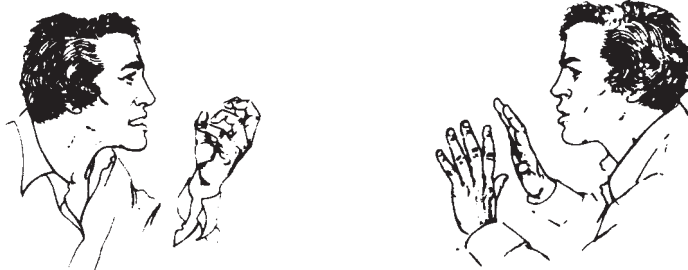


# Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende  
Ein Organ des Chaos Computer Club



## Die gefährlichsten Hacker sitzen bei der IBM?

### Und nicht im Knast?

*Während Sie diese Zeilen lesen,*

*könnte es sein, daß einer unserer Mitarbeiter gerade versucht, sich in Ihre Firmendaten "einzuhacken". Diese eher ungewöhnliche Maßnahme ist eine unserer Dienstleistungen, mit denen wir Schwachstellen in Ihrem Unternehmen aufdecken.*

*Dabei testen CCC-Mitarbeiter quasi als bezahlte Hacker, wie stark sie Ihr System abgesichert haben und auf welche Daten und Programme sie unbefugt zugreifen können.*

*Aber auch sonst können wir Ihnen helfen, den Rohstoff "Information" in Ihrem Unternehmen zu schützen: vor Zerstörung im Fall von Katastrophen, vor Computerviren, vor Mißbrauch oder aber vor versehentlichem Löschen.*

*Der CCC bietet hierfür unter-*

*nehmensweite Gesamtkonzepte an, die nicht nur Systeme innerhalb eines Unternehmens schützen, sondern auch den Anschluß an externe Netze sichern. Netze, in die z.B. Geldausgabeautomaten eingebunden sind, werden zusätzlich durch Verschlüsselungsverfahren gesichert.*

*Ein weiteres Beispiel dafür, wie genau wir es mit ihrer Sicherheit nehmen, ist der CCC HC/423, ein Computersystem, das bisher eigentlich noch nicht geknackt werden konnte.*

*Aber auch sonst können Sie sich bei dem CCC und unseren Geschäftspartnern ganz sicher sein. Sprechen Sie mit uns, was immer passiert: Wir sorgen für eine Lösung.*

## Editorial

Nach einer durchgemachten Nacht, einigen Tassen Kaffee und einer gediegenen Überdosis harzigen Tabaks ist es geschafft... die neue Datenschleuder ist fertig, das Resultat haltet Ihr in den Händen – dieses Mal seit langer Zeit wieder komplett am Bildschirm gemacht. Für einige in der Redaktion das erste Mal, sowohl am Bildschirm als auch überhaupt.

Weitere Neuerungen finden sich auf Seite 3, der Congress findet dieses mal nicht, wie gewohnt, in Hamburg, sondern in Berlin statt. In der ehemaligen Kunsthalle findet sich eine deutlich bessere Infrastruktur und auch sehr viel mehr Platz zum Gestalten als in dem uns ach so vertrauten Bürgerhaus in Eidelstedt.

Neues auch auf Seite 14: dort hat sich ein Mensch entschlossen, Bausätze zu verticken. Mal sehen, was kommt.

Die Clubaktivitäten sind in den letzten Monaten wieder spürbar angewachsen, wie der Schritt nach Berlin auch deutlich zeigt. Davon profitieren soll unter anderem das Chaos-Archiv: Es ist mittlerweile 200-300 Ordner dick, so daß eine Katalogisierung überfällig ist.

Seit nunmehr 10 Jahren sammeln wir Grundlageninfos, Presseberichte, Dokumentationen aus den verschiedensten Bereichen der Informationswelt. Es wird also demnächst ein Verzeichnis geben, in dem alle verfügbaren Titel aufgeführt sind. Schon diesmal enthält der Bestellfetzen (letzte Seite) zwei weitere Dokumentationen (CCC '93 und Lock Picking).

Resumée: Die Unart des Mäuseschubsens und Technohörens verbreitet sich nun auch bei uns immer mehr. Wir sind jetzt müde und legen uns zur Ruh...

Bis zur nächsten DS (Anfang/Mitte Dezember)

Euer Team vom CCC

PS: Einige von "uns" sitzen leider doch im Knast: Grüße und Kraft!

## Kleingehacktes – Kurzmeldungen

### CD-ROM-Spaß

Die Yellow-Point GmbH hat Konkurs angemeldet, IBM noch nicht. Aber auch bei Yellow-Point scheint das nicht richtig ernst gemeint zu sein: das Nachfolgeprodukt "Yellow-Star" ist für Ende September angekündigt, lag bei Redaktionsschluß zur Rezension leider noch nicht vor.

Nachdem IBM mitbekommen hat, daß ihr Show-case-System genauso wie Yellow-Point arbeitet, nur der DES-Key nicht 1 sondern 8 Byte lang ist, haben sie sich sehr redlich um ein Treffen mit einigen CCC'ern bemüht, was dann auch stattgefunden hat - Bericht: hinten in dieser Ausgabe.

### GSM-Ärger

Wie dem Datenschutzbeauftragten im Juni zu entnehmen war, ist es mit dem Datenschutz bei Mobiltelefonen, bezüglich der Ängste, das Bewegungsbilder erstellt werden könnten, noch viel ärger als man gemeinhin annimmt: "eine Ortung von Mobilfunkteilnehmern ist theoretisch mit Hilfe der bestehenden Technik möglich.

Es stellt sich deshalb die Frage, ob solche Verfahren eingerichtet oder bereits genutzt werden. In der Zeitschrift "Telekom Vision" (5/93, S.39) äußert sich Mobilfunkvorstand Klaus Hummel über den Datenschutz bei Funktelefonen. Er antwortet dort auf die Frage, ob Roamingdaten zur Erstellung von Bewegungsprofilen genutzt werden: "... Lediglich für besondere Überwachungsmaßnahmen ist der Netzbetreiber verpflichtet, den Sicherheitsorganen entsprechende Auskünfte zu erteilen. Hierfür werden spezielle Funktionen im Netz bereitgestellt, die über die Festlegungen des GSM-Standards hinausgehen..."

Na dann: Prost Mahlzeit!

LS16

Der Chaos Computer Club lädt ein:

## 11. Chaos Communication Congress '94 Berlin, 27.-29. Dezember 1994

“Internet im Kinderzimmer - Big business is watching you?!”

In der ehemaligen Kunsthalle, D-10787 Berlin, Budapester Str. 42  
(gegenüber Gedächtnis-Kirche, 3 Minuten Fußweg vom Bahnhof Zoo)

Dauerkarten	
Normaltarif	DM 42,00
Mitglieder des CCC e.V.	DM 23,00
Journalisten	DM 75,00 (Pressemappe und ausführliche Congressdokumentation inklusive)
Gewerbliche Teilnehmer	DM 100,00

Tageskarten	
Normaltarif	DM 20,00
Schüler und Arbeitslose	DM 12,00

Eine Voranmeldung durch Überweisung auf das Konto des Chaos Computer Club, Konto-Nr. 599090-201 bei der Postbank Hamburg (BLZ 200 100 20) wird empfohlen.

Veranstalter: Chaos Computer Club e.V., Schwenckestraße 85, D-20255 Hamburg,  
Telefon +49 (40) 4903757, Fax +49 (40) 4917689, Mailbox +49 (40) 4911085

In Kooperation mit dem FoeBuD e.V., Marktstraße 18, D-33602 Bielefeld,  
Telefon +49 (521) 175254, Fax +49 (521) 61172, Mailbox+49 (521) 68000

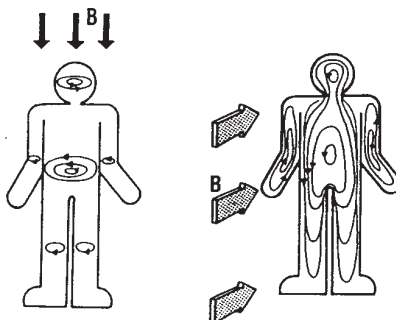


## CCC '94

Der traditionell zwischen Weihnachten und Neujahr vom Chaos Computer Club veranstaltete Chaos Communication Congress bietet auch dieses Jahr wieder allerlei für die Tramper auf den Datenautobahnen und allen anderen.

Nachdem der Congress die letzten 10 Jahre in Hamburg im Eidelstedter Bürgerhaus tagte, öffnet er sich dieses Jahr inhaltlich wie strukturell einem größeren Publikum und findet in der ehemaligen Kunsthalle in der Berliner City am Breitscheidplatz, gegenüber der Gedächtniskirche, statt.

Nachdem der Computer sich als das wichtigste neue Medium durchgesetzt hat, gewinnen die Fragen nach der Gestaltung dieses Mediums, das auch den Fernseher in seiner Bedeutung noch überholen wird, zunehmend gesellschaftliche Relevanz.



Um zu erreichen, daß Stichworte wie z.B. "interaktives Fernsehen" mehr beinhalten als die "buy"-Taste an der Fernbedienung, die den Kauf eines Produktes beim Betrachten des Werbespots aufnötigt, braucht es Visionen. Mit den selbst geschaffenen, frei zugänglichen Netzwerken, die unter dem Stichwort "Interaktivität" weitaus mehr zu bieten haben, erreichen die Hacker jedoch inzwischen nicht nur die Kinderzimmer der Informationsgesellschaft, sondern geraten auch in Bedrängnis durch Großkonzerne, die Netzwerke zunehmend als Betätigungsfeld begreifen.

Die Tendenz der Industrie, eine direkte Glasfaser bis in unsere Brieftaschen zu legen und die damit verbundene Kommerzialisierung von Informationswegen, bedrängt gesellschaftlich orientierte Informationsanbieter, wie z.B. Umweltschutz- und Menschenrechtsorganisationen, Parteien- und Gewerkschaften, deren Interessen nicht vorrangig finanzieller Natur sind.

Aktuelle Themen wie die Entmonopolisierung des Telefonnetzes und die Gestaltung zukünftiger Netzstrukturen stehen daher dieses Jahr genauso auf dem Programm wie die traditionellen Workshops und Informationsveranstaltungen. Der Erörterung und Hinterfragung von Industriekonzepten kommt dieses Jahr neben der Vorstellung eigener Projekte und Ideen eine besondere Rolle zu.

Unter dem Titel "Seid umschlungen, Millionen" werden Workshops und Diskussionen zur finanziellen Zukunft der elektronischen Netze angeboten. Ob Vebacom oder RWE - wer wird am meisten an den Glasfaserpipelines verdienen durch die das graue Gold in Form von Bits und Bytes fließen wird. Sind freie BürgerInnen-Netze und weltweite Kommunikation für Privatleute, Mittelständler, kleinere Firmen und Institutionen in Zukunft erschwinglich? Was wie eine kühle Rechenaufgabe aussieht ist in Wirklichkeit gesellschaftspolitische Kalkulation, wo der Satz "Wissen ist Macht" sich zu "Du sollst nur wissen, was Du Dir leisten kannst" verändern könnte. Auch die Form des Wertaustausches, das elektronische Geld, wird ein Untersuchungsthema in den zahlreichen Workshops sein.

Die eigentliche Lebensader des Congresses: das Informationschaos, strukturiert in einzelnen Workshops, aber auch unstrukturiert bis in alle Flure und vor allem das Chaos-Café, kann thematisch hier nur in Stichworten umrissen werden, wie z.B. CD-ROM-Sicherheit, Phonephreaking und ISDN, Verfassungsschutzanwerbungen in der Mailboxszene, Durchsuchungen wegen "Störung des öffentlichen Friedens" bei Mailboxen, Rechtliches zum BTX-Staatsvertrag und FAG, Unsich-

erheit der Chipkarte und dadurch sich ergebende Fragestellungen...

Sollte die Zeit nicht reichen, steht der 30. Dezember für weitere spontane Veranstaltungen zur Verfügung.

Um die Veranstaltung vom technischen Niveau so verständlich wie möglich zu halten, wird es zu einigen Themen wie z.B. dem Internet einführende Workshops geben. Gelegenheit zu schöpferisch-kritischer Nutzung der vorhandenen Technologie bieten das Hack-Center und die Datentankstellen in jedem Raum. Zum Nachlesen und zur Erstellung dezentraler Sicherungskopien hält das Chaos-Archiv einiges an Literatur und eine Batterie Fotokopierer bereit.

## „Elektronische Beweissicherung“ – der große Lauschangriff

Wer die Geschichte nicht beachtet, wird gezwungen, die Fehler zu wiederholen...

Seit einiger Zeit aus der öffentlichen Diskussion verschwunden gärt das Thema aber immer noch in den „Wahlkampfpapieren“ der Parteien, resp. wird gerade im Bundestag umgesetzt:

Gemeint ist hiermit die Einschränkung eines wichtigen Teils unserer Grundrechte und der Gewaltenteilung. Schon 1993 wurde mit dem Gesetz zur Aufspürung der illegalen Geldwäsche ein wesentlicher Grundsatz unseres Rechtssystems erlegt - die Beweislast wurde vom Kläger auf den Angeklagten überschrieben. Hieß es noch vorher „Im Zweifel für den Angeklagten“ so muß mensch jetzt beweisen, daß er sein sauer verdientes Geld auch redlich verdient hat, ansonsten kann das Vermögen dieser Person eingezogen werden. Mit dem, was als Paket zur Bekämpfung der Kriminalität geplant ist, werden weitere Grundrechte und -sätze untergraben.

Geplant ist unter anderem:

- Die Verwendung der durch den Bundesnachrichtendienst ausgespähten Erkenntnisse zum Zwecke der Kriminalitätsbekämpfung im Inland.

Aufgrund der Erfahrungen im Dritten Reich sieht unsere Verfassung die klare Trennung zwischen geheimen Nachrichtendiensten und Polizei vor.

- Das Erweitern der Ausspähbefugnisse der Polizei auf die Wohnung/Geschäftsräume der Person. (Art. 13GG)

Im Dritten Reich war das Hören von „Feindsendern“ nicht illegal, wohl aber die Teilnahme an einer verbotenen Versammlung. Meist hörte mensch aus Kapazitätsgründen mit mehreren Menschen Radio.

- Ebenso sollen die Möglichkeiten der Überwachung des Telefon- und Briefverkehrs ausgeweitet werden. (Art. 10 GG)

Hier zeigen die Erfahrungen aus dem Dritten Reich, sowie aus dem gescheiterten Versuch DDR, wozu es führt, wenn niemand seiner Leitung mehr trauen kann. So wurden z.B. im Dritten Reich Brieftauben verwendet, um Briefe zu schicken, die keiner lesen sollte (außer der dazu bestimmte Empfänger).

Unter dem Eindruck des „Rechtsrutsches“ in der BRD wurde der Etat für den Verfassungsschutz beibehalten, eigentlich sollte er gesenkt werden. Ebenso soll versucht werden, mit einer erhöhten Präsenz den Mitmenschen ein höheres Sicherheitsgefühl zu geben. Ebenso soll versucht werden, durch eine höhere Strafandrohung Menschen davon abzuhalten, anderen Menschen einen Krankenhausaufenthalt zu vermitteln. Leider ist die erstere Gruppe meistens nach rechtsstaatlichen Verhältnissen nicht ganz schuldfähig, weil angetrunken.

Diesem Paket stehen die Parteien je nach Couleur entweder positiv mit leichten Abstufungen (CDU, FDP, SPD) und negativ (B'90/GAL, PDS) gegenüber. Einig sind sie sich nur darin, daß dies nicht das einzige ist, was gegen die Problematik der Kriminalität getan werden muß. Ebenso propagieren sie auch soziale/zwischenmenschliche Lö-

sungsansätze (Arbeit, Rückkehr zu den Werten der Menschlichkeit).

Um nun auch jeden Menschen anhand seiner Fingerabdrücke erkennen zu können, wurde ein großer Teil der 118(!) neuen Planstellen beim Bunten Krimi Amt für das Automatische Fingerabdruck Identifikationssystem (AFIS) verwendet. Hier soll es drei Ausbaustufen geben:

1. Flüchtlinge (deren Zahl im Vergleich zum 1. Halbjahr 1993 um 161.297 Menschen (72%) auf 62.802 Menschen sank),
2. die "organisierte Kriminalität",
3. wer auch immer (ein Zielobjekt findet mensch immer)

Wie schützt mensch sich vor dem Ausgespäht-Werden?

### Fenster

Viele Wohnungen heutzutage haben Thermopensescheiben, bei älteren Häusern sieht mensch häufiger Kastenfenster (zwei Fenster hintereinander). Erstens haben diese einen noch höheren Isolierungsgrad als Thermopensescheiben, zweitens kann mensch in den Raum zwischen diese beiden Fenster eine Schallquelle einbauen, hierdurch wird ein Abhören erschwert, wenn nicht sogar unmöglich gemacht.

Alte Scheiben gibt es dort, wo neue eingebaut werden - Tip: Fenster ausmessen, wenn die entsprechenden Fenster irgendwo rumliegen die Handwerker fragen, ob mensch den Kram nachher mitnehmen kann - im allgemeinen sind sie froh darüber, den Kram nicht entsorgen zu müssen.

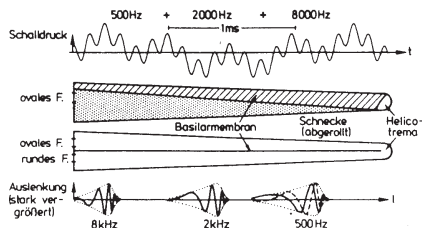
### Wanzen in der Wohnung

Wanzen strahlen HF ab, diese kann mensch messen, Baupläne über diese Thematik gibt es in der entsprechenden Literatur, bei der entsprechenden Nachfrage veröffentlichen wir auch einen. Die Geräte werden in einem Raum in der Umgebung eingestellt, den mensch als sicher empfindet (Nachbar WG) und dann wird der Bereich überprüft, der einem unsicher erscheint. Zu achten ist darauf, daß eventuell verwendete Computer auch HF abstrahlen, deshalb ist es besser, diese auszuschalten. Tip: Auch mit Geräuschen aufpassen,

einige von den Dingen haben eine Sprachsteuerung, hier sollte der Raum einmal ohne und einmal mit getestet werden. In der eher wissenschaftlichen Literatur findet mensch dann auch die Möglichkeiten, wie er/sie diese dann auch aufspürt.

### Verwante(s) Telefon(-Leitung)

Im Prinzip sehr schwierig, siehe auch Punkt "Sprachverschlüsselung" weiter unten. Falls das Signal nicht induktiv (über eine Spule) abgenommen wird, so kann mensch es mit regelmäßigen Messungen von Impedanz (Leitungswiderstand) und Spannungen probieren. Wenn sich was ändert, ist auch was mit der Leitung passiert.



Tendentuell gibt es aber hier Möglichkeiten, die Sprache zu verschlüsseln, dies soll aber auch im Zuge der "elektronischen Beweissicherung" verboten werden. Grundsätzlich gibt es hier verschiedene Verfahren, so kann mensch z.B. die Sprache in ihr Frequenzspektrum zerlegen, die Komponenten nach Schlüssel X verwürfeln, und auf der anderen Seite diese Komponenten wieder in die richtige Reihenfolge bringen, und hieraus wieder die Sprache zurückgewinnen. Einfachere Systeme zerlegen dann nur die Sätze in einige Teile und verwürfeln diese.

Die Digitaltechnik bietet noch weitere Varianten. Empfehlenswert wäre es, sich Unterlagen über den CELP-Standard zu besorgen. Ebenso sollte mensch über die Wirkung eines Tiefpasses in der Telefonleitung nachdenken, da ein Gabelumschalter im Endeffekt auch nur ein Kondensator ist, welcher die Eigenschaft hat, seinen Widerstand frequenzabhängig zu verändern.

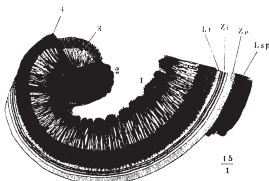
**Mailboxen**

1989 wurde der Art. 10 GG auch auf Mailboxen ausgedehnt, so werden dann Betreiber von kommerziellen Systemen dazu angehalten, den entsprechenden Behörden auf Anfrage Technik und KnowHow zur Verfügung zu stellen, um die Mailfächer der Benutzer zugänglich zu machen. Hier kann jeder nur selbstständig wirken, indem er bei privaten Mailings selber verschlüsselt. PGP hat sich hierbei als eine Art "internationaler Standard" durchgesetzt. Problematik hierbei: Wenn jemand sonst nur unverschlüsselte Mail bekommt, und da auf einmal etwas verschlüsselt drunter ist, so zeigt dies auch schon, daß etwas "im Busch ist".

Tendentuell sind aber auch die Gründe für den Anstieg einer Gefährdung zu erforschen. Verschwörungstheoretiker werden jetzt dahinter eine Art Vorbereitung zum Putsch durch die Regierung sehen. Leute, die sich auch mit der Entwicklung in der EU beschäftigen, werden dies wohl eher als einen weiteren Schritt zur EU als "Festung Europa" sehen. Andere Leute werden sich Zahlen ansehen, und dieses Phänomen als eine Reaktion auf die Bedrohung durch die Kriminalität sehen.

Hier sind auch Gründe zu hinterfragen, woraus Kriminalität entsteht, zum einem lehrte uns mal ein Herr Marx aus dem Unterschied zwischen dem was mensch hat, und dem was mensch will. Zum anderen sind Gründe, die im direkten Zusammenhang mit Arbeitsmarkt- und Wohnraumlage sowie gesamter Lebensperspektive stehen zu finden. Wieder andere werden die Gründe in der Beziehung zwischen den Menschen untereinander suchen. Auch hier gibt es einige Möglichkeiten mehr zu tun, als alle vier Jahre den Schummelzettel auszufüllen.

rowue



**Eine Begegnung der dritten Art**

Eine Zusammenfassung eines Gesprächs des CCC mit der Firma IBM im Hamburger Fernsehturm.

Die Fragen der IBM, "Wie ist die Showcase CD geknackt worden?", "Wird der CCC den Crack der Showcase CD veröffentlichen?", "Was wird der CCC in bezug auf weitere CDs der IBM unternehmen?", zeigten, wie wenig die IBM über die Motive und den Antrieb des Chaos Computer Club wirklich weiß. Allein die erste Frage – als rein technische – steht gut dar.

Die Antworten auf die zwei weiteren Fragen sollte eigentlich jedem klar sein. Nein und Nichts. Beziehungsweise "das kommt darauf an.". Und so wurde das Gespräch eine Diskussion über Motive, gesellschaftliche Zusammenhänge, Ursachen und die Bekämpfung von Symptomen.

Das Titelblatt dieser Datenschleuder wird viele an eine Anzeigenkampagne der IBM "Die besten Hacker sitzen nicht im Kasten, sondern bei der IBM" erinnern. Soll es auch. Wer Betriebssysteme für den Netzwerkeinsatz mit Sicherheitslöchern (Löchern? Da kann man eine Boing 747 durchschieben und keiner hat was gesehen!) in zweistelliger Zahl ausliefert, sollte so etwas nicht von sich behaupten.

Aber solange Hacker nicht für Vertriebskonzepte zuständig sind, werden wohl noch eine Menge Firmen versuchen, das längst gescheiterte Vertriebskonzept "Verschlüsselte Programme zum Freischalten auf CD" auf ihre Weise umzusetzen. Wir jedoch behaupten, Verschlüsselung ist Freiheitsberaubung und Demoprogramme mit eingeschränkten Funktionen entsprechen dem Tatbestand der Körperverletzung. Sechzig Tage währende Testversionen in voller Funktion mit anschließender möglicher Freischaltung ohne Neuinstallation ist das Minimum.

Letztendlich aber muß die Gesellschaft eine Bewußtseinerweiterung erfahren, um die "Raubkopie" als solche überflüssig zu machen. Daß der Staat nicht in der Lage ist, dies zu fördern, haben



die noch nicht begriffen, die sich für eine Kriminalisierung des einzelnen per Gesetz aussprechen. Also muß mensch die Sache selbst in die Hände nehmen - und woraus bestehen auch multinationalale Konzerne, wenn nicht aus Menschen, die lernen können?

Ls 141

## The SAP Trouble A Message To Novell

What is Novell's SAP? SAP stands for Server Advertise Protocol. If you have a server program (perhaps a database like BTRIEVE) you may want client to automatically find this service on your network. A protocol that helps you is the SAP protocol from Novell. It acts as follows:

Every service on the network broadcasts once the minute an IPX packet on the network that has a specific IPX socket number. The socket number is 0x0452. The packet data provides information as follows:

- node ID (Ethernet address)
- network number (IPX network)
- network hops
- name-of-service (48 char unique)
- type-of-service (2 Bytes unique, numbers from 0x0-0x8000 are owned by Novell the others are for other companys, you can apply a number from Novell for your own service at no cost)

Every Novell server catches these information. These information is written out to the Bindery and stored into server memory because it's routing information and that must be fast to get. The information is deleted after a period of 3 minutes if there is no new broadcast of the same packet. If a client wants to have a service he sends a request packet to the next server and the server replys the information under which address the service exists

Now you would say: "What is this guy telling us? We already know this! It is well-proven and running. There is no disgrace!"

You are not right, there is a disgrace! A big one that can crash down your server.

What do you think would happen if you have a program that broadcasts its service announcement packet not once the minute, but continuously as fast as it is possible? Not much. But what would happen if this program always produces new service names or service IDs with every new packet? The server stores all these new services into its Bindery. It will need more and more memory for storing the services because this is routing info and routing info must be fast. The server will allocate more and more memory from the cache buffers since there is no more main memory.

After some time the server has spend ALL of his available memory to store the SAP-info. From this point on you can't login because the login command needs memory and there is no more memory available. You have no longer access to files because this needs memory. You can't look on the packet traffic using the monitor.nlm because this window needs memory. You can't open the router tracking window (say "TRACK ON" on the console) to see what's happening because there is no memory.

The SAP-Broadcasts consumes ALL of the server's memory.

Nothing else as storing AND FORWARDING of SAP-Packets will happen on the server. You can no longer login or query files!

Your server perhaps will crash down if you have loaded NLMs that must have some memory in order to work fine.

If you stop the broadcasts your server will wipeout the SAP infos after a another 3 minutes because they won't be refreshed. Now you will get memory to work as before. On a 3.X server the memory taken from the disc cache won't be given back. It is unused server memory. You will have to shut down and reboot if you don't want a slow Server.

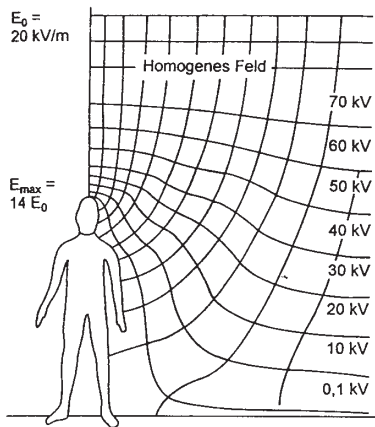


On a 4.X Server the memory will be given back to the disk cache (they have a better memory policy).

You might say that you never will start a NLM containing a database or so that does this. But who said that only servers could produce SAP-Pak-kets?

Every workstation could advertise a service that is stored by the Server because that is its business. Services could reside on workstations too. You can advertise a service and the NetWare server stores it.

So every Workstation on the Net can produce the SAP overflows. You only need the IPX protocol stack being loaded (as playing DOOM on the Net) and a small program as shown below and you can produce a lot of trouble to your supervisor. Imagine what happens on great networks in companys or universities!



Every SAP Packet that is stored by the server will be broadcasted by this server to all other servers to establish the new service. The whole network will be infected.

This would not happen if you have a SAP filter NLM. But Novell only sells this NLM with his Multi-Protocol-Router. As I know it works only as filter to the WAN-Side. Every SAP packet will be

stored on the server as before but probably is not forwarded to the WAN links.

The only chance I see is to have universal packet filters in source that links between the network adapter and perhaps the LSL to filter those pakkets. You must have this as source to make NLMs that specifically meets your needs, because you must write a new one for every form of SAP or RIP abuse.

I have reported this problem to Novell. But they only say: "Well this might be a problem. The only way is to prevent the users to start a program that produces SAP broadcasts". Well, nice try! But this is not a solution!!! Every user who doesn't like me or want to see me work can start such a program and ruin my servers.

**THE SOLUTION MUST BE PROVIDED BY NOVELL AND IT MUST COME FAAAAAASSSST!!!!**

If you don't believe me try out the little program printed below. I've found a program like below in a little BBS were everyone could download it. After I've found out what it does I had to publish it. I've chosen this way to publish the problem because I haven't received ANY reaction from Novell that REALLY helped me.

If you are a USER PLEASE tell your SUPERVISOR about this. Tell him that he has to have a filter NLM loaded. Tell him to talk to Novell for applying one. Novell has to upload one in source in this area so everyone could modify it to meet his needs as filtering out packets so that only 1000 Packets per minutes are given to the server or specific workstations that are not secure are filtered out and so on....

If you have the Client SDK a program that produces this overflow may look like this:

```
#include <stdio.h>
#include <sap.h>
#define NWWIN

main()
{
    char string[20];
    int i;
    long l;
```



```

i = 1 = 0L;
do {
    sprintf(string,"SLOW%081X", 1);
    AdvertiseService(0x2342,string, &i);
    l++;
} while (42);
}

```

Don't blame me for publishing this. Blame Novell for not doing ANYTHING against this.

## Urheberrechtsgesetzpraxis und Computerkriminelle

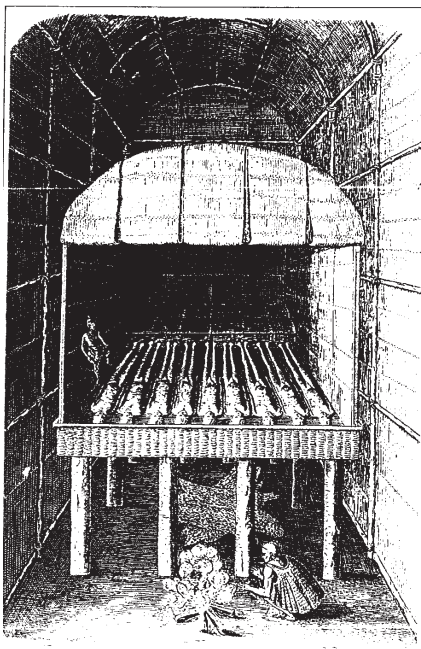
Vielen werden die Methoden des Herrn Gravenreuth durch Presse, Funk und Fernsehen bekannt sein. Wer in Computermagazinen beispielsweise Shareware oder Computer zusammen mit Software zum Verkauf inseriert, dem kann es passieren, daß er Post bekommt von einer minderjährigen Computerbegeisterten, die Software tauschen möchte und auch noch dieses und jenes Spiel sucht, in Kinderschrift natürlich.

Schickt der unwissende Sünder nun eines der angefragten Spiele an dieses Kind, bekommt er kein Dankeschreiben der Beschickten, sondern einige Wochen später eine saftige Abmahnung des Münchner Urheberrechtsanwalts Gravenreuth & Partner, die Aufforderung eine Unterlassungserklärung zu unterschreiben und eine Kostenaufstellung über rund 2500,- DM. Wobei sich die Anzahl der Unterlassungserklärungen und der zu zahlenden 2500,- Markseinheiten beliebig multiplizieren kann, je nach Anzahl der betroffenen Urheberrechtsinhaber (Softwarefirmen), für die Herr Gravenreuth eine Vollmacht vorweisen kann.

Im Extremfall kommt da eine Existenzgrundlage zusammen. Der Anwaltsargumentation zufolge sei dies zwar schmerzlich für den Betroffenen, aber ein gewisser Lerneffekt bleibt eben auch nicht aus, und darum ginge es. Die geläufige Methode des illegalen Softwarehandels ist der Kleinanzeigen-Handel allerdings nicht. Professionell wird so was in sogenannten "Trader-Mailboxen" betrieben. Hier kann der zugelassene User, und dies wird er gegen Entgelt oder durch das Selbst-

Einspielen nicht-lizenzierter Software, allerlei Software downloaden.

Bekannt ist, daß, wenn dem Münchner Anwalt eine solche Trader-Mailbox bekannt ist, und ein hinreichender Verdacht bzw. ein Beweis für den Verstoß gegen das Urheberrechtsgesetz vorliegt, diese sehr bald und meistens in aller Frühe Besuch von der Polizei bekommt. Manchmal wird auch ein MEK um Hilfe gebeten, wenn Hinweise für Vorbereitungen zur Beweismittelvernichtung vorliegen.



Mitte 1993 begab es sich, daß Hinweise sich dahingehend verdichteten, daß der – durch Verkauf von Hacker-Tricks an zahlungskräftige Kundschaft im Kriminellen-Milieu und an Fernseher – in der Hackerszene wenig beliebte "Kimble" in München eine solche "Trader-Box" betrieb, wo munter allerlei Urheberrechtsverstößen, dem Handel mit "Calling-Cards" und anderen Sachen nachgegangen wurde. Auf diesen

Fall bei einer Zusammenkunft mit CCC'ern hingewiesen, erinnerte sich Herr Gravenreuth zunächst an seinen letzten Urlaub, Höhenluft sei ja so gesund und überhaupt. Mit etwas Nachdruck gefragt, fiel der Vergleich zu Kleinanzeigen. Auch hier gebe es ja Anbieter nichtlizensierter Software, die Ärger mit der Polizei bekommen würden, und andere eben nicht.

Das erklärte natürlich auch, warum die Accounts in Kimbles BBS "voice validated" per Telefonanruf auf Angabe der richtigen Rufnummer überprüft waren. Eine amtliche Adressensammlung. "Amtlich" auch im Zusammenhang gesehen mit Kimbles Zusammenarbeit mit einem Herrn Pohl, Betreiber des in Hannover ansässigen Instituts für Informationssicherheit.

Herr Pohl ist schon einige Jahre vorher in der Hackerszene bekannt geworden, und zwar als Leiter der Abteilung des Verfassungsschutzes, die mit den "KGB-Hackern" befaßt war. Jetzt ist er "ehemaliger" Mitarbeiter des Verfassungsschutzes, was das auch immer bei einem Geheimdienst heißt. Dieser hatte irgendwann die brillante Idee, durch Kimble einen "anonymen Fragebogen" in einige Phreaker-Mailboxen zu senden. "Ganz anonym" sollte hier angegeben werden, was man denn so mache und überhaupt.

Zur CeBIT-Zeit, Mitte März, gab es dann mal wieder Schlagzeilen: die Staatsanwaltschaft in Deggendorf (Bayern) machte von sich reden, als sie in Zusammenarbeit mit dem LKA München zeitgleich 60 Hausdurchsuchungen und einige Verhaftungen im gesamten Bundesgebiet vornahm. Tatvorwurf: Handel mit "Blue-Boxes und Calling-Card-Codes".

Unter den Verhafteten: "ein 20jähriger Computerhändler ... der in der Szene unter dem Pseudonym 'Kimble' bekannt ist", sowie einen 22jährigen, "der ebenfalls als 'zentrale Figur' des Hackerkreises gilt".

Wer jetzt allerdings glaubte, daß diesen Computerkriminellen jetzt erst einmal die Möglichkeit verbaut wurde, den Begriff Hacker in Deutschland weiterhin in Verruf zu bringen, wurde bald

eines Besseren belehrt. Der inhaftierte "Kimble" war einer der ersten, die wieder auf freien Fuß gelassen wurden. Von Anfang an bestand ja der Verdacht, es habe sich nur um eine Schutzverhaftung gehandelt, um die Konspirativität nicht zu gefährden (à la Klaus Steinmetz).

Staatlicherseits gab es Stellungnahmen, die den Eindruck aufkommen ließen, die Gruppe würde unter dem Kapitel "organisierte Kriminalität" behandelt. Irgendwann im Laufe des Jahres wurde er dann mal wieder kurzzeitig verhaftet, nunmehr als Bandenoberhaupt einer Calling-Card-Verkaufs-Bande behandelt, aber auch das hielt nicht lange an.

Allerdings sind wohl allerlei Kimble bekannte Leute von ihm belastet worden, sie wären die "wahren" Banden-Häuptlinge (was für staatliche Stellen natürlich ungemünzt die Arbeit erleichtert, herauszufinden wer denn sonst noch so in dieser Szene hängt).

Soweit, so schlecht. Unabhängig von diesem Mammut-Ermittlungsverfahren gab es dann im Sommer noch eine größere Anzahl von Hausdurchsuchungen und Beschlagnahmungen von Mailboxen; der immergleiche Vorwurf: illegaler Handel mit urheberrechtlich geschützten Programmen.

Als hinreichender "Beweis" für diesen Straftatbestand, bzw. als Begründung für eine Hausdurchsuchung zwecks Auffindens von Beweismitteln, reicht den entsprechenden Staatsanwälten ein einfacher Protokoll-Ausdruck aus einer Mailbox, wo z.B. der Systembetreiber in einem Chat zugibt mit Software zu handeln. Vorrausgesetzt, ein solcher Protokoll-Ausdruck kommt aus seriöser Hand.

So etwas zu fälschen, das weiß jeder Benutzer einer Textverarbeitung, ist kein Problem. Der andere Punkt, daß jeder Computerbenutzer de facto meist auch ein Straftäter bzw. ein Besitzer nichtlizensierter Software ist, ist auch allen klar. Und um daraus einen kausalen Zusammenhang zu bilden, muß man eigentlich nur noch wissen, daß es natürlich bezahlte "Testkäufer" und andere Zuar-

beiter (oder sollte man "Menschenjäger" sagen?) der Gravenreuth'schen Anwaltskanzlei gibt.

Braucht man eigentlich nur noch die Telefonnummern von entsprechenden Mailboxen, die Namen der Betreiber etc. - aber an so etwas ranzukommen ist ja kein Problem, wenn man selbst so eine Mailbox betreibt.

In unserem Fortsetzungskrimi über Münchner Urheberrechtsanwälte, die Zusammenarbeit mit dem Verfassungsschutz und den Einsatz von "agents provocateurs" in der Hackerszene, lesen Sie in der nächsten Folge: wie der Agent mit Hilfe des Anwalts eine "Sneakers-Firma" aufbaut, wer davon profitiert, und was die Lufthansa damit zu tun hat. Stichwort: Data Protect GmbH.

Ls16

## Der Chaos Computer Club und die Datenautobahnen

"Was heute noch wie ein Märchen klingt, kann morgen Wirklichkeit sein. Hier ist ein Märchen von Übermorgen. Es gibt keine Kupferkabel mehr. Es gibt nur noch Glasfaser und Terminals in jedem Raum. Man siedelt auf fernen Rechnern. Die Mailboxen sind als Wohnraum erschlossen. Mit heute noch unvorstellbaren Geschwindigkeiten durchheilen Computer-Clubs unser Datenverbundsystem. Einer dieser Computer Clubs ist der Chaos Computer Club – gigantischer Teil eines winzigen Sicherheitssystems, das die Erde vor der Bedrohung durch den Gilb schützen soll. Begleiten wir den CCC und seine Mitglieder bei ihrem Patrouillendienst am Rande der Unkenntlichkeit."

Aus der Ankündigung des Chaos Communication Congress 1984:

Der Chaos Computer Club, gegründet 1981, seit 1984 Herausgeber der Zeitschrift "Datenschleuder" (dem wissenschaftlichen Fachblatt für Datenreisende) und Veranstalter des Chaos Communication Congress, etwa zur Zeit der Einführ-

ung des "2. Wirtschaftskriminalitätsgesetzes" (1986) zum eingetragenen Verein mutiert, hat sich sehr früh bereits für grenzüberschreitende Informationsfreiheit, ein neues Menschenrecht auf weltweite ungehinderte Kommunikation und ähnliches in diesem Sinne eingesetzt.

Bei der in den frühen 80ern noch sehr jungen Datfernübertragung mit Telefonmodems wurden schnell Erfahrungen mit den Telekommunikationsmonopolisten, zu deutsch dem Gilb (der Post) und anderen, den freien Kommunikationsfluß behindernden Instanzen gewonnen, etwa unter dem Stichwort Gebühren. Nach verschiedenen Gesetzesnovellierungen im Jahre 1986 entschied man sich alternativ zur Möglichkeit des §129a, einen eingetragenen Verein zu gründen, um so rechtliche Fragen besser kanalisieren zu können und den CCC als eine Art Forum für die Hackerszene zu betreiben.

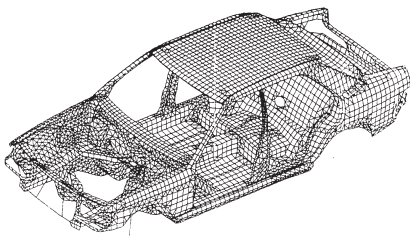
In diesem Sinne ist der CCC ein Vermittler zwischen Hackern, Systembetreibern, gesetzlichen Instanzen und vor allem der Öffentlichkeit, der die Beobachtungen und Ideen der Hackerszene vertritt.

Auf den jährlich zwischen Weihnachten und Neujahr stattfindenden Chaos Communication Congressen findet neben der Diskussion und Umsetzung inhaltlicher und technischer Gestaltung von Kommunikationssystemen eine intensive Auseinandersetzung mit rechtlichen Problemen, etwa der presserechtlichen Verantwortlichkeit einer Mailbox bzw. ihres Betreibers statt, mit der Formulierungen wie "Erbringer einer Telekommunikationsdienstleistung für andere" in ihrer Konsequenz beleuchtet werden.

"Per Anhalter durch die Netze" war das Motto des Chaos Communication Congress 1988, zeitgemäß wäre vielleicht "Trampen auf der Infobahn". Doch bei der jetzigen Diskussion um die Breitbandnetze stellen sich Hacker nicht nur die Frage nach der eigenen Rolle auf den zukünftigen Datenautobahnen, sondern auch und vor allem nach der inhaltlichen Gestaltung, geprägt durch rund 10 Jahre Erfahrungen mit diesem Medium. Genauso wie die Hacker die selbst aufgebauten und betriebenen

Netze mit ihren Diskussionsforen, Newsgroups, Chat-Kanälen, dem verschlüsselten persönlichen Nachrichtenaustausch etc. bei der Einführung der allgemeinen und jeden Haushalt erreichenden Datennetze auf genau diesen Bereich ausdehnen und weiterentwickeln möchten, um IHRE Vision vom "globalen Dorf" zu verwirklichen, verstärken die konventionellen Medienproduzenten wohl ihre jetzigen Strukturen der kommerzialisierten, einseitigen Medien.

Denn – verglichen mit dem jetzigen Medium Internet als kommerzfreie Zone (keine Werbung, Finanzierung der Infrastruktur über die Nutzer bzw. Systembetreiber) – bietet, bedingt durch die Kommerzialisierung der Sender, ein Medium wie das Fernsehen etwa für einen Hacker wenig authentische Information. Mit authentischer Information meine ich hierbei eine nicht zum Einwegprodukt geronnene und an Einschaltquoten orientierte, sondern z.B. eine aus der Beobachtung eines x-beliebigen Subjekts resultierende, als persönlicher Eindruck formulierte Information, die dadurch einen Wahrheitsgehalt hat, daß sie hinterfragt und kommentiert werden kann, kurz: eine interaktive Information.



So groß das Bemühen der Produzenten einer Nachrichtensendung beispielsweise sein mag: die schlichte und einseitige Übermittlung ist abstrakt. Im Fernsehen ist das World-Trade-Center so groß wie eine Packung Butterkekse, Kriegsbilder bewegen sich in der Dimension eines Haufens dreckigen Geschirrs, und Filme über Umweltprobleme erinnern an lange nicht gewaschene Scheiben. Hierdurch, und durch die Einseitigkeit dieses Mediums, wird beim Fernsehen nicht in erster Linie begriffen, sondern konsumiert.

Und ernährt damit einen ganzen Industriezweig, wenn nicht ein ganzes Wirtschaftssystem. Wenn Repräsentanten dieser Medien an Veranstaltungen wie der des WZB teilnehmen, und unter dem Stichwort "interaktives Fernsehen" beispielsweise neben der Buy-Taste an der Fernbedienung, die den Kauf des Produktes bei Betrachtung des Werbespots ermöglicht, gerade noch Video- & Sex-on-Demand und ähnliche Dienstleistungen (Hacker-spott: "Glasfaser bis in die Brieftaschen") präsentieren, stößt das bei mir nicht nur auf Ablehnung wegen der Phantasielosigkeit sondern auch wegen der verpaßten Chancen des neuen Mediums.

Außerdem: wer übernimmt die Verantwortung für eine Gesellschaft, deren Mitglieder in standardisierten virtuellen Welten leben, in denen es so etwas wie "primäre kollektive Erfahrungen ("Erlebtes" statt "Imaginiertes") vielleicht immer weniger gibt. Vermutlich wird es möglich sein, Weltkriege und allerlei Umweltprobleme zu verpassen, weil sie nicht mit dem persönlichen Interessensprofil kompatibel waren. Um jedoch eine Situation zu vermeiden, die einem mit der Meldung "Bitte neuen Planeten in Laufwerk A: einlegen und anschließend eine beliebige Taste drücken" begegnen könnte, bedarf es eines Abgleiches zwischen virtuellen und nicht-virtuellen Realitäten.

Den Gestaltern und Interessierten an dieser Entwicklung seien aber nicht nur diese Bedenken, sondern vor allem die Auseinandersetzung mit den existierenden Computernetzwerken empfohlen. Abgesehen von Phantasieanregendem erhoffe ich mir dadurch mehr Respekt vor den "gewachsenen" Informationsstrukturen, deren Vielseitigkeit durch eine etwaige Kommerzialisierung bedroht wäre. Eine Entwicklung zu einer Gesellschaft, in der das elementare menschliche Bedürfnis nach Kommunikation durch Geldbarrieren beschnitten wird (Kommerzialisierung der Kommunikationswege), produziert nicht nur Verblödung und Gewaltbereitschaft, sondern ist auch zutiefst undemokratisch.

Dieser Text ist für die Broschüre des Wissenschaftszentrums Berlin (WZB) geschrieben, in der die Veranstaltungsteilnehmer etwas zu ihrer Position schreiben sollten (siehe auch nachstehenden Artikel über die Veranstaltung selbst).

Andy M.-M. Hamburg/Berlin

## Datennetze der Zukunft? Eine Tagung in Berlin...

Durch einen CeBIT-Kontakt ergab es sich, daß zwei CCC'ler nach Berlin geladen wurden, um an einer Tagung des Wissenschaftszentrums Berlin über die Datennetze der Zukunft teilzunehmen, neben "visionären" Bertelsmännern (Fazit: dieses Medium erlaubt es jedem, seinen Verlag aufzumachen), ratlosen Technikern ("wir haben es entwickelt, nutzt es doch bitte") und realitätsfremden PostsubGmbH'lern gab es auch noch einige witzige Aspekte, wie z.B. einen Siemensphilosophen, der hier lieber Stätten des Wissens mit Interdisziplinären Markthallen schaffen möchte, in denen sich mensch über Probleme und deren Lösungen austauscht, anstelle die 500 Kanäle Fernsehen zu konsumieren, und dabei zu vergessen, was Leben ist.

Ebenso hart waren die Prognosen über die Stadtentwicklung Berlins des Projektes "Metropole" der Telekom, Entwohnung des Stadtkerns aufgrund der Mietpreissteigerung, dabei mit Flip-Chart aufzeigend, daß demnächst ca. 2 Millionen Menschen ihren Wohnort wechseln müssen, soziales Umfeld und, wenn vorhanden, Arbeitsplatz ebenso.

Fazit: interessante Veranstaltung, die Datennetze werden sich, trotz der sozialen Probleme, durchsetzen, mitgestalten ist besser als Ausbuhen. So hat mensch noch die Chance etwas besseres als den 499. Soft-Porno zu sehen. Ähnlicher Ansatz: Kanal 4 auf RTL oder Sat1, eingekaufte Teilhaberschaft sichert Sendezeit, hier Kunst, Satire, Aufklärung in Vergangenheit und Gegenwart.

rowue

## Anzeige

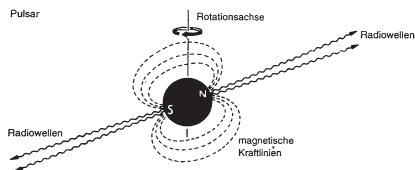
### Bausätze und Kompletteräte

Aus den diversen Anfragen und Bitten heraus hat sich einer unser Mitarbeiter entschlossen, privat den Dienst des Bausatz/Fertigerät-Versendens anzubieten, als Einstig gibt es den POCSAC-Decoder (Version 1.2) als Bausatz für DM 30,- und für DM 60,- als Fertigerät (ohne Gehäuse).

Bausatz und Fertigeräte sind erhältlich bei:

rowue Datentechnik  
c/o Rolf Würdemann  
Annenstr. 31  
20359 Hamburg

Bestellung über Vorkasse (bar oder Überweisung) auf Konto 1015/849449 Haspa (200 505 50), Rolf Würdemann. 25% des Gewinns gehen an den CCC. Das Abhören von Cityruf-Mitteilungen ist ein nicht genehmigter Eingriff in den Fernmeldeverkehr und somit strafbar.



Achja: Version 1.2: Schmitt-Trigger (LS14), Spannungsteiler mit Poti und Widerstand (100K, 68K), Gleichspannung ohne Signal am Eingang auf 1,2V einstellen, Kondi mit 0,1µF vorsetzen, Ausgang auf nächsten Eingang, davon Ausgang auf MAX 232, Signal rein, und ab dafür. Einfach aufzubauen, einfach einzustellen, der Rubel rollt, die Wanne quirlt. Software siehe Bestellfzetzen oder DS 41, Radio siehe einschlägigen Radiohandel, gesamt siehe DS 35, 36 und 41.

rowue

## Adressen

### CCC-HH – CCC Hamburg

Treff jeden Dienstag ab 20 Uhr in den Clubräumen.  
Danach meistens Fleischdröhnung bei Costa. Adresse  
siehe Impressum.

### CHAOS-B - CCC Berlin

Treffen jeden Dienstag ab 20 Uhr in der Kronenstr. 3,  
Berliner-Mitte (U6/2-Station Stadtmitte) im dritten  
Stock (über dem Friseur). Fax c/o Botschaft +49 (30)  
2292429 (eigene beantragt). Briefpost: CCC, Kronen-  
straße 3, D-10117 Berlin.

### CHAOS-HL - CCC Lübeck

Treff am ersten und dritten Freitag im Monat, 19 Uhr in  
der Röhre (gerade Querstraße, geht von der Meng-  
straße ab). Briefpost: CCC-HL, c/o Benno Fischer, Bu-  
genhagenstr. 7, D-23568 Lübeck, Voice +49 (451)  
34799, Mailbox Mafia +49 (451) 31642.

### CCC-Ulm - Treffen jeden Mittwoch, 19 Uhr im Café "Einstein"

### SUECRATES - Stuttgarter Computerrunde mit Zeit- schrift d'Hacketse

Kontakt: T.Schuster, Im Feuerhapt 19, D-70794 Fil-  
derstadt, e-mail: norman@delos.stgt.sub.org

### 2600 Magazine - Amerikanische Hackerzeitschrift

Overseas \$30 individual, \$65 corporate. Back issues  
available for 1984-88 at \$25 per year, \$30 per year  
overseas. Adress all subscription correspondence to:  
2600 Subscription Dept., P.O. Box 752, Middle Island,  
NY 11953-0099. Office Line: +1 (516) 751-2600, Fax  
+1 (516) 751-2608

### Hack-Tic - Niederländische Hackerzeitschrift.

Hack-Tic, Postbus 22953, NL-1100 DI Amsterdam, Tel  
+31 (20) 6001480, Fax +31 (20) 6900968

### Foebud-BI - Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V., Bielefeld

Treffen jeden Dienstag, 19:30 Uhr im Cafe "Spin-  
nererei", Heeperstrasse 64, dort voice: +49 (521) 62339  
Monatliche "Public Domain"-Veranstaltung zu  
Themen aus Randbereichen der Computerkultur jew.  
am 1. Sonntag im Monat (außer Januar, Juli und Au-  
gust) ab 15 Uhr, im Bunker Ulmenwall, Kreuzstraße 0,  
D-33602 Bielefeld. Termine siehe Mailbox BIONIC.  
Voice: +49 (521) 175254, Fax +49 (521) 61172, Mail-  
box BIONIC +49 (521) 68000. FoeBuD, Marktstraße  
18, D-33602 Bielefeld, e-mail: ZENTRALE@BION-  
IC.ZER / zentrale@bionic.zer.de

## Impressum

### Die Datenschleuder Das wissenschaftliche Fachblatt für Datenreisende

#### Nummer 48, Quartal III, September 1994

**Adresse:** Die Datenschleuder, Schwenckestr. 85,  
D-20255 Hamburg, Tel +49 (40) 4903757, Voice-  
Mailbox +49 (40) 497273 (Tonwahl erforderlich),  
Fax +49 (40) 4917689, BBS +49 (40) 4911085  
(chaos-hh.zer), Internet: ccc@t42.ccc.de,  
Mailserver: ccc-serv@mail.ccc.de, Datex-J:  
\*CCC#

**Redaktion:** (A)ndy, cash, Hacko, Rowue, Bar-  
bara, Alf, Tim

**ViSdPg:** Rolf Würdemann

**Herausgeber:** Chaos Computer Club e.V.

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

Namentlich gekennzeichnete Beiträge geben nicht  
unbedingt die Meinung der Redaktion wieder.

Einzelpreis 3,50 DM. Mitglieder des Chaos Com-  
puter Club e.V. erhalten die Datenschleuder im  
Rahmen ihrer Mitgliedschaft. Abopreise siehe Be-  
stellfetzen.

Adressänderungen von Abonnenten am besten  
schriftlich (Postkarte genügt).

© Copyright 1994: Alle Rechte bei den AutorIn-  
nen. Kontakt über die Redaktion. Nachdruck für  
nichtgewerbliche Zwecke mit Quellenangabe er-  
laubt. Belegexemplar erbeten.

**Eigentumsvorbehalt:** Diese Zeitschrift ist  
solange Eigentum des Absenders, bis sie dem Ge-  
fangenen persönlich ausgehändigt worden ist.  
Zur-Habe-Nahme ist keine persönliche Aushändi-  
gung im Sinne des Vorbehalts. Wird die Zeitschrift  
dem Gefangenen nicht ausgehändigt, so ist sie dem  
Absender mit dem Grund der Nichtaushändigung  
in Form eines rechtsmittelfähigen Bescheides  
zurückzusenden.





