-Dollar an Service-Gebühren, da der Student sein Computerprogramm, das er „AOL4FREE“ („AOL für umsonst“) nannte, an Hunderte von Computerbenutzern verteilt hatte.

Zitiert aus UPI 9. Jan 1997
frank@ccc.de

## Internet-Streitigkeiten

Network Solutions Inc., die autorisierte Einnahmestelle für Gebühren, die für Internet-Adressen bezahlt werden müssen, berichtet, daß noch ungefähr 10 Millionen der 20,7 Millionen US-Dollar ausstehen, die gemäß der Anzahl registrierter Adressen auf dem Konto sein müßten, seit die Gebührenerhebung 1995 erstmalig eingeführt wurde. Zum Teil gehen die ausstehenden Zahlungen auf „Spekulanten und Wiederverkäufer zurück, die nicht die Absicht haben zu zahlen,“ sagte ein Sprecher der National Science Foundation (NSF), einer amerikanischen Bundesbehörde, die Network Solutions Inc. mit der Gebühreneinnahme beauftragt hat und die deren Arbeit überwacht. 30 Prozent des eingenommenen Geldes ist für die „Erhaltung und Verbesserung“ der „intellektuellen Infrastruktur“ des Internet vorgesehen, **aber bisher wurde noch kein Geld ausgegeben.**

„Meine Meinung ist, je eher das Geld für die Verbesserung des Internet ausgegeben wird, um so besser,“ sagte der Präsident der Internet Society. Währenddessen hat sich ein Chemieprofessor an der Virginia Tech für die öffentliche Bekanntgabe der Schuldner ausgesprochen, zu deren Lasten die fehlenden 10,7 Millionen US-Dollar gehen: „Meiner Meinung nach hat sich die NSF mit der Gebührenerhebung übernommen. Das klügste wäre es, die Sache auf sich beruhen zu lassen oder wirkliche Maßnahmen zu ergreifen.“

Zitiert aus Washington Post, 11. Januar 1997
frank@ccc.de

## Gateway 2000 Opfer einer Porno-Sabotage


Ein Video, das von Gateway 2000 Inc. verteilt wurde, um für ihren neuen PC mit Grossbildschirm zu werben, der Fernseher, Kabeltuner und Stereoverstärker in sich vereint, enthielt 30 Sekunden pornographischer Szenen. Das Unternehmen war daher gezwungen, die 20000 verteilten Kopien des Bandes wieder zurückzurufen. Ein leitender Mitarbeiter des Unternehmens sagte, daß es sich hierbei um Sabotage durch einen verärgerten Angestellten handele. Man sei sich aber nicht sicher, ob Gateway 2000 selbst oder die Video-Firma, die das Band produziert hat, das Ziel der Sabotage gewesen sei.

Wall Street Journal, 14. Januar 1997
frank@ccc.de

## Bahnerpresser wollte Millionen mit gestohlenen Kreditkarten kassieren

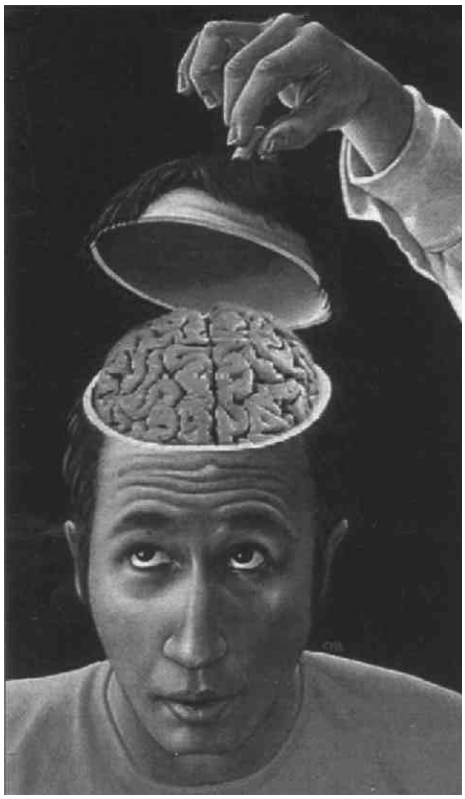
Hamburg - Mit einem besonderen Dreh wollte ein Bahnerpresser an die von ihm geforderten Millionen kommen. Nach Informationen von DPA hatte der Unbekannte in Briefen an die Polizei gefordert, zwei in Leipzig gestohlene und später gesperrte Kreditkarten

# Kurzmeldungen

für das Abheben der Millionen freizuschalten. Nach Angaben der betroffenen Barclay-Bank ist das jedoch technisch nicht möglich. Eine einmal gesperrte Kredikarte kann demnach nicht wieder freigeschaltet werden. Zudem können mit den gestohlenen Kreditkarten höchstens 1.000 Mark pro Tag abgehoben werden.

Ohnehin wär er mit den Dingern nicht weit gekommen, von wegen online-POS Teminals und so...

Zitiert aus dpa 24 Jan 97
andy@ccc.de



## Korrektur zu „Ruhe vor dem Telefon“ in DS 57

Die Funktion „Ruhe vor dem Telefon“ (s. Nr. 57) wurde wieder abgeschaltet, bevor die Datenschleuder erhältlich war. Die eigentliche Funktion von *000#, *888# und *555# gehörten zu dem geplanten Dienst „Anrufbeantworter im Netz“, der Mitte 97 aktiviert werden sollte. Sie stellten im Prinzip eine Umleitung auf diesen (nicht vorhandenen) Anrufbeantworter dar.

redbaron@ccc.de

## Lauschangriff: CSU als verfassungsfeindlich verbieten?

Bonn - Die CSU besteht darauf, gemeinsam mit der Einführung des sogenannten großen Lauschangriffs auch die Möglichkeit zur Videoüberwachung von Wohnungen zu schaffen. Diese Forderung, die vom Bonner Koalitionspartner FDP bislang strikt abgelehnt wird, ist Teil eines zwölf Punkte umfassenden Thesenpapiers zur Innen- und Rechtspolitik, das die Bonner CSU-Landesgruppe auf ihrer Klausurtagung in Wildbad Kreuth diskutieren will.

In dem Papier, das der Deutschen Presse-Agentur (dpa) vorlag, werden im Zuge einer verbesserten Kriminalitätsbekämpfung lückenlose Kontrollmöglichkeiten für alle privaten Telekommunikationsnetze verlangt. Die CSU-Innenpolitiker Norbert Geis und Wolfgang Zeitelmann als Autoren sprechen sich außerdem dafür aus, bundesweit eine sogenannte Schleier-Fahndung einzuführen. Solche gezielten, verdachtsunabhängigen Personenkontrollen auf den Straßen hätten sich in Bayern vor allem bei der Suche nach untergetauchten Schleppern und illegal eingewanderten Ausländern bewährt.

[...] Bei der Reform des Strafgesetzbuchs müsse das bisher bestehende Ungleichgewicht, das bestimmte Eigentumsdelikte härter bestrafe als Gewaltdelikte, beseitigt werden. Stärker berücksichtigt werden müsse künftig auch der Schaden, den die Täter anrichten. Dies gelte beispielsweise für die «systematische bandenmäßig organisierte» Zerstörung von gentechnologischen Versuchsfeldern. Strafbefehle wegen

Sachbeschädigung seien für «solche ideologisch motivierten» Täter keine Abschreckung.

Zitiert aus dpa 5. Jan 97
andy@ccc.de

## 1984 In 1996?

While the PGP software helps keep outsiders from tracking your users' Internet habits, another new program can help you track those habits yourself. LittleBrother, a software package from Kansmen Corp., lets administrators track where employees go on the Internet, how long they stay and what they download. LittleBrother is being pitched as a way of helping network managers reduce „wasted time" by „slackers" in the organization. Administrators can use the software to analyze Internet usage, limit unproductive activity and block sites not related to work. And because LittleBrother lets users do their own policing of network usage, it reduces the need for Internet censorship, said Kan Ng, president of Kansmen, Milpitas, Calif. „Now, each business can decide which sites are productive or unproductive and limit access appropriately, which reduces the need for government interference on the Internet," he said. But even Kansmen conceded that all this technology is a bit Orwellian. The press release for the product reads: „Twelve years after 1984, Kansmen Corp. has introduced its LittleBrother software, which takes the job of monitoring cyberspace away from Big Brother and puts it into the hands of the public."

Quelle: Communications Week, December 16, 1996

## Links illegal?

## Nachricht vom 10.01.97 weitergeleitet
## Ursprung : WAU@CCC.DE
## Ersteller: 100655.2414@compuserve.com

Hallo,

Seit ein paar Tagen ist es amtlich. Fuer Links im Netz auf Seiten, die der deutschen Justiz nicht passen, wird mensch strafrechtlich verfolgt. Nach der Zensur meiner Seiten bei Compuserve, steht ein Verfahren in dieser Sache an.

Weitere Infos unter
http://yi.com/home/MarquardtAngela/
<case sensitive!!>

Viel Freude
Angela Marquardt [PDS]

## UK - Labour Party Web Hack Starts To Unravel

LONDON, ENGLAND, 1996 DEC 17 (NB) via Individual Inc. — By Steve Gold. Police investigating the systematic hack of the Labour Party World Wide Web site, which was hacked on three separate occasions last week, have started the process of tracing down the hacker, Newsbytes has learned.

As reported last week by Newsbytes, during the first raid, which occurred 12 days ago, the Labour Party Web site hacker changed the title „Road to the Manifesto" to „Road to Nowhere." He also tinkered with links to other sites on the Web so they read „The Labour Party sex shop," and transferred visitors to a series of pages carrying pornography.

# Kurzmeldungen

Despite Labour sealing administrator access to the Web site at http://www.labour.co.uk , the hacker, who had a US accent, regained access and almost rewrote the site, adding images of Labour head Tony Blair taken from the Spitting Image comedy puppet series, under the banner headline of „Hacked Labour: Same Politicians, Same Lies.“


The hacker also re-routed Web links which were supposed to detail information on the various personalities within the Labour party to information on the puppets on Jim Henson's Muppet Show, on the Henson Web site in the US.

Newsbytes notes that the running of the site is contracted out to two companies, On-line Publishing, which maintains the pages, and Poptel, which provides the Web space on its servers. Both companies have said they are investigating how the hacker gained access to the pages.

Newsbytes has discovered that BT has traced the first hacker call of Saturday, December 7, to an Internet cafe in Manchester, with the call time logged at 5am. Curiously, the cafe was shut at the time, but Newsbytes notes that there was an all-night „2600“ hacker party going on in Manchester at the time, forcing investigators to the conclusion that the hack may have been part of a demonstration for the hackers.

So far, neither the police nor the Labour party will comment on these revelations, which were published in the „Londoner's Diary“ of the London Evening Standard.

Newsbytes has discovered, however, that at least one person attending the 2600 hacker party i under investigation by the London Fraud Squad.

(19961217/Press Contact: Labour Party, tel +44-171-701-1234, fax +44-171-234-3300/Reported By Newsbytes News Network: http://www.newsbytes.com)

## US-Forscher warnen vor neuer Internet-Sicherheitslücke

München (ots) - Ein Programmierer-Team der US-Universität Princeton hat jetzt eine neue Sicherheitslücke im Internet entdeckt, gegen die bisher keine geeigneten Abwehrmaßnahmen bekannt sind. Wie die „Computerwoche“ in ihrer neuen Ausgabe berichtet, handelt es sich bei der neuen Internet-Attacke um das sogenannte „Web-Spoofing“. Dabei schaltet der Hacker seinen Server zwischen das eigentliche Zielsystem und den Rechner des Anwenders und täuscht auf seinem System eine „echte Kopie“ der Daten vor, die er komplett kontrollieren und für seine Belange modifizieren kann.

Danach kann er nach Belieben vom arglosen Benutzer verschickte Informationen abfangen oder sogar manipulieren, in dem der Hacker die Uniform Resource Locators (URLs) auf dem ursprünglichen Ziel so verändert, daß sie auf die Kopien in seinem System verweisen. Eine weitere Möglichkeit des Hackers besteht laut „Computerwoche“ darin, Links in das falsche Web auf vielfrequentierten Internet-Seiten zu plazieren oder die Links im Usenet, per E-Mail im Index von Suchmaschinen zu publizieren.

Besonders gefährlich wird das „Web-Spoofing“, wenn sich der Hacker auf diese Weise Paßwörter oder Kreditkartennummern von Benutzern beschafft. Das funktioniert sogar, wenn der Benutzer eine vermeintlich sichere Verbindung über den Secure Sockets Layer (SSL) gewählt hat. Diese besteht auch tatsächlich, allerdings zum Server des Hackers. Da die meisten Web-Transaktionen über HTML-Formulare laufen, wie etwa bei einer Warenbestellung, kann der Hacker diese Bestelldaten für seine Zwecke manipulieren und sich so auf Kosten des Benutzers Waren bestellen.

Das US-Forscher-Team um Edward Felten empfiehlt als Gegenmaßnahme des „Web-Spoofings“ die ständige Kontrolle der Status- und Adresszeile des Web-Browsers. Vor allem aber sollten die Internet-Anwender Javascript, Active X und Java in ihrem Browser deaktivieren, auch wenn dadurch einiges an Funktionalität verloren geht. Bei Bedarf könnten die Zusatzfunktionen auf bestimmten vertrauenswürdigen Seiten zeitlich begrenzt wieder aktiviert werden.

(Quelle: Spiegel Online, neulich)

## WWW-Seiten zu Polizei und Überwachung - Update

Liebe Freunde und Interessierte,

ich moechte Euch mit dieser e-mail darueber informieren, dass ich meine WWW-Seiten zu ‘Polizei und Ueberwachung’ im Rahmen einer ‘Generalueberholung’ meines WWW-Angebots komplett ueberarbeitet habe.

http://www.rrz.uni-hamburg.de/kr-p1/polsurv.htm

[...] nogala@rrz.uni-hamburg.de

## Rinderwahn online

[...] Zusätzlich findet beim Dezernat 34 des Polizeipräsidiums München eine deliktsübergreifende anlaßunabhängige Auswertung elektronischer Medien statt.

Dieses Konzept wird durch die Tätigkeit des Sachgebiets 522 beim Bayerischen Landeskriminalamt ergänzt, das ebenfalls anlaßunabhängige Recherchen in Datennetzen durchführt. Darüber hinaus fungiert das Landeskriminalamt in Bayern für diesen Kriminalbereich als Koordinierungsstelle. „Seit Beginn des Pilotprojekts waren die bayerischen Netzpatrouillen insgesamt über 5.000 Stunden im Internet. Das zeigt wie personal- und zeitaufwendig Ermittlungen im Internet sich gestalten“, so Regensburger. Das Verhdltnis von durchgeführten Recherchen zu Treffern beträgt etwa 70 zu 30, das heißt, daß im Durchschnitt jede dritte Recherche zu einem Treffer führt.

http://www.polizei.bayern.de/aktuell/index.htm

rowue@digitalis.org


# ActiveX: Unsicherheit einer Software-Philosophie

Eher am Rande des 13. Chaos Communication Congress im Dezember 1996 wurde die Idee entwickelt, die Unsicherheit von ActiveX durch Fernsteuerung einer Homebanking-Software zu demonstrieren.

Der letztlich entstandene Fernsehbeitrag des MDR bei „PlusMinus“ benannte das Problem jedoch eher nicht: anstelle von ActiveX wurde nur die mißbrauchte Homebanking-Software Intuit Quicken gezeigt und benannt. Für den Fernsehbeitrag war ein „Control“ für ActiveX geschrieben, welches die Homebanking-Software quasi fernsteuerte. Während der Benutzer glaubte, eine bunte Web-Seite anzugucken, wurden seiner Transaktionsliste (Sammelüberweisung) ein Überweisungsauftrag hinzugefügt. Auch wenn es wichtig war, eine sensible Applikation zur Demonstration des ActiveX Problems (volle Fernsteuerbarkeit des Computers) auszuwählen und insbesondere die kundenunfreundliche Haftungs- und Beweislage deutlich machen, so war es dann für die Journalisten doch schwierig, zwischen Ursache und Wirkung zu unterscheiden.

Dies nutzte natürlich noch am ehesten Microsoft, die zumindest in Amerika dann auch mit entsprechenden Meldungen den Nebel noch verstärkten um vom eigentlichen Problem, nämlich ActiveX, abzulenken.

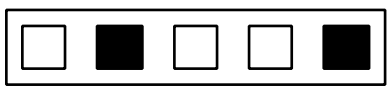
Daher waren wir nach Kräften bemüht, Mißverständnissen und Desinformation entgegenzuwirken. Die Meldungen, die wir hier aus Platzgründen nicht abdrücken können sind im Web (http://www.ccc.de/radioactivex.html bzw. http://www.iks-jena.de/mitarb/lutz/security/activex.html) vollständig mit einer Chronologie der Ereignisse dokumentiert. Auch finden sich dort die Source-Codes und andere Beispiele.

Apropos Mißverständnisse: es möge bitte nicht der Eindruck aufkommen, wir würden jetzt Java oder Homebanking ohne ActiveX auf der Maschine als „sicher“ bezeichnen.

Wir müssen hier zwischen „Bug“ (Java-Implementationen, Interpreter etc) und „Bug by design“ (ActiveX) unterscheiden. Java wird - zumindest vom theoretischen Konzept her - in einer Sicherheitsumgebung („Sandbox“) ausgeführt, die nur eingeschränkten Zugriff auf das System erlaubt. Auch wenn diese mittlerweile aufgeweicht wird und spätestens über Plug-Ins etc. durchlöchert werden kann so gibt es zumindest eine Art von Sicherheitskonzept und -bewußtsein. ActiveX ist unmittelbarer Maschinencode, der alles mit der Maschine anstellen kann, was der (eingeloggte) Benutzer auch kann. Bei nicht-NT Maschinen ist das schonmal pauschal *alles* und bei NT-Maschinen hängt es nur unter anderen von den Rechten des eingeloggten Benutzers ab.

Die „Authentifikationsstruktur“ von ActiveX kann die technische Unsicherheit nicht ausgleichen - sie fügt den „controls“ (was auch immer sie tun) nur ein Zertifikat (Absenderkennung/Echtheit) an. Auch hierzu mehr im Netz. Zur allgemeinen Erheiterung dokumentieren wir hier die Antwort von Fred Cohen auf eine Erklärung des Microsoft-Vizepräsidenten zur Sache. Cohen gilt immerhin als der Autor des ersten Computervirus - und das war Anfang der achtziger Jahren.

Andy Müller-Maguhn, andy@ccc.de



# Re: MS on the CCC ActiveX virus

Date: Fri, 21 Feb 1997 11:46:11 -0800 (PST)
From: fc@ca.sandia.gov (Fred Cohen)
Subject: Re: MS on the CCC ActiveX virus (RISKS-18.83)

Re: SBN Wire: News Flash, Brad Silverberg

> You may have heard reports about a malicious software program created and
> demonstrated recently by the Chaos Computer Club (CCC) in Hamburg, Germany.
> I want to personally assure you that Microsoft(R) Internet Explorer 3.0 has
> the appropriate safeguards to protect against this type of threat. By using
> its default security level (High) that comes pre-set, Internet Explorer 3.0
> will not download and run any "unsigned" control such as the one from the
> CCC.

I appreciate your insightful opinion on this matter, however...
Anyone can get a signature key without authenticating their legitimacy. It's relatively easy to break into a system and take a legitimate key. The default may be changed by the user for one use and remain changed. Other flaws in Explorer may be used to turn that feature on - then look out.

> The CCC demonstrated its malicious executable code running on Microsoft
> Internet Explorer 3.0, though they could just as easily have demonstrated a
> similar attack on any other browser. While it is unfortunate that hackers
> have created this harmful program, it does point out the need for users to
> act cautiously and responsibly on the Internet, just as they do in the
> physical world.

I appreciate your insightful opinion on this matter, however...
This is not accurate. The very nature of ActiveX makes it impossible to operate it securely. Unlike other vendors who make attempts at providing improved protection, ActiveX is a hole waiting to be exploited.

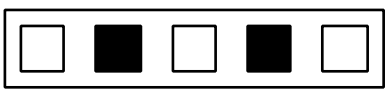
> Malicious code can be written and disguised in many ways - within
> application macros, Java(tm) applets, ActiveX(tm) controls, Navigator
> plug-ins, Macintosh(R) applications and more. For that reason, with
> Internet Explorer 3.0, Microsoft has initiated efforts to protect users
> against these threats. Microsoft Authenticode(tm) in Internet Explorer 3.0
> is the only commercial technology in use today that identifies who published
> executable code you might download from the Internet, and verifies that it
> hasn't been altered since publication.

I appreciate your insightful opinion on this matter, however...
No disguise is needed for malicious ActiveX programs. Any ActiveX program can potentially - either maliciously or by accident or even as a result of configuration differences, cause a system crash, the corruption or destruction of information and/or unlimited leakage and it doesn't depend on some hard-to-find hole in an otherwise secure application. It is a direct result of the methods used by Microsoft, cannot be easily cured with any bug-fix.

> If users choose to change the default security level from High to Medium,
> they still have the opportunity to protect themselves from unsigned code.
> At a Medium setting, prior to downloading and running executable software on
> your computer, Microsoft Internet Explorer presents you with a dialog either
> displaying the publisher's certificate, or informing you that an "unsigned
> control" can be run on your machine. At that point, in either case, you are
> in control and can decide how to proceed.

I appreciate your insightful opinion on this matter, however...
Even if you choose wisely, ActiveX is a hole waiting to be exploited and provides essentially no protection. As the folks at Microsoft





# Re: MS on the CCC ActiveX virus

know well, impediments are easily and commonly removed - and the
use of the display box for popular applications is likely to result in
the question being turned off in favor of easy access.

> As you know, Microsoft is committed to giving users a rich computing
> experience while providing appropriate safeguards. Most useful and
> productive applications need a wide range of system services, and would be
> seriously limited in functionality without access to these services. This
> means that many Java applications will have to go "outside the sandbox" to
> provide users with rich functionality. By signing code, a developer can
> take advantage of these rich services while giving users the authentication
> and integrity safeguards they need. Other firms such as Sun and Netscape
> are following our lead, and have announced that they will also provide code
> signing for Java applets. Microsoft will also be providing an enhanced Java
> security model in the future, giving users and developers flexible levels of
> functionality and security.

I appreciate your insightful opinion on this matter, however...
"...while providing appropriate safeguards" is just not true.
Microsoft has a long history of providing systems with no
protection, and only recently introduced the first system with
even mild protection in it's NT product. Java provides a lot of
functionality within the "sandbox", but I am not an advocate of
Java either. The syle of computing being pushed out to consumers
is inherently risky and must be implemented with substantial controls
if it is to be used safely. But this is not Microsoft's goal.

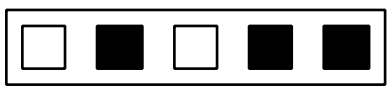
There is nothing wrong with having signatures, but it is no
guarantee either.

> Microsoft takes the threat of malicious code very seriously. It is a
> problem that affects everyone in our industry. This issue is not tied to
> any specific vendor or group of people. All of us that use computers for
> work, education, or just plain fun need to be aware of potential risks and
> use the precautions that can insure we all get the most out of our
> computers. For this reason, we are committed to providing great safeguards
> against these types of threats in Internet Explorer. We expect hackers and
> virus writers to get increasingly sophisticated but we pledge we'll continue
> to keep you and us one step ahead of them.

I appreciate your insightful opinion on this matter, however... Microsoft
still has not addressed Work Macro viruses, PC viruses, Windows
viruses, etc. The claim that "Microsoft takes the threat of
malicious code very seriously" is ludicrous on its face. This is
the same company that has distributed viruses to its customers because
it didn't do adequate checking of its distributions for known viruses.
This is the company whose Windows installation deleted all of the
README files on a system when the user upgraded. This is the same
company that continues to ship software with inadequate protection.
All of this "perception management" doesn't change the fact, and it
shouldn't sway the readers of this letter either.

FC [Fred Cohen can be reached at tel:510-294-2087 fax:510-294-1225]

[NOTE: I usually truncate all but a salient excerpt from included message
text on which a responder is commenting. In this case, it would have
required too much editing effort to delete the interstitiated originals
and still convey the sense of the relevant references. Your cross-reading
effort would also have been much greater. PGN]



# Chaosradio Ticker

## Internet I

Neue Gefahren für Netscape Navigator Anwender unter Windows 95 entstehen schon durch falsche Datumsangaben. Nachrichten eines Anwenders, der das Datum seines PCs irrtümlich auf das Jahr 2096 gesetzt hatte, führten bei den Empfängern, die ihre Mail mit Navigator lasen, zu spontanen Abstürzen. Ob auch andere Jahreszahlen eine Bedrohung für die Systemstabilität darstellen wird noch erforscht.

## Boston

Ein Programmierfehler im vor zwei Jahren neu eingeführten Computersystem der Massachusetts Registry of Motor Vehicles führte jüngst dazu, daß manche Führerscheininhaber ihren neuen Ausweis gleich mehrmals erhielten. Eine Verkehrsteilnehmerin erhielt an einem Tag gleich sechs Kopien der kleinen Plastikkarte. Die Behörde versprach, der Fehler sei gefunden und behoben werden. Na dann, bis zum nächsten Fehler...

## Internet II

Ein Web-Versprechen besonderer Art konnte wieder einmal nicht eingehalten werden. Ein Anbieter versprach, ein besonderer Pornoservice könnte problemlos mit einem herunterzuladenden Programm genutzt werden. Just Click Here. Das Programm allerdings offerierte keinerlei Triple-X Inhalte. Stattdessen warf es das Modem an und wählte unablässig Telefonnummern in Moldawien. AT&T, mit der Frage konfrontiert, ob es die entstandenen Telefongebühren für die Programmopfer erlassen könnte, erwiderte, daß das aus Gründen der Fairness anderer Teilnehmer nicht möglich wäre, die ihre Rechn ja auch zahlen müßten.

## Bogota

Im letzten August entführten die Fuerzas Arm Revolucionarias de Colombia, kurz FARC, eine Marxistisch-Leninistische Guerillagruppe, sech kolumbianische Soldaten. Die kolumbianische Regierung gab daraufhin bekannt, daß sie dies Mal bei den Verhandlungen aus Sicherheitsgrü auf E-Mail umsteigen wollte. Die FARC wiedersprach: sie hatte bereits 2 E-Mails von L erhalten, die sich als die Regierung ausgegeben ten.

## USA

Ein Treffen der ISO / ANSI Standardisierungsgr für die C++ Programmiersprache kam im November 96 nicht zum Arbeiten. Da ein mitgebrachter Text mit Word erstellt wurde un sog. „Concept“ Word Makro-Virus enthielt, inf ten sich innerhalb kurzer Zeit alle anwesenden Laptops. Die Gruppe kam nicht zum Arbeiten, sie sich stundenlang bemühten, den Virus wie loszuwerden.

Die Gruppe fragte sich danach, wie normale Anwender damit Leben könnten, wenn schon Bande von Programmierexperten nicht klar ko Microsoft hat das Problem von Makroviren im noch nicht gelöst.

## Chaosradio Berlin

Live: chaos@orb.de
Redaktion:
chaosradio@berlin.ccc.de
http://berlin.ccc.de/Chaosradio

# Wirtschaftsspionage...

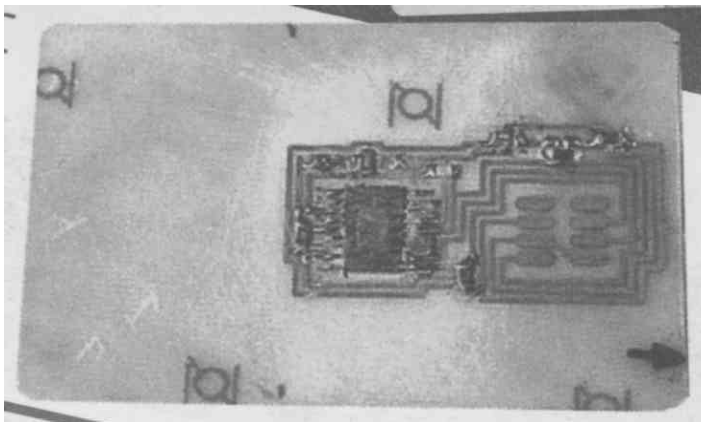
## Nordamerika auf dem Weg zur Weltregierung

Nach Promis, Windows, Clipperchip und Stress für Phil Zimmermann hat sich die nordamerikanische Regierung mal wieder was neues ausgedacht um doch zumindest Zugriff auf *alle* Informationen zu haben. Derzeit wird in verschiedenen Zügen ein globaler Plan umgesetzt. Verschiedene Crypto- & Sicherheitsprodukte & -verfahren werden zunächst einmal von der „Liste der Waffen“ des DOD (department of defense) gestrichen und werden zu genehmigungspflichtigen Angelegenheiten unter der Obhut des Wirtschaftsministeriums (department of commerce).

Wer nun allerdings glaubt, dies sei ein Zeichen von Entspannung und Lockerung täuscht sich gewaltig: das Gegenteil ist der Fall. Wie untenstehende Mail andeutet und vor allem der Gesetzestext explizit benennt wird eine *globale* „key escrow“ Struktur aufgebaut: Schlüssellängen-Beschränkung bzw. Nachschlüsselhinterlegung im Klartext.

Die dazugehörige Propaganda ist die Mär von der „organisierten Kriminalität“ und die Sicherheit gegenüber Gefährlichkeiten im Allgemeinen. Worum es wirklich geht, ist mit einem Wort zu benennen: Wirtschaftsspionage. Mit welcher Dreistigkeit dabei „befreundete“ europäische Staaten als „Partner“ gewonnen werden ist angesichts der Geschichte mit den Gatt-Verhandlungen eigentlich unglaublich: da marschiert der CIA mal eben mit Kenntnis der Hintertür durch eine Firewall, holt sich die Verhandlungspositionen in Ruhe aus dem Rechner und kann entsprechend verhandeln.

Und die EU? Das Untersuchungsergebnis war immerhin so deutlich, daß es durchsickerte und nicht abgestritten werden konnte. Aber eine öffentliche Aufklärung des Vorfalls hat es nicht gegeben. Auch auf Nachfragen von Angehörigen des europäischen Parlaments gab es dazu bislang keine Auskunft.



Problematisch wird das jetzt ganz konkret in diesem unserem Lande: Kanther und das BMI samt Kanzler nahe Personen wurden unlängst als Opfer der Spionage - im offiziellen Sprachgebrauch „zur Kooperation im Kampf gegen die organisierte Kriminalität“ gewonnen. Ob wir es hier mit blöden, gutgläubigen, machtgeilen oder gut-geschmierten zu tun haben ist vom Ergebniss her unerheblich - siehe auch http://www.inka.de/~maya/krypto.html

Und so warten wir es besser nicht ab, bis uns das Kryptogesetz überrollt.

Andy Müller-Maguhn, andy@ccc.de

# und Kryptoverbot

Date: Tue, 31 Dec 1996 19:05:05 -0800

From: Lucky Green <shamrock@netcom.com>

Subject: New US regs ban downloadable data-security software

The new US crypto export regulations control the export of most if not all data-security software. Regardless if the software uses cryptography or not. Many software archives seem to be in violation of the new regs.

[Federal Register: December 30, 1996 (Volume 61, Number 251)]

[makes it illegal to export without a license:]

c.3. ``Software'' designed or modified to protect against malicious computer damage, e.g., viruses;

[For the full text, see http://www.epic.org/crypto/export_controls/interim_regs_12_96.html]

This certainly controls virus checkers, firewalls, and other security software. There are substantial penalties involved in violating the EAR.

The US can assess daily penalties and block all exports of a company's non-violating products. Criminal penalties apply as well. „Export", as defined in the new regs, includes making software available on the web or via ftp.

If you have a virus checker or similar software available for ftp inside the US and the software can be downloaded from outside the US, you are most likely in violation of the new EAR which took effect on 12/30/1996.

If you do not wish to go to prison, you may want to consult an attorney immediately and remove all data security software from your server.

IANAL —Lucky Green <mailto:shamrock@netcom.com

# Termine 1997

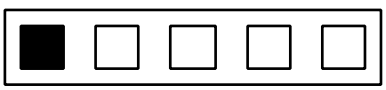
**13.-19.3.97**
CeBIT Hannover
Der Stand des CCC ist in Halle 22, A16.
Am Dienstag, den 18.3. um 16 Uhr Treff auf dem Stand der Telekom in Halle 16, B35.
http://www.ccc.de/CeBIT97.html

**8.8-10.8.97**
HIP '97: Hacking in Progress in Holland
http://www.hip97.nl

**8.8-10.8.97**
HOPE II in New York,
http://www.2600.com

**27.-29.12.97**
14. Chaos Communication Congress
http://www.ccc.de





# Chaos Communication Congress 96

## Firewalls - Aufzucht und Pflege

Referenten: Jan Haul (pirx@ccc.de), Ron Hendrik Fulda (hhf@ccc.de)

Zu Beginn des sehr gut besuchten Workshops (selbst Fußbodenplätze waren bei den ca. 70 Besuchern am Ende ausverkauft) wurden erstmal die vier W-Fragen zu Firewalls gestellt:

Warum? Wie? Was hilft's? Was hilft's nicht ?

Diese sollten dann im Laufe des Workshops geklärt werden. Ron stellte zunächst einmal fest, daß es „Firewalls" als solche nicht gibt, daß zwar Geräte verkauft werden, auf denen außen Firewall draufsteht, die sich aber in Aufbau und Funktion teilweise deutlich voneinander unterscheiden. Was es gibt, sind Firewall-Prinzipien, die umgesetzt werden, aber auch noch miteinander kombiniert werden können.

Warum soll man nun als Betreiber eines Netzes eine Firewall einsetzen? Eine Firewall kontrolliert die Kommunikation zwischen Rechnern des eigenen inneren Netzes mit der Außenwelt, in der Regel dem Internet, jedoch in etlichen Fällen z.B. auch innerhalb des inneren Netzes, z.B. um Daten innerhalb einzelner Abteilungen zu schützen.

Angriffe, die möglicherweise auf ein Netz ausgeübt werden können, sind:

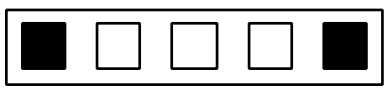
* spoofing = Vortäuschen / "Faken" von IP-Adressen und Source-Route-Hacking sind heute meist nur noch zum „Tarnen" bei Hacking- und Floodingaktionen geeignet. Das Problemdabei ist: Antworten kommen nicht zurück, die Methode ist also nur für „Dialoge" geeignet, wo man weiß, was der Gegenüber antwortet
* denial of service _(System kann nicht mehr benutzt werden)
* Informationsdiebstahl
* Zerstörung von Systemen / Daten; Datenmanipulation
* Kontrolle der Nutzung
* Flooding (Überschwemmen des Systems mit gefakten Paketen, die Systemleistungen zum Empfang verbrauchen) .

Wenn man nun den Einsatz einer Firewall für sinnvoll hält, muß man sich fragen, was man damit erreichen will, sein System „sicher" zu machen. Dafür ist es wichtig zu wissen, wie die Komunikation von einer Firewall gefiltert werden.

Paketfilter:

* Source Address
* Destination Address
* Service (Port)
* Content (Inhalt; theoretisch)
* Masquerrading (Beim Masquerading wird die Real-Adresse durch die eigene Adresse ersetzt und verändert die Portadresse. Die Verbindung wird in einer Tabelle mitprotokolliert, damit die Rückübersetzung der veränderten Adressen möglich ist. Für FTP in der Regel nicht möglich.)

Möglich sind auch Firewalls, die auf dem Application-Layer aufbauen, z.B. durch WWW-Proxy, FTP-Proxy, Telnet Proxy, Socks.



Es muß immer abgewägt werden, wie wichtig die Sicherheit ist und was sie an Aufwand und Kosten mit sich bringt. Man kann mehrere Firewalls hintereinanderschalten, auch in der Praxis werden tatsächlich bis zu 5 Firewalls hintereinandergeschaltet, die die Pakete mit unterschiedlicher Hardware und nach unterschiedlichen Kriterien filtern.

Nach Adressen kann in beiden Richtungen von einer Firewall sehr einfach gefiltert werden, Service(Dienste)-Filterung ist auch gut möglich (z.B. wer darf Send-Mail betreiben, wohin darf Sendmail nicht gehen). Die Kombination von Adreß- und Dienst-Filtern ist schon sehr feingliedrig.

Für den Aufbau von Firewalls lassen sich verschiedene Konzepte finden, von denen die verbreitetsten hier vorgestellt werden:

1. Konzept:

Einsatz von Filtern nach verschiedenen Kategorien, z.B.: nicht mehr als bestimmte Anzahl von Paketen pro Zeit (erhöhter Zugriff), Einschränkungen beim Zeitpunkt des Verbindungsaufbaus (nicht am Wochenende). Die benötigte Hardware ist nicht aufwendig und auch die nötige Programmierung läßt sich einfach erledigen.

2. Konzept:

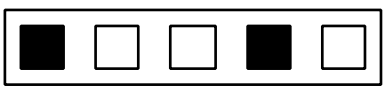
Ein Netzwerkprotokoll verwenden, das über das Internet nicht geroutet wird, z.B. Class-A-Netzwerk (Netzwerkadresse ist nicht erreichbar). Die Adresse wird nach außen durch die Adresse des Firewallrechners, der zwischen Netz und Router geschaltet wird, ersetzt. Dafür muß sich der Firewall-Rechner die Realadressen zu jeder Verbindung merken, für nicht-verbindungsorientierte Protokolle (z.B. UDP, verwendet durch Nameserver, Nichtfunktionieren ist also sinnvoll; NFS, sehr unsichere Architektur, ergo Nichtfunktion gut; oder Real-Audio, was die Netzlast hochtreibt, also auch nicht erwünscht ist) aber nicht geeignet.

Spoofing verbunden mit Flooding läßt sich von außen nicht abwehren. Es ist nur möglich, ein Netz von innen her abzusichern, indem man (z.B. als Provider) nicht Adressen des inneren Netzes nach außen senden läßt. Die Firewall hat hier aber immer noch die Schutzfunktion, daß im Falle des Falles nur die Firewall lahmgelegt wird, eine interne Netz-Kommunikation aber noch möglich ist.

Um eine größtmögliche Sicherheit zu erreichen, sollte der Firewall-Rechner am einfachsten nach der Devise „was nicht erlaubt ist, ist verboten“ verwaltet werden. So hat man die Sicherheit, daß nur die Prozesse ausgeführt werden können, die benötigt werden und auch vorgesehen sind.

Gegen einen Teil von unerwünschten Zugriffen aus dem inneren Netz nach außen kann man sich auch durch Firewall-Proxies schützen. Während normalerweise ein Mailpaket in den Schichten zwei oder drei des 7-Schichtmodells (s. auch Artikel TCP/IP) im Router vom inneren in das äußere Netz gelangt, kann man dies unterbinden und über den Application-Layer (Schichten vier bis sieben) mit wenigen Code-Zeilen einen wirkungsvollen Filter aufbauen, der nicht nur nach den äußeren Paket-Kennungen (Absender, Empfänger, verwendeter Dienste-Port), sondern auch nach Inhalt filtern kann (keine Bilder, kein Real-Audio, kein Java, ausführbare Dateien werden vor dem Weitersenden auf Viren untersucht...). Ein Proxy hat neben den möglichen Filterfunktionen auch noch den Vorteil, daß oft verwendete Anfragen





zwischengespeichert werden und damit nicht über das Netz geholt werden müssen. Gerade im HTTP-Bereich kann so viel unnötige Übertragung gespart werden.

Firewall-Socks arbeiten nach einem ähnlichen Prinzip wie das Masquerading: Pakete werden mit der Socks-Adresse weiterverschickt, dies aber unter Unterstützung der Clients. Hierbei müssen die Clients „socksified“ sein, d.h. die Applications müssen um Socks-Funktionalität erweitert sein. Nicht für alle Clients gibt es Socks-Versionen. Bei OS/2 Warp 4 wird inzwischen die Socks-Unterstützung auf Betriebssystem-Ebene umgesetzt, so daß die Clients es nicht mehr unterstützen müssen.

Will man nun aber nicht ein Netz gegen die Umgebung abschließen, sondern sichere Netze z.B. über Internet miteinander verbinden, kommt man mit Firewalls nicht weiter - hier hilft ein weiteres Protokoll: das PPTP, das Point to Point Tunneling Protocol, mit dem für die Übertragungsstrecke über das Internet die Datenpakete noch einmal

eingepackt werden, diesmal verschlüsselt, und am anderen Ende der Leitung werden sie einfach vom Header befreit und entschlüsselt und erhalten so ihre ursprüngliche Form wieder.

Abschließend darf man den Referenten / Moderatoren für den gelungenen Workshop danken, da teils mit Beispielen aus dem menschlichen Leben eine sehr humorige Stimmung erreicht wurde und trotz der großen Menge an Teilnehmern mit den unterschiedlichsten Wissensständen (vom Anfänger bis zum Vollprofi war wirklich alles vertreten) die Gestaltung von Anfang bis Ende nicht langweilig wurde und jedem sicherlich noch interessantes Wissen vermittelt werden konnte.

* Security in Open Systems (ca. 280 Seiten, Postscript), ftp://ftp.nist.gov/pub/csrc/nistpubs/800-8.ps

* Firewalls (ca. 80 Seiten, Postscript), ftp://ftp.nist.gov/pub/csrc/nistpubs/800-10.ps

Zusammenfassung von
Derk Marko Reckel, Derk.Reckel@link-goe.de

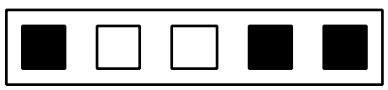
## Keep it simple, keep it fast: IPv6

Referent: Tim Pritlove, tim@ccc.de

„Wenn irgendwas komplizierter ist, als ein Toastbrot, wird es nicht benutzt.“

Wir schreiben das Jahr 1997. Das Routing im Internet basiert auf IP Version 4, die eigentlich Version 1 ist. Jeder Rechner (genauer: jede Schnittstelle) benötigt eine eindeutige Adresse. Diese Adressen werden aus 4 Bytes (=32 bit) zusammengesetzt. Es bestehen ein ganze Reihe von Problemen: Die maximal verfügbaren Adressen reichen demnächst nicht mehr aus, wenn Taschenrechner, Toaster und Fernseher (sowieso) meinen, über IP miteinander verkehren zu müssen.

Darüberhinaus zwickt und zwackt es an noch mehr Stellen, und das im Gegensatz zum zu kleinen Adressraum schon jetzt ganz konkret: Die 32 Bit Adressierung reicht in großen Netzen nicht mehr, die erforderlichen Subnetze zu verwalten. Mit der IP V.4 Adressierung verknüpft ist die Existenz unzähliger verschiedener Routerprotokolle.



Daher rührt auch die Nichtbenutzung vieler Features, die IP V.4 durchaus anbietet. Ein Router, der das machen würde, wäre sehr langsam und nicht kompatibel zu den anderen. Das an sich ist ein Problem, schlimmer ist aber noch, daß praktisch jeder Router auf der Welt Routingtabellen verwalten muß, die seit langer Zeit exonentiell wachsen und inzwischen kaum mehr zu verarbeiten sind. Etwas neues muß her und das heißt dann IP V.6. Viele Gruppen haben an etwas neuem herumgebastelt, IP V.6 stammt aus der Feder der IP Next Generation Gruppe. (***Buchtip)

Und das ist wohl etwas ganz tolles.

Neuer Aufbau der IP-Pakete an sich

Der Grundsätzliche Aufbau eines IP Paketes ist:

Header + Payload

Payload ist sind die eigentlichen Daten, die transportiert werden sollen. Die Länge des Headers kann bei V.4 varieren, was das Handling natürlich erschwert.

In IP V.6 ist ein Header konstant lang, und im Vergleich zu V.4 einfach aufgebaut. 90 Prozent aller Pakete werden mit einem einfachen Header auskommen. Für besondere Anwendungen Extension Headers, die dem Basisheader (im Sinne einer verketteten Liste folgen).

Base Header + Extension Header ( + Extension Header) + Payload

Extension Header sind z.B:

* Sourcerouteheader - Zum Festlegen der Route, die ein Paket nehmen soll. Z.B. ‘Das Paket hier soll über meinen Provider laufen’

* Authentication Header - Authentifizierung aller nachfolgenden Header und der Payload (Signatur)

Neue Adressen

Wie gesagt, jetzt hat eine Adresse 32 Bit. Bei V.6 werden es 128. Das ist doppelt so viel, wie mathematisch betrachtet nötig wäre. Aber wir sind ja lernfähig und planen gleich etwas mehr ein. (Wobei die Adressverlängerung den Adressraum hier exponentiell erweitert und ‘etwas mehr’ stark untertrieben ist.)

Die Adressen sagen dann etwas über den Standort des Empfängers aus, früher war es halt einfach irgendeine Nummer, deren Zuordnung zu realen Maschinen über ausufernde Tabellen lief. Die Adresse enthält dann 5 Informationen: Registry, Provider, Subscriber, Subnet, Interface.

* Die Registry ist eine von mehreren Adressverteilungsautoritäten: IANA, RIPE, INTERNIC, usw.

* Der Provider ist die Organisation, die einem die Leitung gibt.

* Der Subscriber ist der Kunde.

* Subnet, falls der Kunde so groß ist, daß er das braucht. Sollte sich herausstellen, daß eine Firma nicht einfach aus Subnets besteht, sondern auch Subsubnets und so weiter, sind immer noch genug Bits frei, das zu integrieren.

* Interface, das Endgerät. Neu ist hier noch, daß ein Interface, also die z.B. Netzkarte in einem Rechner beliebig viele IP Adresse



haben kann, bisher ging das nicht so einfach.

Die Notation der Adressen ist Hexadezimal mit Doppelpunkten als 2 Byte Trennung. Es treten immer an einer Stelle in der Adresse eine größere Anzahl Nullen auf, die durch zwei aufeinanderfolgende Doppelpunkte repräsentiert und abgekürzt werden. Zum Beispiel:

FEDC:B198::7654:3210

Es fällt ins Auge, daß die letzten 32 Bit für die abwärtskompabilität zu V.4 bestimmt sind. Die Adressen sind großräumig für bestimmte Aufgaben verteilt. Je 1/8 aller Verfügbaren Adressen fällt auf:

1. Geographic Basis Unicast
   Wir brauchen es zwar noch nicht, aber wer weiß - Für jeden Quadratmeter der Oberfläche Planeten Terra sind schon mal ein paar IP-Adressen reserviert.

2. Alte V.4 Adressen
   Sie fangen mit 96 Nullen an und haben dann die die alte Form:

   ::1234:3210

Je 1/256 des gesamten Adreßraums verteilen sich auf:

1. Provider based Unicast Adresses

2. Link-Local Adresses
   Weltweit festgelegte einmalige Adressen zur automatischen Konfiguration von Ethernetadressen bestimmt. Die den Rechnern vom Lokalen Router zugewiesene Adresse setzt sich zusammen aus eben dieser Link-Local Adress und der weltweit einmaligen und hardwaremäßig eingebauten Identifikationsnummer der Netzwerkkarten.

3. Site-Local Adresses
   Entsprechen den 10er und 23er Netzen für abgeschlossene Intranetz. Die Adressen sind so ausgelegt, daß sie einfach auf Provider Adressen umgestellt werden können.

4. Multicast Adresses
   Siehe unten bei Multicast. Für Router, Timeserver und Co.

IPv6 führt völlig neue Routing-Konzept ein und macht mit alten Schluß:

*Sourcerouting*
Das gibt es im Prinzip auch schon bei V.4, ist aber aufgrund der vielen zusammengestrickten Routingprotokolle nicht durchführbar. Es gibt hier die Möglichkeit festzulegen, welchen Weg ein IP-Paket nehmen soll, und den Weg dadurch z.B. auf einen bestimmten Provider festzulegen.

*Unicast*
Das bisher auch übliche Routing. Es wird ein Empfänger angegeben und nur der nimmt auch das Paket in Empfang

*Multicast*
Mehrere Empfänger sind möglich, z.B. bestimmte Dienstanbieter in definierten Netzabschnitten. Diese Möglichkeit bietet bahnbrechende neue Möglichkeiten, im Netz zu agieren. Z.B das automatische konfiguieren von Netzanbindungen. Man nehme einen Computer, stecke ihn an das Ethernet der Zahnarztpraxis. Der Computer schickt ein einziges IP-Paket ins Netz, mit dem Empfänger ‘Irgendein Router auf meiner Leitung’ und der Payload ‘Arrg, wer bin ich,

gib mir eine Adresse, gib meinem Leben ein Sinn.' Nun sind alle Router im LAN verpflichtet sich des hilflosen Newbies anzunehmen und ihm zu sagen, wer er sein soll.

Das Einstellen von TCP/IP Adressen, DHCP und andere Workarounds haben sich erledigt. Und es geht weiter. Man nehme einen Laptop, verlasse seinen Heimatarbeitsplatz Arbeitsplatz in Klein-Ellershausen in Nordrhein-Westfalen und begebe sich nach Timbuktu. Und jetzt? Bei V.4 heißt das: an ein Netz in Timbuktu anschließen und sich mit einer neuen IP Nummer und allen damit verbundenen Unannehmlichkeiten abfinden.


In Verbindung mit der neuen 128 bit Adressierung geht das so: Ein IP-Paket ins Netz schicken, Empfänger 'Mein Heimat-Router', Botschaft 'Ähh, an wen soll ich mich denn jetzt wenden, damit ich mein Heimatnetz erreiche? Und übigens: um zu mir zu kommen guck Dir mal an, welchen Weg das Paket genommen hat'. Aufgrund von Multicast fühlen sich jetzt alle erreichbaren Router angesprochen, ohne das der Laptop sie kennen muß, und leiten dieses Paket in die Heimat weiter.

*Anycast*
Gib mir irgendeinen aus einer definierten Gruppe von Empfängern, aber nur einen. Z.B. wenn man einen Router haben will, die Zugang zu einem bestimmten Netzabschnitt hat.

Weitere Features von IPv6

*Encryption*
Es existieren definierte Methoden für die Implementierung beliebiger Verschlüsselungsverfahren für die Payload. (Ebenso wie für die Autentifizierung derselben, aber das hatten wir schon oben.) Und sehr wichtig, es wird Methoden geben, Schlüssel auf IP Ebene auszutauschen. Es ist keine bestimmte Methode ausschließlich festgelegt, aber eine Methode, wie die dieses Methode festzulegen ist. Bisher ist die Rede von Photuris, einen Verfahren zum Austausch symmetrischer Schlüssel.

*Neues Fragmenthandling*
Überschreitet die größe eines IP-Paketes die Fähigkeiten eines Netzabschnittes, so kann es in Fragmente zerlegt werden. Das war bisher die Aufgabe der Router. Nun muß sich der Absender selber darum kümmern. Das ist für die Performance der Router wichtig.

*Encapsulation*
You'll be assimilated. Resistance ist futile. Ade IPX, Appletalk und so weiter. IP V.6 sieht vor diese Protokolle zu kapseln, so daß alte Applikationen und Betriebsysteme so weiter machen können wie bisher und neue sich nur noch um IP V.6 kümmern müssen.

# Chaos Communication Congress 96

*Realtime Dataflow*
Die Massenanwendungen der Zukunft, Telefonie und Video, brauchen angemessene Bandbreite. Hierzu können den entsprechenden Paketen variable Prioritäten eingeräumt werden. Beim Multicasting kann die Priorität der Anzahl der Adressen, die auf Empfang gehen, angepaßt werden. Multicastet einer ins Netz und keiner wills haben, bleibt die Priorität niedrig.

Zusammenfassung von
Krischan Jodies, Krischan.Jodies@link-goe.de

## Telefon und Internet

Referent: Olaf Strawe

Einleitung

Das Internet ist wohl das Modewort der 90er-Jahre geworden. Neben einschlägigen Diensten wie EMail und WWW bietet das Netz natürlich sehr viel mehr Möglichkeiten. Relativ neu ist allerdings die Möglichkeit der Internet-Telefonie. Olaf Strawe - Mitherausgeber der „TeleTalk“ - informierte das diskussionsfreudige Publikum über das

Telefonieren im Netz der Netze, und darüber, welche Funktionen des Telefonnetzes das Internet übernehmen kann. Jim Clark (Chairman der Netscape Co.) lieferte seine eigene Prognose zu diesem Thema:

„Die Internet-Telefonie wird erheblich größere Veränderungen für den Telekommunikationsmarkt mit sich bringen als die Einführung der Tonwahl oder Digitalisierung des Telefonnetzes.“

Tatsächlich liegt der Anteil der Gesamteinnahmen der Sprachtelefonie im Telekommunikationsbereich bei 85%.

*Internet-Telefonie*
Internet-Telefonie ist ein Begriff für zwei Dinge. Einerseits ist damit das Telefonieren mittels PC und Internetverbindung gemeint. So können zwei oder mehr Benutzer, die sich lokal bei ihren Internet-Providern eingewählt haben, über das Netz telefonieren. Dazu ist lediglich ein Mikrofon und eine Soundkarte nötig. Mit einer zusätzlichen Kamera (z.B. QuickCam) ist ohne großen Aufwand eine Videokonferenz möglich. Andererseits steht Internet-Telefonie für den Versuch der Implementation einer paketorientierten Sprachverbindung. Es soll das Zusammenwachsen der verschiedenen Kommunikationsnetze ermöglicht werden, die aufgrund historischer Gründe eigentlich getrennt sind.

Funktionsweise

Die Funktionsweise des Internet-Telefonierens entspricht technisch dem normalen Telefonieren (an digitalen Vermittlungsstellen). Die Sprache wird nach dem Codex-Prinzip digitalisiert (bei ISDN direkt im Telefon - bei Analogverbindungen in der entsprechenden Ortsvermittlungsstelle). Die Digitaldaten werden dann zum Zielort übertragen und wieder in analoge Signale umgesetzt. Hat der Benutzer noch kein direktes Internet-Telefon (als Zusatz für seinen PC), so übernimmt die Soundkarte die Umsetzung der Sprachsignale.

Erfunden wurde die Internet-Telefonie von der Firma Vocaltec. Der erste Client war das Programm IPhone, das zuerst noch auf dem IRC-Dienst aufsetzte. Mittlerweile laufen alle

# ..., Telefon und Internet, ...

Clients über den firmeneigenen Server oder über PPP (Point-To-Point-Protokoll). Die Standardisierung eines sinnvollen Protokolls erfolgte durch die ITU, die H.323 zum geltenden Standard für Realzeitübertragung auf Digitalstrecken erklärte (H.324 ist das entsprechende analoge Protokoll, da keine konstante Bitrate wie z.B. bei ISDN vorhanden ist).

Realität und Vision

Das weltweite Telefonnetz hat sich innerhalb von 120 Jahren entwickelt. Internet-Telefonie wurde erstmal vor zwei Jahren (Ende 1994) vorgestellt und hat besonders in diesem Jahr eine rasante Entwicklung erfahren. Mittlerweile gibt es 12-15 Anbieter von Clients.

Die erste Frage eines erfahrenen Internet-Surfers ist natürlich die Frage nach dem Datendurchsatz. Momentan ist dies noch eines der größten Probleme im Internet. Allerdings kann man optimistisch in die Zukunft sehen, denn technisch gesehen ist die Bandbreite fast vorhanden. „Fast“ deshalb, weil z.B. im Transatlantikbereich nur 20% der Kapazitäten genutzt werden. Die anderen 80% der Glasfaserkabel sind zwar physikalisch vorhanden, aber nicht angeschlossen. Der Betrieb von Internet-Leitungen ist relativ kostspielig und wird von den großen Telefonfirmen nicht mehr als nötig durchgeführt. Das Transatlantikkabel als solches hat sich bereits rentiert. (Rechenbeispiel: AT&T hat eine Leitung von Tokyo nach London legen lassen und bräuchte nur 37 Stunden volle Auslastung, um die Kosten voll wieder einzuspielen. Die Kosten von 1 Mrd. DM für das Transatlantikkabel sind bereits längst wieder eingenommen.) Mit einer veränderten Organisationsstruktur im Internet wäre also ein leistungsfähigerer Betrieb des Internet durchaus denkbar.

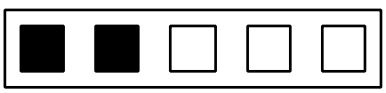
Angenommen, der Datendurchsatz wäre erträglich, so bräuchte man lediglich den PC entsprechend auszurüsten. Für $49 sind bereits komplette Endgeräte in Telefonform zum Anschluß an die Soundkarte erhältlich, mit denen man direkt am Telefon wählen kann. Im kommenden Jahr will auch die Firma Creative Labs ihre Soundkarten mit einem Chip ausliefern, der den Anschluß eines handelsüblichen Analog-Telefons erlaubt.

Desweiteren gibt es bereits einen ISP (Internet Service Provider), der ein Gateway in das normale Telefonnetz ermöglicht. Zu weitaus niedrigeren Gebühren kann so der Internet-Benutzer mit beliebigen Nicht-Internet-Benutzern telefonieren. Das Prinzip ähnelt dem des Callback: der Provider wählt eine landesinterne Rufnummer an und setzt die Signale zwischen beiden Netzen um. Im Idealfall könnte man in Deutschland mit einer Rufnummer in Amerika bereits zu $0.10 pro Minute telefonieren und sogar die Service-Rufnummern 1-800 kostenfrei abrufen (entsprechen unseren 0130er-Nummern).

*Legalität*

Da mit der Hilfe dieser Technik natürlich internationale Gespräche zum Ortstarif möglich sind, stellt sich die Frage nach der Legalität. Ein Zuhörer fragte z.B., ob man als Anwender nicht die Leitungskapazitätender Telekom „schmarotzen“ würde. Dem ist nicht so, denn prinzipiell ist eine Verbindung immer gleich teuer, ob über dieselbe Vermittlungsstelle oder quer durch Deutschland. Die Kosten der Verbindung zwischen den Ortsvermittlungsstellen kann man fast vernachlässigen. Da der Benutzer





für den Zugang zum Telekom-Netz zahlt, ist dies vom moralischen Standpunkt her völlig legitim.

In Amerika gibt es allerdings noch rechtliche Streitigkeiten. Der Verband der amerikanischen Telefongesellschaften (ACTA - America's Carriers Telecommunications Association) wandte sich an die FCC mit zwei Forderungen:

1. Internet-Telefonie-Software soll verboten werden

2. Softwareanbieter dieser Clients sollen als Telefongesellschaften (mit allen Pflichten) betrachtet werden

Noch ist die Verwendung allerdings möglich und legal. In absehbarer Zukunft wird aber jeder ISP und jeder Benutzer eine Flat-Rate von $3 bis $6 pro Monat zahlen müssen.

Status Quo

* Der Internet-Telefonie-Markt wächst stark.1995 nutzten 500.000 Anwender entsprechende Clients. Heute sind es bereits über 2 Mio.

* Mit der Einführung von Gateways zum Telefonnetz wird sich dieser Dienst (laut IDC-Prognose) auf 60 Mio. Nutzer bis zum Jahr 2000 erweitern.

* Kritisch betrachtet ist der NC (network computer) kein abgespeckter PC, sondern ein überdimensioniertes Telefon. Jeder NC verfügt über Mikrofon und Lautsprecher, läßt sich aber aufgrund der fehlenden Festplatte nicht als PC nutzen.

* Die QOS (quality of service) ist momentan aufgrund der Engpässe im Internet noch relativ niedrig. Allerdings wird uns von den Telefongesellschaften die Notwendigkeit des sekundenschnellen Verbindungsaufbaus und glasklarer Verbindungen als zu wichtig verkauft. Bei günstigeren Tarifen nimmt der Benutzer auch gerne einmal langsamere oder rauschende Verbindungen in Kauf. Es wird in Zukunft vermutlich mindestens zwei Netze geben: das überteuerte Telekomnetz (für Firmen) und günstige qualitativ niedrigere Netze (für Privatpersonen) - Stichwort „Aldi-Telefon".

Also: Es gibt derzeit bereits mehrere anwendbare Clients für Internet-Telefonie. PGPPhone erlaubt einem sogar eine kodierte Sprachverbindung. Im nächsten Monat soll es sogar eine Version für Microsoft Windows geben. Der Netscape Navigator bietet ebenfalls seit zwei Tagen mit der Version 4.0 einen Client an.

Laut Olaf Strawe wird sich die Internet-Telefonie auf Dauer durchsetzen. Jeder sollte es nutzen oder zumindest ausprobieren, um diese neue und günstige Kommunikationsform zu unterstützen.

Zusammenfassung von Christoph Haas, haas@informatik.uni-hamburg.de

## Furcht und Abneigung in Ungarn

von Tamas Bodoky, jr. <[1]>

(Übersetzung aus dem Englischen von Wau Holland [2])

Für den Außenstehenden mag es so aussehen, als ob es gar keine Datenkonflikte in Ungarn gibt. Es gibt keine blutigen, gewalttätigen Kriege und keine echten

# ..., Telefon und Internet, Ungarn, ...

Schlachtfelder abgesehen von den „Multiplayer Action Games“, den Spielen mit vielen Teilnehmern und nicht enden wollenden Netzwerk-Kämpfen der Fans von Quake, Doom und Duke Nukem.

Es gibt in Ungarn keine institutionalisierte amtliche Zensur. Während deutsche Behörden in Bezug auf das Internet konservativer sind als ungarische, die diesem bislang wenig Beachtung schenkten.

Ungarn ist im Bereich der Informationstechnologie zwar kein „Dritte-Welt-Land“. Aber beim näheren Hinsehen beträgt die gesamte internationale Bandbreite Ungarns beim Internet-Zugang weniger als 10 Megabit pro Sekunde. Die teilen sich zwei Dutzend nationale und regionale Internet Service Provider. Etliche zehntausende User im Bereich von Wissenschaft und Forschung nutzen davon weniger als ein Zehntel.

Zwischen Budapest und den anderen grossen Städten gibt es gerade einmal 64 kbps Kupferdrähte. Das gesamte ungarische Glasfasernetz besteht aus einem kurzen FDDI Ring zwischen den vier Universitäten in Budapest.

Statistiken besagen, dass auf dem Inlands-Infohighway zehnmal mehr Verkehr herrscht als im Auslandsverkehr. Damit liegt Ungarn irgendwo zwischen den Informationsmächtigen und den informationellen Habenichtsen —- eine aufsteigende Mittelklasse in der Region.

Das Fehlen grösserer Konflikte meint aber nicht Frieden: es gibt in Ungarn mehrere kleinere Konflikte, die eher typisch sind für den ehemaligen Ostblock. Hier ein paar Beispiele.

Beim langsamen Wegrosten des eisernen Vorhanges Ende der 80er besass Ungarn schon einen Internet-Zugang als Experimentierobjekt. Genau genommen spielte das Netz keine nennenswerte Rolle bei den politischen Veränderungen. Es war eine eng begrenzte Spielwiese für Experten, die zu sehr mit dem Diebstahl westlicher Technologie beschäftigt waren, um an oppositionellen Bewegungen teilnehmen zu können. Immerhin hielt der Staat das Netz für gefährlich: ich kenne ein paar Systemverwalter, die vom Geheimdienst um Mitarbeit gebeten wurden.

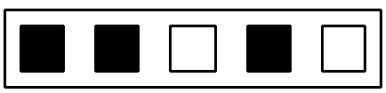
Das Internet bot keine Möglichkeit, unkontrolliert Informationen auszutauschen, wie es heute in China oder ex-Yugoslawien geschieht. 1988-89 waren sogar Fotokopierer und Faxgeräte selten und wurden streng beaufsichtigt.

Die Opposition benutzte während der letzten zehn Jahre des Kommunismus publizistische Steinzeit-Verfahren —- sehr zum Schaden ihrer Visionen. In ländlichen Sommerhäusern versteckten kognitive Dissidenten ihre Steinzeit-Druckmaschinen.

Auch diese Druckerpressen und zahllose antikommunistische Zeitschriften spielten nur die zweite Geige bei der Wende: die liberalisierten Reiseprozeduren 1988 in Verbindung mit den Werbespots im deutschen Sat-TV schaufelten das Grab für den Kommunismus in Ungarn.

Via Sat-Schüsseln und Kabel-TV-Netze sahen die Leute die Unterschiede im Lebensstandard. Damals gab es mehrstündige Warteschlangen an den Grenzübergängen für alle, die übers Wochenende nach Österreich fuhren. Ungarn fuhren nach Wien, um Kühlschränke, Videorekorder und CD-Player

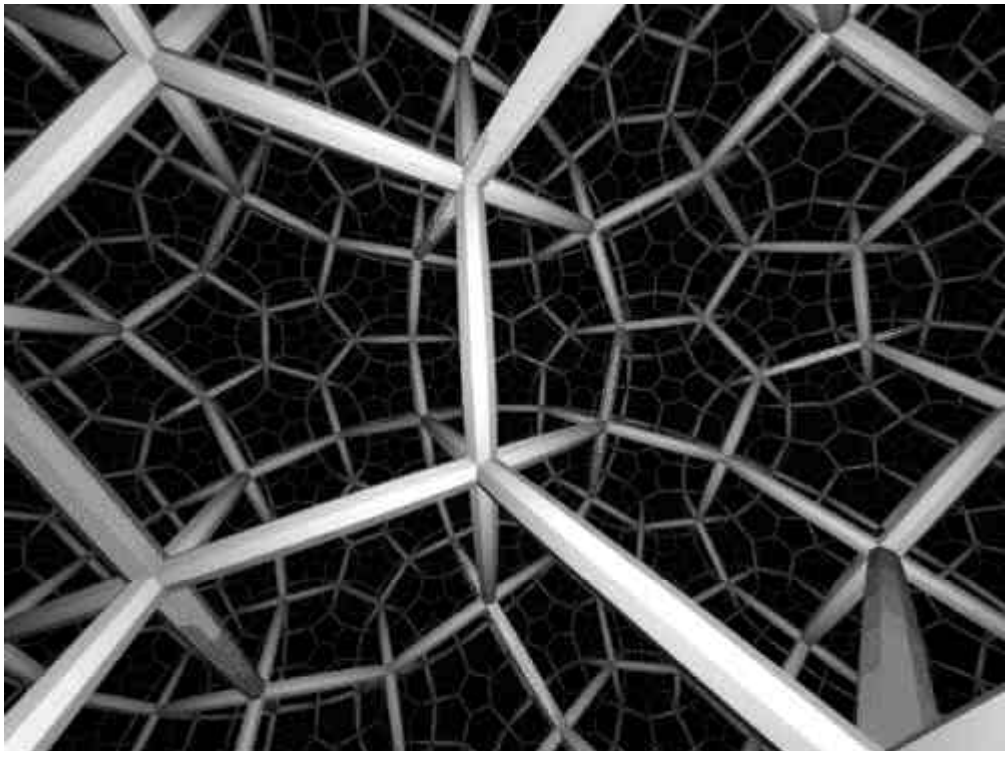




zu kaufen, wie sie in den kommerziellen Satelliten- und Kabelprogrammen gezeigt wurden. Diese Technik hatte sich gerade in Ungarn verbreitet.

Die Leute wollten eine Konsumgesellschaft und glaubten daran, sie würden all das kaufen können, wenn sie den Kommunismus abschaffen. Später waren sie enttäuscht, dass kein West-Ungarn erschien und die Kosten des Face-Lifting übernehmen wollte.

Zensur geschah indirekt und war so „soft“ wie das Regime. Privatpersonen konnten Schreibmaschinen oder PCs kaufen, aber in staatlichen Einrichtungen waren an staatlichen Feiertagen die Schreibmaschinen weggeschlossen und die Einschaltknöpfe von Fotokopierern lagen im Tresor.



Für Kopien brauchtest Du einen Antrag, den Du Deinem Boss zur Genehmigung vorlegen musstest. Bei Computern waren strikte Kontrollen unnötig, weil dieser Job bereits von den USA gemacht wurde. Sie hatten mit der COCOM-Liste den Verkauf von Mikroelektronik und High-Tech an den Ostblock verboten.

Wegen COCOM kauften Ungarn Computer im Westen, zerlegten sie und schmuggelten sie Stück für Stück über die Grenze. So wurden diese Produkte verfügbar, aber sehr teuer. Für den häuslichen Gebrauch wurden Rechner von Commodore und Sinclair ähnlich populär wie DEC und IBM bei Mainframes, wo von Amts wegen die Kräfte für den High-Tech-Diebstahl im Ostblock koordiniert wurden. Ungarn war spezialisiert auf PDP und VAX von DEC und baute davon auch Clones. Andere grössere Staatsbetriebe der CSSR, DDR oder der Sowjet-Union bauten IBM-Clones mit geklauten Betriebssystemen und Software. Diese Diebstähle wurden nicht als kriminell betrachtet, weil sie vom Staat begangen wurden. In der Folge führte das im Ostblock zu einem allgemeinen „Verfall der Moral“ in Bezug auf Technologie und Software. Das zeigen die jetzigen Fälle erheblicher Copyright-Verletzungen.

Nach den politischen Veränderungen kam es zum ersten Datenkonflikt zwischen Ost und West, als eine einzelne Kopie eines

# ..., noch mehr Ungarn, ...

Programmes Ungarn erreichte. Es wurde kopiert und verteilt durch informelle Zirkel, die intensive Verbindungen durch Clubs und Treffen hatten; später auch durch Modems und Telefon. Der Gebrauch von illegaler Software betrifft auch staatliche Einrichtungen und Büros.

Der Witz machte die Runde, daß in Ungarn eine einzige Kopie von Microsoft Word existierte, und der Lizenznehmer war Ungarn. 1995 warf die Business Software Alliance (BSA) ihren ersten Schatten über das Land und betrieb eine groß angelegte Kampagne für legale Software. Seither haben wir gigantische Reklametafeln an den Straßen, auf denen Leute, die illegale Software nutzen, in Handschellen gezeigt werden. Mit harten Devisen sponsort die BSA die ungarische Polizei. Und die nutzt ebenso wie fast jede andere staatliche Behörde illegale Software. Im Gegenzug ist die Polizei der willige Büttel, um Räume von Fido-Sysops zu durchsuchen; gewidmet dem Fetisch legaler Software. Die BSA betreibt eine anonyme Hotline, wo Anrufer nicht lizensierte Software melden können. So wird die Polizei auf die Software-Schwarzmärkte geführt. Die ersten Aktionen der BSA sorgten für Panik beim öffentlichen ungarischen Netzwerk FidoNet BBS, das Teil des weltweiten FidoNet ist. Im Ergebnis wurde die Verbreitung kommerzieller Software bei Fido verboten.

FidoNet war ein sehr effektives BBS Netzwerk und läuft weiterhin. Aber die Store&Forward-Netze verloren ihre Bedeutung, als Internet an Popularität gewann. Ein weiteres Offline-Netzwerk ist Green Spider, gefördert von regionalen Umwelt-Zentren. Ein Unixserverer dient via Telefon für hunderte von Mitgliedsorganisationen dem e-Mail-Tausch und als Newsfeed.

Das Internet begann auch in Ungarn als ein staatliches Informationsprojekt zur Infrastrukturentwicklung. Ungarische Universitäten und Forschungseinrichtungen nahmen seit 1991 am System teil. Das meint, es herrschte eng begrenzter Zugang in Ungarn vor dem Erscheinen des WWW.

Etliche Mailing-Listen, Gopher-Menus und Usenet-Newsgroups brachten auf einer non-profit-Basis Inhalte ins Netz. Mehrere ungarischsprachige Foren wurden in den USA von HIX, dem Hollosi Information Exchange, gestartet. Er wird betrieben von Jozsef Hollosi, einem ungarischen Experten, der in den USA arbeitet. Ich selbst, damals Student, begann eine Mailingliste für die Leser von „Magyar Narancx“, dem besten Wochenmagazin Ungarns (http://www.net.hu/narancs/) und bald fand sich bei narancs-l - bis heute - eine der populären virtuellen Gemeinschaften. Es war ein frühes Experiment des interaktiven Journalismus. Denn die Teilhaber der Liste konnten direkt auf meine Beiträge antworten, Themen vorschlagen oder selbst Texte verfassen. Die ungarisch-sprachige Liste ist ein Platz innigen Soziallebens mit durchaus internationalen Verbindungen: als der Skandal, als „Fishman Affidavit“ bekannt, durchs

Netz fuhr, spiegelten wir die geheimen Dokumente der Scientology-Kirche auf einigen Uni-Servern und BBS-Systemen.

Die weltweite Verbreitung des Internet durch das World Wide Web begann seinen Hype in Ungarn 1995. Bald traten die ersten kommerziellen Provider auf. Die Kosten für vollen Zugang zum Netz fielen binnen eines Jahres von rund 200 auf 40 US-Dollar pro Monat. Zahlungen „pro Megabyte“ entfielen, und Hardware wurde erschwinglich. Der erste kommerzielle Provider war eine Tochter



von SZTAKI, dem staatlichen Institut für die Internet-Entwicklung. Es unterhielt das „National Information Infrastructure Development Program“, ein staatliches Projekt mit ungarischen und internationalen Geldquellen.

Das „Lake Success agreement“ versorgte SZTAKI mit billiger Hardware für nichtkommerzielle Zwecke. Das wurde missbraucht, um Profit zu erwirtschaften aufgrund des frühen Monopoles auf dem ISP-Markt. 1995 startete rund ein Dutzend private Internet Service Provider. Die meisten überschätzten die Wachstumsrate des Marktes. Einige davon starren nun dem Bankrott ins Auge, wo die eine und einzige ungarische Telecom, MATAV, das Spielfeld betritt.

MATAV hat ein Staatsmonopol über die Drähte in Ungarn für die nächsten 25 Jahre, das 2018 endet. MATAV gehört aber nicht nur dem Staat. Der Hauptaktionär ist MagyarCom, ein Joint Venture zwischen Deutsche Telekom und Ameritech International. Da stellt sich die Frage der wirtschaftlichen Rekolonialisierung des früheren Ostblocks durch multinationale Konzerne. MATAV besitzt bereits den Löwenanteil der Internet-Bandbreite zwischen Ungarn und dem Rest der Welt und besitzt alle Kabel und Kabelschächte im Land.

Nach der Versuchsphase jetzt wird MATAV ab 1.1.1997 im Regelbetrieb ein Internet Service Provider, MATAVNet. Die können mit Leichtigkeit ein vergleichbares ISP-Monopol in Ungarn schaffen wie beim Telefon.

Das Internet ist weit davon entfernt, Massenmedium zu werden in Ungarn. TV ist die Droge des Volkes. „mainstream“-Empfinden und Handeln wird geprägt von den zwei staatlichen TV-Programmen, Radiokanälen und einigen Tages- und Wochenblättern, die eine zwiespältige Rolle bei der Popularisierung des Internet spielten. Das ungarische Medienpublikum hat ein extrem polarisiertes Bild des Netzes; zum einen das Versprechen eines utopischen Paradieses vom globalen Dorf, das naht —- und zum andern die Alpträume und Klischees konservativer und bürokratischer Kräfte, die das Netz als Gemengelage von Kinderpornos, internationalen Terroristen und illegaler Wissenspfründe darstellen und als Bedrohung für Christentum und Familie und Staat anschwärzen. Grotesk ist dabei die Rolle von Microsoft, die das Bild des Internet in den Medien etwas schützten, nachdem sie ein Jahr vorher versuchte, Leute vom Internet fernzuhalten und abgesehen davon, daß sie weiter stiller Sponsor von BSA Ungarn sind. Microsoft spendete einer Handvoll „wichtiger“ Leute (Politikern und Journalisten) Computer, Sofware und Internet-Zugang. Die surfen nun im Netz eine Zeit lang und loben Microsoft dann für das Werk, „Internet nach Ungarn“ zu bringen. Bill Gates besuchte kürzlich das Land und unterzeichnete ein Abkommen mit dem Premierminister und MATAV.

Die kleine Internet-Gemeinschaft Ungarns war empört, konnte jedoch nichts tun ausser einer Debatte, welche Chancen eine Kundgebung gegen Gates hätte bei seiner Rede im staatlichen Opernhaus. Denn die Massenmedien waren nicht interessiert, die nichtgesponsorte Wahrheit zu drucken.

[Relativierender Einschub des Übersetzers: Bei der Rede von Bill Gates auf der CeBIT 1994 in Hannover hielten einige Menschen in der letzten Reihe ein Bettlaken hoch, das nur Teile der Saalrückwand verdeckte und

niemanden behinderte. Bill Gates stockte kurz und bleich, als er las, was auf dem Bettlaken stand: „ALT-F4“ und klein in der Ecke „C.C.C.“.

Doch Bills Blässe währte nicht lange: CeBIT-Saalwächter rissen das Laken unter Missachtung der Eigentumsrechte an sich. Seither fehlt das Dokument dem Museums-Bestand des CCC. Dabei übersteigt sein Wert den einer Microsoft-Pauschal-Lizenz für jedes bettlakenbestohlene CCC-Mitglied. Und die BSA redet vom Diebstahl bei Bits, wo Bill Gates sich freut, wenn vor seinen Augen physikalisches Eigentum offensichtlich gestohlen wird! Soviel zur Relativierung der Handschellenplakate in Ungarn.]

Später in diesem Sommer, nach einem Bombenanschlag, behauptete Objectiv, eines der am meisten angesehenen Nachrichtenprogramme des staatlichen Fernsehens, dass das Rezept für den Sprengstoff aus dem Internet stammen würde. Daraufhin verlangte die Polizei von allen Internet-Providern aus der Gegend des Bombenanschlages die Herausgabe der Kundenliste.

Die meisten ISP taten das, aber einige wandten sich an den Ombudsman für Daten. Der prüfte die Rechtmässigkeit der Forderung und fand heraus, dass die Gesetze Ungarns den Behörden alle Rechte geben, alle Daten von Abonnenten von Datendiensten zu bekommen. Im ungarischen Parlament wird ein Gesetz über das Abhören von Mobiltelefonen beraten. Bürgerrechtliches Engagement ist im Vergleich zu westlichen Ländern eher nicht vorhanden. Nur wenige Organisationen begreifen Macht und Bedeutung solcher neuer Medien; das gilt bislang auch für unabhängige Journalisten. Beim Sichten des ungarischen WWW-Angebotes findest Du die alten Machtstrukturen und etwas Geschäfts-Schnickschnack.

Schließlich baten mich die Organisatoren dieser Konferenz, über die osteuropäische Cyberpolitik der Soros-Stiftung zu sprechen. Da ich nicht offiziell mit der Stiftung verbunden bin, weiss ich nicht viel dazu, aber ich kann einem Projekt berichten, an dem ich teilnahm.

Im Frühling 1995 brachte Geert Lovink, unser Freund, der wohlbekannte niederländische Medientheoretiker, die Idee eines Non-Profit ISP nach Ungarn. Diese Idee gewann deutliche Popularität unter Internet-Usern und NGOs, die unter hohen Zugangskosten und fehlender Infrastruktur litten. Sie gründeten eine Non-Profit-Organisation namens Koz-Hely Association for Public Computer Networks und kamen zur Soros Stiftung mit Bitte um Hilfe. Die Stiftung würdigte die Idee, entschied aber, es auf ihre Weise umzusetzen. Ein Jahr später schuf sie eine Organisation namens „Center for Culture and Communication“ (C3), mit einem eigenen 512 Kilobit/s Satelliten Uplink, Hardware von Silicon Graphis und Terminal-Einwahlservern für Nonprofit-Zwecke. Das Vorgehen von C3 ähnelt sehr dem ein Jahr vorher veröffentlichten Konzept von Koz-Hely.

In der Zwischenzeit wurde der ursprüngliche Ansatz von Koz-Hely, günstiger Internet-Zugang, im Wettbewerb der kommerziellen Provider realisiert. Die ungarische Soros-Stiftung hat bis jetzt nicht auf den Entwurf von Koz-Hely reagiert, aber zwei Leiter als Angestellte angeheuert. C3 ist nicht wirklich unabhängig, sondern Teil der geschlossenen Hierarchie der Soros Stiftung und ihrer kulturellen und politischen Aktivitäten - die offene

Gesellschaft der Elite - und wird gesponsort von MATAV und Silicon Graphics.

C3 bekam eine umstrittene Publizität in der kurzen Zeit, wo sie den sogenannten Domain-Name-Registrierkrieg in Ungarn begannen.Sie wählten c3.hu als Domainname. Das widersprach den Regeln der Registratur. Danach war es erforderlich, dass eine juristische Person (vergleichbar z.B. e.V. oder GmbH) mit dem gleichen oder einem ähnlichen Namen existiert, um unter der Domain .hu registriert zu werden. Da C3 keine juristische Person war, verweigerte der offizielle Registrar die Eintragung von c3.hu

Es gab einen Haufen Argumente auf beiden Seiten und ich konnte dem liberalen Ansatz von C3, den Registriervorgang betreffend, folgen. Doch ist es nach meiner Meinung nicht hinnehmbar, dass die Stiftung ihren politischen Einfluss nutzte, um den Namen einzutragen. In der Folge trat der Registrar zurück und seit Frühjahr 1996 gibt es niemanden, der für die Registratur verantwortlich ist. Ungarische ISPs begannen einen endlosen Kampf über die Regeln der Registratur von Domainnamen, der nach mehreren Monaten ergebnislos blieb. Nun bereitet das Ministerium für Telekommunikation eine Enscheidung vor, um den Konflikt zu beenden.

Wer eine .hu Domain registrieren will, wartet Wochen oder Monate - oder er kennt irgendwen im Ministerium, bei MATAV, SZTAKI oder bei der Soros-Stiftung. Es geht viel schneller einen Domainnamen unter .com bei InterNIC zu kaufen, wenn die amerikanische Firma Motherland das nicht schon vorher getan hat.

Motherland hat im Blick auf die diffizile ungarische Lage bereits die Namen mehrerer wohlbekannter ungarischer Unternehmen registriert, darunter malev.com für das ungarische Luftfahrtunternehmen. Solche Namen werden dann für ein paar tausend Dollar, zahlbar binnen 24 Stunden, angeboten - anstatt der 100 Dollar Registriergebühr.

Wie Du nun feststellen kannst, gibt es einige Gründe für Furcht und Abneigung in Ungarn. Aber im Unterschied zu anderen in der Region sind unsere Datenkonflikte leicht zu überleben.

Ich danke [3]Tamas Szalay für seine wertvollen Anmerkungen und [4]Diana McCarty für ihre sorgfältige Übersetzung ins Englische, die Grundlage der deutschen Übersetzung von [5]Wau Holland.

Die Homepage von Tamas Bodoky ist [6]

References

[1] bodoky@caesar.elte.hu
[2] WAU@OLN.comlink.apc.org
[3] tszalay@caesar.elte.hu
[4] diana@dial.isys.hu
[5] wau@ccc.de
[6] http://caesar.elte.hu/~bodoky/

## Was ist eigentlich ein Trust-Center und warum sollte ich einem vertrauen?

Im ersten Trust-Center-Workshopauf diesem Congress ging es um die Grundlagen von Trust-Centern, die möglicherweise schon bald als Autoritäten unsere digitalen Existenzen bestimmen werden. Trust-Centers (korrekterweise wohl besser als „CA“, also „Certification Authority“ zu bezeichnen) nehmen sich eines der großen Probleme im

# ..., Ungarn, Trust Center.

Internet an: Wer garantiert eigentlich, daß die Person, mit der ich Geschäfte tätigen oder Nachrichten austauschen möchte, tatsächlich diejenige ist, die sie vorgibt zu sein?

CAs sind Institutionen, die elektronische Unterschriften beglaubigen — damit sitzen sie an den Schaltstellen der Macht im elektronischen Handel, entscheiden sie doch über die Identität (und damit die Glaubwürdigkeit) von Geschäftspartnern oder Privatpersonen. Wodurch sind diese wichtigen Stellen autorisiert? So seltsam es auch klingen mag, aber sie sind es gar nicht. Verisign Inc. aus den USA und Thawte aus Süd-Afrika sind die beiden Unternehmen, die am lautesten und finanzkräftigsten erklärt haben, daß sie für diese Aufgabe geeignet sind.

Dies hat dazu geführt, daß die Zertifikate dieser beiden Firmen fest in den beiden wichtigsten Internetbrowsern (Netscape Navigator und Microsoft Internet Explorer) eingebaut sind. Andere Zertifizierungsstellen für digitale Unterschriften sind entweder nicht vorgesehen (Internet Explorer) oder nur über komplizierte Umwege zu benutzen (Netscape).

Nicht jeder möchte aber bei einer so wichtigen Sache wie die Bestätigung der digitalen Identität auf Privatunternehmen hoffen. Und wer hat schon das nötige Kleingeld, um zur Beglaubigung in die USA oder nach Süd-Afrika zu reisen?

In Deutschland gibt es mit der DFN-CA (für das Deutsche ForschungsNetz, das sich um universitäre Rechenzentner und ihre Internetanbindung kümmert) auch eine Initiative aus den Reihen des Individual Network e.V. Dieser Verein fühlt sich den privaten Internetbenutzern verpflichtet und möchte mit seinem Projekt IN-CA vor allem Kompetenz in Sachen Authentifizierung beweisen. Nur rechtlich verbindlich möchte die Initiative bitte nicht sein; nach Aussagen des IN-CA-Sprechers Lutz Donnerhacke ist die CA des Individual Networks „nur eine Spielerei“.

Abseits der ebenfalls im Workshop erläuterten technischen Fragen zu Vor- und Nachteilen von SSL (Secure Sockets Layer, die die Authentifizierung möglich machen) stand vor allem die Frage nach dem gesellschaftsrelevanten „CA, quo vadis?“ im Raum: „Wollen wir nur ein Spielzeug haben, oder bieten wir eine echte Hacker-Alternative zu den kommerziellen Stellen wie Verisign oder Thawte? Wollen wir Verantwortung übernehmen und eine eigene CA schaffen und damit selbst in die Rolle der bösen, nur auf Kommerz und Sicherheit bewußten Buben schlüpfen?“, fasste Hacker Rop Gronggrijp aus den Niederlanden die Vorbehalte im Workshop-Publikum zusammen.

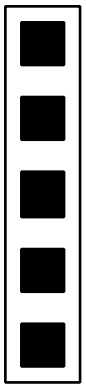
Mit der eventuellen Umsetzung der kühnen Pläne von einer eigenen Zertifizierungsstelle wollen sich Congressteilnehmerinnen und -teilnehmer morgen in einem weitern Workshop beschäftigen.

Zusammenfassung von Jens Ohlig,
j.ohlig@bionic.zerberus.de

## Die Congress-Dokumentation

Die gesamte Dokumentation kann mittels des Bestellfetzens (Rückseite) als Hardcopy bestellt werden.

Außerdem liegt die gesamte Dokumentation auf dem CCC Web Server (http://www.ccc.de).



Die Datenschleuder
Nummer 58, März 1997

# Der Bestellfetzen

Literatur

_____ DM 42,00  Mailbox auf den Punkt gebracht
_____ DM 29,80  Deutsches PGP-Handbuch, 3. Auflage + CD-ROM
_____ DM  5,00  Doku zum Tod des „KGB“- Hackers Karl Koch
_____ DM 25,00  Congressdokumentation CCC ‘93
_____ DM 25,00  Congressdokumentation CCC ‘95
_____ DM 50,00  Lockpicking: Über das Öffnen von Schlössern

Alte Datenschleudern

_____ DM 50,00  Alle Datenschleudern der Jahre 1984-1989
_____ DM 15,00  Alle Datenschleudern des Jahres 1990
_____ DM 15,00  Alle Datenschleudern des Jahres 1991
_____ DM 15,00  Alle Datenschleudern des Jahres 1992
_____ DM 15,00  Alle Datenschleudern des Jahres 1993
_____ DM 15,00  Alle Datenschleudern des Jahres 1994
_____ DM 15,00  Alle Datenschleudern des Jahres 1995
_____ DM 15,00  Alle Datenschleudern des Jahres 1996

Sonstiges

_____ DM 50,00  Blaue Töne / POCSAG-Decoder /
                PC-DES Verschlüsselung
_____ DM  5,00  1 Bogen „Chaos im Äther“
_____ DM  5,00  5 Aufkleber „Kabelsalat ist gesund“

    + DM 05,00  Portopauschale!

_____ Gesamtbetrag

Die Kohle liegt

    o in bar
    o als Verrechnungsscheck

bei bzw.

o  wurde überwiesen am ___.___._____ auf
      Chaos Computer Club e.V., Konto 59 90 90-201
      Postbank Hamburg, BLZ 200 100 20

Name _____

Straße _____

PLZ, Ort _____

# Der Mitgliedsfetzen

Mitgliedsanträge und Datenschleuderabonnement

o Satzung + Mitgliedsantrag
  (DM 5,00 in Briefmarken)

o Datenschleuder-Abo
  Normalpreis DM 60,00 für 8 Ausgaben

o Datenschleuder-Abo
  Ermäßigter Preis DM 30,00 für 8 Ausgaben

o Datenschleuder-Abo
  Gewerblicher Preis DM 100,00 für 8 Ausgaben
  (Wir schicken eine Rechnung)

Die Kohle liegt

    o in bar
    o als Verrechnungsscheck
    o in Briefmarken

bei bzw.

o  wurde überwiesen am ___.___._____ auf
      Chaos Computer Club e.V., Konto 59 90 90-201
      Postbank Hamburg, BLZ 200 100 20

Ort/Datum _____

Unterschrift _____

Name _____

Straße _____

PLZ, Ort _____

Tel/Fax _____

E-Mail _____