Postvertriebstück
C9927F

DM 2,50

datenschleuder

Nummer 16 — September 1986

HILFE HACKER

Dieser Hilferuf hallt durch manchen Operatorraum in den Rechenzentren unserer Welt. Doch um Mißverständnissen gleich vorzubeugen: In den USA ist dieser Ruf etwas anders zu interpretieren als in diesem unserem Lande. So bedeutet "Hilfe Hacker" in der BRD eifriges Gelaufe mehr oder weniger kompetenter Personen durch verwinkelte Gänge im Rechenzentrum, faszinierte und/oder bestürzte Gesichter vor wild blinkenden Masterkonsolen, schimpfende Putzfrauen, die sich durch Berge von Printouts kämpfen und Hab-ichs-nichtgleich-gesagt Blicke frustrierter Betriebsräte, bis einer auf die Idee kommt, den 220V-Reset durchzuführen, der auch den hartnäckigsten Hacker auf die Erde zurückholt (DATEX-P: Ausloesung - Gegenstelle eingeschlafen).
In den USA werden Hacker mit etwas anderen Augen betrachtet, wurde doch der Nutzeffekt der Phreaks schon vor Jahren erkannt (Viva Cheshire !), ja, die ersten Hacker haben eine regelrechte Tellerwäscherkarriere hinter sich und leiten jetzt diejenigen Konzerne, die die ja so hackerfreundlichen Rechner der Nachfolgegeneration produzieren. In Deutschland ist so etwas momentan noch undenkbar, die liberale Denkweise scheitert wieder mal am Konservatismus. Gerade ein (Kommunikations-)Entwicklungsland wie das Unsrige sollte auch Denkanstößen aus Hackerkreisen Gehör schenken: es kann nur von Vorteil sein, denn bei uns wären Hacker noch billig zu bekommen (vgl. USA), wenn nicht umsonst, denn es zeichnet sich eine Symbiose ab: der Hacker gemäß der Philosophie "Öffnet die Netze - Dezentralisierung der Information" freut sich über jedes Passwort, der Betreiber kann seinen Rechner vor wahren Gefahren (durch Crasher, Wirtschaftkriminalität usw.) durch erfahrene Hacker schützen lassen. Nicht zu verachten der Lerneffekt, denn spielerisch lässt es sich nun einmal leichter lernen, und Bildungsförderung nimmt der Staat ja für sich in Anspruch.
In der Realität sieht es leider noch so aus: Softwaretests auf Großrechenanlagen werden von Hackern in Eigenregie durchgeführt. So konnte man das auf der CeBit vorgestellte Programmpaket ALL-IN-1 (alles eins, konzeptionell mit Lotus-1-2-3 auf Personals vergleichbar) fuer VAX-Rechner von DEC auch im praktischen Einsatz auf einem Rechner in Ottawa bewundern. Unter dem Usernamen OPF konnten die Vorzüge des Programmpaketes mit einem VT-100 Emulator und einer Datexverbindung genauestens untersucht werden. Eher zufällig stiess man bei dem inoffiziellen Softwaretest auf die Datenbankdefinition der Ottawa Police Force (eben jener ominoese OPF) für ein Rasterfahndungssystem (suspicious flag = false). Der Test fiel von Hackerseite her recht positiv aus, die Gegenstelle antwortet allerdings bis heute nicht (kommentarloser Rausschmiss). Ueberhaupt zeigen sich Rechnerhersteller recht unkooperativ gegenüber Hackern, zumindestens, was größere Konzerne angeht ("Wozu haben wir unsere teuer bezahlten Spezialisten"). Ein weit umhergereister Hacker beweist innerhalb von Minuten, daß das Geld fuer teure Spezialisten sinnvoller angelegt werden könnte, z.B. zur Finanzierung einer Nui für Weiterbildungszwecke (Teilnehmerkennung dBildung sehr aktiv). Datenreisen bleibt immer noch eine teure Angelegenheit, es beginnt schon bei den Postdiensten. Wir warten noch auf Billigreisen, sei es nun nach Neckermannschema ("3 Wochen Sonne im Bitnet") oder Rainbow-Tours ("2 1/2 Tage Superstimmung im Fermilab"), warum nicht öffentliche Datenbank-Telefonzellen mit Terminal und Geldeinwurf (Ortsgebühr versteht sich, und kommt mir jetzt nicht mit Blödeltext)! Es gibt noch viel zu tun in diesem unserem Lande, es sind die Hacker, die sich aufraffen und die Betreiber zum Handeln zwingen! Denn der Hilferuf soll in Zukunft nicht als "Hilfe wir haben Hacker!", sondern als "Hilfe, wir brauchen Hacker!!" interpretiert werden.

DS16HILFHACK.TXT FRIMP 29.04.1986

Impressum :
Die Datenschleuder 16, 11. Sep 1986.
·Das Wissenschaftliche Fachblatt
fuer Datenreisende
D-2000 Hamburg 20
Schwenckestrasse 85
Geonet:Geo1:Chaos-Team
Btx : *655321#

Herausgeber und ViSdPG:
Herwart Holland-Moritz

Mitarbeiter dieser Ausgabe (u.a.)
R. Schrutzki, S. Wernery, A. Eichler,
P. Franck, H. Gruel, M. Kuehn.,
Andy M.-M., S. Stahl
Eigendruck im Selbstverlag.
September 1986.

* 6 5 5 3 2 1 #

To : VMS System Managers
From : SecurityManager
Subject : Security Against Hackers

Recently, we have seen a number of occurrences of people logging in to CERN VAXs via unauthorised accounts and establishing new accounts for themselves or altering existing accounts for their own use. Last year, this happened mainly to the VXGIFT machine and on two occasions, time was lost after malicious damage was done.

Since the start of February, VXCRNA has been the main target, but not the only one; VXDEV, VXMERL, VXOMEG have been affected also. On VXCRNA, the effects have been less severe in terms of actual damage (although at least one system crash can be traced to the running of a privileged program by the intruder). However, several members of the support team have had to spend a lot of time investigating these incidents and repairing the damage and a few users have had their accounts made temporarily unavailable when the intruder(s) changed the password or when the support team suspended access to them after they had been used to enter the VAX.

We will leave aside for now the question of how such "hackers" first get access to privileged accounts in a given machine. Once they get such access, these people are very knowledgeable about VMS and they can set themselves up many other ways into the system. It has taken much effort to reach the stage where we now believe that they can do no further harm inside VXCRNA and even now, we accept that there may still be ways in which they can log in.

Who are these people and how do they access CERN. Apart from the occasional hacker who may be a user on some connected system who gets bored late at night and tries to see what he can reach and what fun he can have, there seems to be a club based in Germany called the "chaos club" whose collective hobby is hacking systems connected to public X25 networks. We have identified one member of this club in Dusseldorf and the "working alias" of a second in Berlin. We are currently investigating what steps we can take to curtail their anti-social activities.

This paper lists a few hints on how to make systems a little more secure. It must be emphasised that ALL CERN systems must be protected. The people doing this hacking are very ingenious. They know all about networks. We have seen evidence that they enter CERN via one system and use DECNET to get to their real target system. Even if all CERN systems were fully protected, it might not be enough. There would still remain two large gaps through which they might pass. One is via the CERN EXCITE network where they would log into INDEX and then connect to any VAX; the second is through a system outside CERN, for example, on INFNET and then into CERN via DECNET.

Stopping the second of these might be possible if we encourage the system managers of all systems on the network to take the same steps as described in this note with the threat that we would be obliged to close the link to any system though which an intruder tried to pass (as already happens for VXCRNA). Closing the EXCITE/INDEX gap is equally difficult since it implies closing access from a set of X25 addresses, some of which might be legitimately employed by valid CERN users.

Most of the following points are fully described in the VMS V4 System Security manual

* The most obvious first precaution is for all users to have effective passwords. Cases where username = password should be positively banned. At first sight, the only risk in having such trivial passwords would be the loss or corruption of that user's files. However, once inside the system, a VMS-knowledgeable intruder may well find other interesting possibilities. VMS is not hacker-proof, especially if some of the following items are not respected. A simple DCL command file can be used to check for such useless passwords.

However, even this rule is not sufficient. Using first names as passwords is almost equally useless; or initials; or IBM login codes. System managers should enforce minimum length passwords, say a minimum of 5 characters. In the limit, the use of password expiry times might be necessary, forcing regular changes of password. This last item, forcing password changes, might be thought to reduce the user-friendliness of VMS (as do most of the suggestions in this paper), but it would be useful to trace accounts unused for a long time; these are exactly the accounts that hackers pick on to adapt for their own use.

Where a user has some special privilege (and this should be kept to a minimum), such regular changes should be enforced and perhaps the minimum length should be longer. Apart from the obvious privileges to be careful with (SETPRV, SYS*, CMKRNL, BYPASS, OPER, etc) are DETACH and READALL. The first gives its owner the possibility to issue a RUN/UIC= command where the UIC could be a system ID! The second gives write access to all file headers, thus allowing its owner to change a file protection, for example.

* Users should NOT keep passwords in files on disc, for example to help them log in to another VAX across the network. This compromises not only the account being hacked, but the corresponding VAX also.

* Some terminals allow their owners to store character strings in memory to be activated on a single or multiple keystroke(s). Unless you can be sure that your terminal is totally secure (either in a permanently locked office or at home and out of reach of the children!!), then you should not store login sequences in the memory of your terminal.

* The BACKUP program stores the command string used to create a backup save set in the save set itself. If you use DECNET to create a backup save set and you include the username and password in the command string in the form node"username password"::... then the password will appear in clear text in the save set. We have complained to the author of BACKUP about this but

there is little chance of a solution.
* From time to time, bugs or security gaps are reported in particular versions of VMS. These should be closed as soon as a fix is available. For example, under VMS x.x, any user in the system can xxxxxxxxxxxxxxxxxxxxxxxx to the system xxxxxxxxxxxxxxx(andonother xxxxxxx xxxxxxxxx in the system). This is equivalent to the xxxxx xxxxxxxx and can lead to abuse. The published protection against this is to set the following command into the xxxxxxxxxxxxxxxxxxxxxx
$xxxxxxxxxxxxxxxxxx
$xxxxxxxxxxxxxxxxxxx
-
xxxxxxxxxxxxxxxxxx
This bug is fixed in VMS x.x.
* System managers might consider restricted access to certain privileged accounts during nights and weekends. This is easy to implement using the primary/secondary options in the authorisation file and a command file run at regular times. Accounts such as xxxxxxx and xxxxxxxxxxx should allways be disabled when not in active use and their passwords should allways be changed from the VMS default. However, does the SYSTEM account need to be open all weekend when you know it will not be needed until Monday? Perhaps such accounts should be disabled for access in NETWORK mode or from DIALUP lines. And so on.
A particular case of this is the xxxxx account. In general, xxxxxxxxxxxxx are not careful with their passwords, especially on a site with many VAXs. It is strongly suggested that xxxxx should be generally disabled unless xxxxxxxxxxxxx have been called. A trivial command file run by any privileged user (OPS or SYSTEM) could be written to enable it. If you want xxxxx xxxxxxx to be able to look at your error log without your enabling their account, they could be given a non-privileged account and access to the error log via an access control entry. While xxxxxxxxxxxxx might (will) not like this, it is standard practice in many Digital offices as well as at some user sites.
* Some files should be protected by security access control entries such that certain types of access to them are logged. Examples would be SYSUAF.DAT, VMSIMAGES.DAT, the NET*.DAT files in SYS$SYSTEM, all page, swap and dump files. All thes files have no need to have any "world" access, not even read. The RIGHTSLIST.DAT file however, does need world-read access but could have an access control entry for other types of access. Finally, any xxxxxx and xxx xxxxx xxxxx should have no world access since they may xxxxxxx xxxx xxxxxxxxx.
* Some images may be left generally accessible but installed with accounting selectively enabled so that their use is recorded. Examples here would include INSTALL, NCP, AUTHORIZE, ACCOUNTING. The aim is not to stop them being used (a clever hacker could easily get round this) but to be able to see when they are used and by whom.
* The various VMS xxxxxxxx xxxxxx should be xxxxxxx. These will log breakin attempts, changes to the authorisation file and so on. These can be linked to CERN-written programs which will, for example, kill any unauthorised process which tries to change the authorisation file, close a DECNET link which is being used to hack the system, send warning messages to a given account or accounts when such incidents occur; and so on. These programs are available from xxxxxxxxxx
* If you have xxxxxxxxxxxxxx, your system could be used as a "port of entry" for these hackers. There exists a standard xxxxxx utility called xxxxxxxxxxxx which will allow the system manager to set up a list of DTE (X25 addresses) to or from which calls are allowed or excluded; a list of users who are allowed to use X25 to gain access to or from a remote system; and a list of "objects" (programs) which are accessible via X25 for remote users. Although this might seem a little heavy - and the documentation may need to be read several times before it is understood - X25 system managers are strongly encouraged to consult the xxx documentation for more details on xxxxxxxxxxx.
* Other network products, e.g. J-NET, may have their own security gaps. We have done some simple tests on TCP/IP and EAN and found the following.

In TCP/IP, the system manager can declare server processes. It seems that TCP/IP starts such processes with whatever privilege it itself is installed with. Since this usually includes CMKRNL, your system is thus vulnerable to simple coding errors by the author of the server, without even considering the dangers of hackers! We are investigating this.
EAN has an even bigger loophole. When users register with EAN, they are asked for an EAN password. This is then stored in a file on the users account with a standard name - in clear text. Further, this file is created by EAN with world read privilege! Although users are requested to choose a different password to their VMS passwords, many use the same password. We are investigating making this file less accessible. System managers with EAN installed are invited to contact me for the name of this file.
* If you suspect that your system has been hacked, isolate the account used as soon as possible. Making it xxxxxxx is not enough since batch and network jobs can still pass. Use the xxxxxxxxx qualifier in AUTHORIZE. Also, check that the hacker has not altered other records if you suspect he had privilege. xxxxxxxxxxxx has a trivial command file to check for this. Finally, check that strange files were not created in the "attacked" account.

(Special Thanx to A.S.)

Vic. & Obi

Kinder an die Macht

"The reach of children" steht für "Gefahrenzone" bei System-Managern, die Hacken als antisoziale Tätigkeit schildern. Das widerlegt "Hilfe-Hacker" in dieser Ausgabe. "2 bis 3% offener , Kommunikation, frei und unzensiert auf allen Medien" fordert MultiMediaGruppe MinusDeltaT. Diesen Anteil haben Hacker auf den Rechnersystemen - auch auf VAXen - noch längst nicht erreicht. wau

*** Dokumentation ***

Satzung des Chaos Computer Club

Präambel

Die Informationsgesellschaft unserer Tage ist ohne Computer nicht mehr denkbar. Die Einsatzmöglichkeiten der automatisierten Datenverarbeitung und Datenübermittlung bergen Chancen, aber auch Gefahren für den Einzelnen und für die Gesellschaft. Informations-und Kommunikationstechnologien verändern das Verhältnis Mensch-Maschine und der Menschen untereinander. Die Entwicklung zur Informationsgesellschaft erfordert ein neues Menschenrecht auf weltweite ungehinderte Kommunikation.
Der Chaos Computer Club ist eine galaktische Gemeinschaft von Lebewesen, unabhängig von Alter, Geschlecht und Rasse sowie gesellschaftlicher Stellung, die sich grenzüberschreitend für Informationsfreiheit einsetzt und mit den Auswirkungen von Technologien auf die Gesellschaft sowie das einzelne Lebewesen beschäftigt und das Wissen um diese Entwicklung fördert.

§ 1 Name, Sitz, Geschäftsjahr
(1) Der Verein führt den Namen "Chaos Computer Club". Der Verein wird in das Vereinsregister eingetragen und dann um den Zusatz "e.V." ergänzt. Der Verein hat seinen Sitz in Hamburg.
(2) Das Geschäftsjahr beginnt am 1. März jeden Kalenderjahres.

§ 2 Zweck und Gemeinnützigkeit
(1) Der Club fördert und unterstützt Vorhaben der Forschung, Wissenschaft & Bildung, Erziehung, Kunst & Kultur, sowie der Völkerverständigung im Sinne der Präambel oder führt diese durch.
Der Vereinszweck soll unter anderem durch folgende Mittel erreicht werden:
1. regelmäßige öffentliche Treffen und Informationsveranstaltungen
2. Veranstaltung und/oder Förderung internationaler Congresse, Treffen, sowie Telekonferenzen
3. Herausgabe der Zeitschrift "Datenschleuder"
4. Öffentlichkeitsarbeit und Telepublishing in allen Medien
5. Arbeits- und Erfahrungsaustauschkreise
6. Informationsaustausch mit den in der Datenschutzgesetzgebung vorgesehenen Kontrollorganen
7. Hacken
8. Hilfestellung und Beratung bei technischen und rechtlichen Fragen im Rahmen der gesetzlichen Möglichkeiten für die Mitglieder
(2) Der Club ist gemeinnützig; er dient ausschließlich und unmittelbar der Volksbildung zum Nutzen der Allgemeinheit. Er darf keine Gewinne erzielen; er ist selbstlos tätig und verfolgt nicht in erster Linie eigenwirtschaftliche Zwecke. Die Mittel des Club werden ausschließlich und unmittelbar zu den satzungsgemäßen Zwecken verwendet. Die Mitglieder erhalten keine Zuwendung aus den Mitteln des Clubs. Niemand darf durch Ausgaben, die dem Zwecke des Clubs fremd sind oder durch unverhältnismäßig hohe Vergütungen begünstigt werden.

§ 3 Mitgliedschaft
(1) Ordentliche Clubmitglieder können natürliche und juristische Personen, Handelsgesellschaften, nicht rechtsfähige Vereine sowie Anstalten und Körperschaften des öffentlichen Rechts werden.
(2) Die Beitrittserklärung erfolgt schriftlich oder fernschriftlich gegenüber dem Vorstand. Über die Annahme der Beitrittserklärung entscheidet der Vorstand. Die Mitgliedschaft beginnt mit der Annahme der Beitrittserklärung.
(3) Die Mitgliedschaft endet durch Austrittserklärung, durch Tod von natürlichen Personen oder durch Auflösung und Erlöschen von juristischen Personen, Handelsgesellschaften, nicht rechtsfähigen Vereinen sowie Anstalten und Körperschaften des öffentlichen Rechtes oder durch Ausschluß; die Beitragspflicht für das laufende Geschäftsjahr bleibt hiervon unberührt.
(4) Der Austritt ist nur zum Schluß eines Geschäftsjahres zulässig; die Austrittserklärung muß spätestens drei Monate vor Ablauf des Geschäftsjahres gegenüber dem Vorstand schriftlich abgegeben werden.
(5) Die Mitgliederversammlung kann solche Personen, die sich besondere Verdienste um den Club oder um die von ihm verfolgten satzungsgemäßen Zwecke erworben haben, zu Ehrenmitgliedern ernennen. Ehrenmitglieder haben alle Rechte eines ordentlichen Mitglieds. Sie sind von Beitragsleistungen befreit.

§ 4 Rechte und Pflichten der Mitglieder
(1) Die Mitglieder sind berechtigt, die Leistungen des Clubs in Anspruch zu nehmen.
(2) Die Mitglieder sind verpflichtet, die satzungsgemäßen Zwecke des Club zu unterstützen und zu fördern. Sie sind verpflichtet, die festgesetzten Beiträge zu zahlen.

§ 5 Ausschluß eines Mitgliedes
(1) Ein Mitglied kann durch Beschluß des Vorstandes ausgeschlossen werden, wenn es das Ansehen des Clubs schädigt, seinen Beitragsverpflichtungen nicht nachkommt oder wenn ein sonstiger wichtiger Grund vorliegt. Der Vorstand muß dem auszuschließenden Mitglied den Beschluß in schriftlicher Form unter Angabe von Gründen mitteilen und ihm auf Verlangen eine Anhörung gewähren.
(2) Gegen den Beschluß des Vorstandes ist die Anrufung der Mitgliederversammlung zulässig. Bis zum Beschluß der Mitgliederversammlung ruht die Mitgliedschaft.

§ 6 Beitrag
(1) Der Club erhebt einen Aufnahme- und Jahresbeitrag. Er ist bei der Aufnahme und für das Geschäftsjahr im ersten Quartal des Jahres im voraus zu entrichten. Das Nähere regelt eine Bei-

tragsordnung, die von der Mitgliederversammlung beschlossen wird.
(2) Im begründeten Einzelfall kann für ein Mitglied durch Vorstandsbeschluß ein von der Beitragsordnung abweichender Beitrag festgesetzt werden.

§ 7 Organe des Clubs
Die Organe des Clubs sind
1. die Mitgliederversammlung
2. der Vorstand

§ 8 Mitgliederversammlung
(1) Oberstes Beschlußorgan ist die Mitgliederversammlung. Ihrer Beschlußfassung unterliegen
1. die Genehmigung des Finanzberichtes
2. die Entlastung des Vorstandes,
3. die Wahl der einzelnen Vorstandsmitglieder,
4. die Bestellung von Finanzprüfern,
5. Satzungsänderungen,
6. die Genehmigung der Beitragsordnung,
7. die Richtlinie über die Erstattung von Reisekosten und Auslagen,
8. Anträge des Vorstandes und der Mitglieder,
9. die Ernennung von Ehrenmitgliedern,
10. die Auflösung des Clubs.

(3) Die Mitgliederversammlung ist beschlußfähig, wenn mindestens fünfzehn Prozent aller Mitglieder anwesend sind. Beschlüsse sind jedoch gültig, wenn die Beschlußfähigkeit vor der Beschlußfassung nicht angezweifelt worden ist.
(4) Beschlüsse über Satzungsänderungen und über die Auflösung des Clubs bedürfen zu ihrer Rechtswirksamkeit der Dreiviertelmehrheit der anwesenden Mitglieder. In allen anderen Fällen genügt die einfache Mehrheit.
(5) Jedes Mitglied hat eine Stimme. Juristische Personen haben einen Stimmberechtigten schriftlich zu bestellen.
(6) Auf Antrag eines Mitgliedes ist geheim abzustimmen. Über die Beschlüsse der Mitgliederversammlung ist ein Protokoll anzufertigen, das vom Versammlungsleiter und dem Protokollführer zu unterzeichnen ist; das Protokoll ist allen Mitglieder zugänglich zu machen und auf der nächsten Mitgliederversammlung genehmigen zu lassen.

§ 9 Vorstand
(1) Der Vorstand besteht aus sieben Mitgliedern:
1. den Vorsitzenden,
2. zwei stellvertretenden Vorsitzenden,
3. dem Schatzmeister,
4. zwei Beisitzern und

(2) Vorstand im Sinne des § 26 Abs. 2 BGB sind die Vorstandsmit glieder. Die Vertretungsmacht ist durch Beschlüsse des gesam ten Vorstandes begrenzt.
(3) Der Vorstand beschließt mit der Mehrheit seiner satzungsge mäßen Mitglieder. Sind mehr als zwei Vorstandsmitglieder dauernd an der Ausübung ihres Amtes gehindert, so sind unver züglich Nachwahlen anzuberaumen.
(4) Die Amtsdauer der Vorstandsmitglieder beträgt zwei Jahre; Wiederwahl ist zulässig.
(5) Der Vorstand ist Dienstvorgesetzter aller vom Club angestell ten Mitarbeiter; er kann diese Aufgabe einem Vorstandsmitglied übertragen.
(6) Der Schatzmeister überwacht die Haushaltsführung und verwaltet das Vermögen des Clubs. Er hat auf eine sparsame und wirt schaftliche Haushaltsführung hinzuwirken. Mit dem Ablauf des Geschäftsjahres stellt er unverzüglich die Abrechnung sowie die Vermögensübersicht und sonstige Unterlagen von wirtschaft lichem Belang den Finanzprüfern des Clubs zur Prüfung zur Verfügung.
(7) Die Vorstandsmitglieder sind grundsätzlich ehrenamtlich tätig; sie haben Anspruch auf Erstattung notwendiger Auslagen im Rahmen einer von der Mitgliederversammlung zu beschließenden Richtlinie über die Erstattung von Reisekosten und Auslagen.
(8) Der Vorstand kann einen "Wissenschaftlichen Beirat" einrich ten, der für den Club beratend und unterstützend tätig wird; in den Beirat können auch Nicht-Mitglieder berufen werden.

§ 10 Finanzprüfer
(1) Zur Kontrolle der Haushaltsführung bestellt die Mitgliederversammlung Finanzprüfer. Nach Durchführung ihrer Prüfung geben sie dem Vorstand Kenntnis von ihrem Prüfungser gebnis und erstatten der Mitgliederversammlung Bericht.
(2) Die Finanzprüfer dürfen dem Vorstand nicht angehören.

§ 11 Erfa-Organisation
(1) Der Club bildet zur Durchführung seiner Aufgaben regionale Erfahrungsaustauschkreise (Erfa-Kreise). Sie bestimmen ihre Organisationsstruktur selbst.
(2) Aufgabe der Erfa-Kreise ist ferner,
1. die Entscheidungsbildung im Club zu fördern und vorzubereiten,
2. Mitglieder für den Club zu werben.

(3) Beabsichtigt ein Erfa-Kreis, bestimmte Themen oder Aktivitäten mit überregionalen Bezug an die Öffentlichkeit zu tragen, ist dies vorher mit dem Vorstand des Clubs abzustimmen.
(4) Jeder Erfa-Kreis bestimmt einen Erfa-Kreis-Vertreter. Die Erfa-Kreise sollten sich eine Organisationsstruktur geben, die mit dem Erfa-Beirat abzustimmen ist.

§ 12 Erfa-Beirat
(1) Der Erfa-Beirat besteht aus den Erfa-Vertretern, die Clubmitglieder sind.
(2) Der Erfa-Beirat schlägt der Mitgliederversammlung aus seiner Mitte den Erfa-Repräsentanten zur Wahl in den Vorstand vor.
(3) Der Erfa-Beirat wirkt bei der Führung der Clubgeschäfte beratend und unterstützend mit. Er hat dabei insbesondere die Aufgabe, die Belange der Erfa-Kreise zu vertreten.

§ 13 Auflösung des Clubs
Bei der Auflösung des Clubs oder bei Wegfall seines Zweckes fällt das Clubvermögen an eine von der Mitgliederversammlung zu bestimmende Körperschaft des öffentlichen Rechts oder eine andere steuerbegünstigte Körperschaft zwecks Verwendung für die Volksbildung.

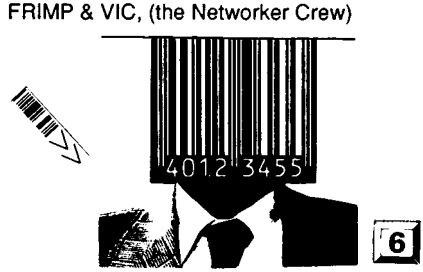
Hamburg, den 16. Februar 1986

Bitnepp

"Für immer wurde der Betrieb des Relays an der Cornell Universität in New York eingestellt"; so berichtete die dpa-Meldung vom ....
Wir wissen nicht, wer ihnen diese freundliche Mitteilung überreicht hat, wir empfehlen 'SEND/REM CORNELLC RLY' (ehemals CORNELLC MAS).

Angeblich haben es die Hacker doch geschafft, über BITNET ganze Rechnernetze herunterzufahren und wichtige Dateien "unwissentlich vernichtet". Wilde Spekulationen über Planungen "elektronischer Bombeneinschläge" wurden in den Pressemeldungen verlautbart.
Die "Hackergefahr" kann nach Ansicht der Cornell Uni nicht so groß gewesen sein, da das System bereits nach etwa drei Monaten unter geringfügig geändertem Namen wieder am Netz hing.
Zu EARN/BITNET, um das es in diesem Zusammenhang geht einige sachliche Anmerkungen:
Tatsache ist, daß Dialoge auf EARN/BITNET (von IBM gesponsort) mittels Konferenzprotokollen ständig überwacht werden können und auch wurden.
BITNET verbindet nahezu sämtliche Universitäten und Forschungszentren in den USA und Europa (über EARN = European Academic Research Network) und bietet JEDEM Benutzer der Rechner die Möglichkeit, Dateien mit JEDEM Benutzer desselben oder eines anderen Rechners übers Netz auszutauschen.
Zur Förderung der Kommunikation wurde ein sog. "Interchat Relay Network" eingeführt, das online Konferenzschaltungen erlaubt. So haben sich zum Beispiel die Wissenschaftler, die die Giotto-Sonde zur Erforschung des Kometen Halley überwachten in der Zeit, in der sie nur darauf warteten, daß irgendetwas schiefgeht die Langeweile bei einem lockeren Chat vertrieben.
Eben auf diesen "Relays" haben sich auch deutsche und Schweizer Hacker etabliert, um an den Gesprächen konstruktiv teilzunehmen.
Es ist also wie gesagt nicht möglich, auf fremden Rechnern Dateien zu löschen oder gar Betriebssystemkommandos auszuführen, d.h. die dpa-Pressemeldung lieferte einfach irreführende Informationen.
Doch zurück zu BITNET/EARN: Der Schweizer Zentralknoten CEARN (Genf) ist mit Darmstadt, Paris, Rutherford, Rom und Stockholm direkt verbunden und führt via diese Knoten theoretisch direkt in die USA, z.B. an die George Washington University in New York, praktisch klappt die Verbindung nicht immer reibungslos (Murphy schlug bereits diverse Male zu). An EARN hängen z.B. (fast) alle deutschen Unis, das DESY in Hamburg, das DFVLR in München, Cern in der Schweiz und einige NASA Rechner. Für Ottonormalforscher sind derartige interessante Perspektiven völlig verschlossen, Heinz Hacker wird von Netzbetreibern immer noch ungern gesehen ("Fritz is online").
EARN/BITNET ist für jeden eine sehr interessante Sache, denn neben lockeren Chats findet speziell in den Konferenzen ein reger Know-How-Austausch statt, über letzteres verfügen Hacker unbestritten !
Nebenbei: EARN wird von der 3-Buchstaben-Firma bis Ende 1987 finanziert, so daß es natürlich für diverse Forschungsinstitute in Deutschland kein Problem ist, sich (via Datex-L) daran zu beteiligen, zumindest solange es sich um SNA-(un)fähige Systeme handelt. Nicht erst ab 1988 gilt also für IBM: "Let's EARN some money!", von der parasitären Know-How-Beschaffung ganz abgesehen.
Warum eigentlich den Hackern, den wahren Verfechtern der freien Kommunikation der Zugriff verweigert werden soll, ist nicht einzusehen, denn unbestritten bleibt doch der Forschungsauftrag der Hacker, der eine Teilnahme an diesem Netz geradezu zwingend vorschreibt !
Zum Schluß noch ein paar Tips für jene Datenreisenden, die über einen EARN oder BITNET Zugang verfügen:
Auf VAXen: SEND/REM CEARN RELAY in Europa oder SEND/REM BITNIC RELAY in USA, um an den Konferenzen teilzunehmen, dann /h für Help.
Auf IBM/VM Kisten: TELL RELAY AT CEARN /h usw.! Empfehlenswert: das Relay an der Cornell-Uni sollte bevorzugt behandelt werden (CORNELLC RLY), ist aber nur zwischen 9:00 pm und 6:00 am lokaler Zeit erreichbar.
Aber keine elektronischen Bombeneinschläge planen oder gar Giotto auf dem Mars landen lassen, sonst wird die Cornell-Uni keine weiteren Studienbewerbungen mehr annehmen.

FRIMP & VIC, (the Networker Crew)



Mailboxen im Btx-Wartesaal

Über externe Rechner wurde in Bildschirmtext eine Dialogmöglichkeit geschaffen.
Einen guten Eindruck gibt der folgende Dialogmitschnitt; die Btx-üblichen Verwaltungs- und Farbinformationen wurden gestrichen.
Teilnehmer waren hallo und chaos-team

001: Dialog-Beginn 14:55:26
hallo aus HH
hallo aus hh, hier ist das chaos-team.
und welche Mission treibt euch hierher?
wir testen die wartezeiten
(abgeschickt 14:58:22; angezeigt wurde durch Übermittlungsfehler "Eilgabe abgeschickt" statt "Eingabe abgeschickt". Die Antwort traf um 15:01:03 ein.)
na dann viel Spaß. Testet mal auch, wie oft man hier rausfliegt. Ich wurde heute schon 6 mal hinausbefördert, aber das glauben die Veranstalter mir nicht.
ß da ist der msg dienst im postsystem schneller und bald wohl auch preiswerter
ganz sicher, aber nicht das Angebot
wie endet der dialog, wenn du nicht mehr da bist (rausfliegst) für uns, merkt das system das?
mein Partner sendet noch eine Mitt. ab, die nicht ankommt, ich erhalte eine Postseite mit: die Verbindung wurde unterbrochen aus technischen Gründen.
ist bekannt, welche gebühren geplant sind?
ich weiß nur das, was am Anfang gesagt wird. 0,08 pro Dialogschritt und 0,50 für den Einstieg.
0,07 kostet eine versendete msg über mailboxsysteme, der dialog dort in echtzeit 25 pfg die minute - welchen namen hat die systemzentrale?
weiß nicht, aber da sind meistens Beobachter im Programm unter ICR, Baff oder eine Kombination davon.
danke, dürfen wir diesen dialog veröffentlichen?
gerne, wenn er aussagekräftig genug ist
ok, wie beendet man den dialog?
die nächste msg nicht absenden

Um 15:22:14 konnten wir den zweiten und vorerst letzten Dialog beginnen. Ein Testlesen des Artikels dauerte xx Sekunden; per Btx ca. 20 Minuten.
/xi/ws/btxmbx16.wau 860401 1911

Glaube an neue Dienste

Btx-Schwund statt Schwung bringt die neue Gebührenordnung. Zum Rückgang der Anbieterzahlen meinte der Leiter des Fernmeldeamtes in N. (Q:sz860701s26): "Man muß an neue Dienste glauben...".

CCC auf kommerziellen Boxen – Rückschlag für private Betreiber ?

"...aber in den Zentren keimt es. Einige Sysops gestalten ihre rmationssysteme bewuat, sie agieren als elektronische Verleger."

So stand es in DS14 in der Ankundigung des Chaos Communication Congress '85. Den lokalen Mailboxen wurde steigende Qualitat bescheinigt, das Bewusstsein der Betreiber fur die Erfordernisse der Kommunikationsgesellschaft sei gestiegen.

Tatsachlich gibt es uberall in diesem unseren Lande Sysops, fur die ihre Mailbox mehr ist, als nur eine elektronische Mullhalde. Diese Betreiber investieren sehr viel Zeit und noch mehr Geld in die Entwicklung der lokalen Systeme, um eine Angleichung an den Standard der kommerziellen Boxen zu erreichen, ja diesen Standard in der Hinsicht zu ubertreffen, daa sie dem alten Grundsatz treu bleiben "Soviel Information wie moglich, so preiswert wie moglich". Da werden mal eben 10.000 DM in Hardware gesteckt, hunderte von Arbeitsstunden in Programmentwicklung investiert. Treibende Kraft bei dieser Entwicklung war dabei auch der CCC, der immer wieder unablaaig forderte, die lokalen Systeme muaten weg von der CB-Mullbox, hin zum (semi-) professionellen Standard. Und tatsachlich fielen diese Anregungen bei etlichen Betreibern auf fruchtbaren Boden, inzwischen entstehen bundesweit uberall Systeme, die auf mehreren Leitungen gleichzeitig erreichbar sind, teilweise auch uber Pattex-D.

Das Hauptproblem fur die Betreiber dieser Systeme ist dabei, dem Otto-Normal-User klarzumachen, daa diese qualitativ hochwertigen regionalen Systeme nicht mehr kostenlos zuganglich sein konnen, wenn allein die Fernmeldegebuhren bis zu 400.- DM pro Monat betragen. Das ist angesichts der unzahligen C64-Boxen, die zum Nulltarif am Netz hangen, schon ein schwieriges Unterfangen, das nur durch die erhebliche Leistungssteigerung gegenuber den herkommlichen Systemen sinnvoll und damit machbar wird. Nicht zu vergessen, daa die neuen regionalen und uberregionalen Boxen auch ein gutes Stuck mehr an informationeller Selbstbestimmung bieten, denn es stecken ja immer noch dieselben Leute dahinter, die im besten Sinne chaotischer Tradition agieren. In diese sehr schwierige Situation hinein platzt nun die Ankundigung des CCC, seinen Mitgliedern die Moglichkeit zu geben, ein kommerzielles Mailboxsystem fur einen unglaublich gunstigen Preis zu nutzen. Das ist auf den ersten Blick eine sensationelle Sache, denn bisher waren kommerzielle Boxen aufgrund der hohen Monatsgebuhren fur normale Sterbliche unerreichbar. Auf den zweiten Blick jedoch ergeben sich daraus harte Konsequenzen fur diejenigen Sysops, die erade dabei sind, ihre Systeme, wie oben beschrieben, auszubauen, denn angesichts der neuesten Entwicklung erscheint es zunachst sinnlos, die Projekte weiterzufuhren. Wozu ein System errichten, dass dem Benutzer fur funf Mark im Monat ein Subset der Leistungen kommerzieller Boxen bietet, wenn fur relativ geringe Mehrkosten der Zugang zu den kommerziellen Systemen offen ist? Zwar ist dafur die Mitgliedschaft im CCC notwendig, was bei den normalen Boxen nicht der Fall ist, aber es steht zu befurchten, daa es ublich wird, CCC-Mitglied zu werden, um in den Genuss der kommerziellen Box zu kommen. Diese Entwicklung kann durchaus dazu fuhren, daa die augenblicklichen Versuche, eine autonome Informationsszene hohen Standards auzubauen, im Keime erstickt, oder zumindest auf lange Sicht behindert werden und es stellt sich die Frage, ob das tatsachlich im Sinne des Chaos Computer Clubs ist.
ccobox16.da 860502 2020 goblin

recht

Zu Artikel 1 Nr. 5 — § 266a StGB —

Neben einer redaktionellen Klarstellung hat der Ausschuß die Überschrift erweitert. Dadurch soll vor allem die unterschiedliche Schutzrichtung zwischen Abs. 1 und Abs. 2 noch stärker verdeutlicht werden. Während Absatz 2, wie sich schon aus der Fassung ergibt, ein untreueähnliches Verhalten des Arbeitgebers (und der ihm durch § 14 StGB gleichgestellten Personen) zum Nachteil des Arbeitnehmers erfassen will, handelt es sich bei Absatz 1 (und ähnlich bei Absatz 3) um den Schutz der Solidargemeinschaft. Das Aufkommen der Sozialversicherungsträger und der Bundesanstalt für Arbeit soll dadurch strafrechtlich gewährleistet werden. Dies ist in Absatz 1 durch die Streichung eingrenzender Merkmale des geltenden Rechts („erhalten", „einbehalten") verdeutlicht worden, wodurch sich Absatz 1 bewußt von Absatz 2 unterscheidet. Damit können künftig auch Fälle bestraft werden, in denen Arbeitgeber und Arbeitnehmer einvernehmlich verabreden, bei Lohnzahlungen keine Beiträge abzuführen (zum bisherigen Recht vgl. BGH wistra 1982, 111). Da sich dies aus dem Wortlaut der Entwürfe bereits ergibt, ist eine zusätzliche Ergänzung des Textes, wie dies von dem Sachverständigen Stahlschmidt in der öffentlichen Anhörung erwogen wurde (vgl. Prot. Nr. 26, Anl. S. 6), nicht erforderlich. Auch unter Berücksichtigung der im Wirtschaftsausschuß geäußerten Kritik an § 266a StGB ist der Ausschuß der Meinung, daß die Aufbringung der Mittel der Sozialversicherung ebenso wie die des Steueraufkommens eines besonderen strafrechtlichen Schutzes bedarf. Davon geht schon das geltende Recht aus.

Zu Artikel 1 Nr. 5 — § 266b StGB —

Der Rechtsausschuß empfiehlt mit Mehrheit, eine Strafvorschrift gegen den Mißbrauch von Scheck- und Kreditkarten einzuführen.

Das Scheck- und Kreditkartensystem hat inzwischen zu einer außerordentlichen Ausweitung des bargeldlosen Zahlungsverkehrs geführt und dadurch eine erhebliche volkswirtschaftliche Bedeutung erlangt. Das Scheckkarten ausstellende Kreditinstitut garantiert hierbei die Einlösung von Schecks auf speziellen zur Scheckkarte ausgegebenen Scheckformularen bis zu einem bestimmten Betrag (zur Zeit 400 DM) und nimmt damit dem Schecknehmer das Risiko eines ungedeckten Schecks ab.

Das Kreditkartengeschäft im Drei-Partner-System beruht auf dem gleichen Grundgedanken. Das Karten ausstellende Institut verpflichtet sich gegenüber dem Vertragsunternehmen, seine Forderungen gegen dem Karteninhaber auszugleichen. Dabei ist es üblich, dem Vertragsunternehmen jeweils unterschiedliche Obergrenzen für einzelne Geschäfte zu setzen, bei deren Überschreitung Vertragsunternehmen bei Vorlage der Kreditkarte eine Genehmigung des Kreditkarteninstituts einholen müssen oder die Einlösungsgarantie verlieren. Daneben ist auch das Zwei-Partner-System gebräuchlich. Hierbei räumt ein Unternehmen mit der Kreditkartenausgabe seinem Kunden lediglich einen für alle Filialen gültigen Kundenkredit ein.

Durch die neue Strafvorschrift soll der Fall erfaßt werden, daß ein Scheck- oder Kreditkartennehmer unter Verwendung der Karte Waren kauft und Dienstleistungen in Anspruch nimmt, obwohl er weiß, daß das Kreditinstitut seine Rechnungen zu bezahlen hat, und er selbst aber, z. B. nach einem Vermögensverfall nicht mehr in der Lage sein wird, die Auslagen zurückzuerstatten. Bestraft werden soll die dadurch verursachte Vermögensschädigung der Kreditinstitute.

Der Bundesgerichtshof hat in einem Urteil vom 13. Juni 1985, 4 StR 213/85 (BGHSt 33, 244) zum Kreditkartenmißbrauch festgestellt, daß eine solche Tathandlung nicht den Tatbestand der Untreue und des Betrugs erfülle. Allerdings hat der Bundesgerichtshof in seiner Entscheidung vom 13. Juni 1985 unter Bestätigung seiner Entscheidung vom 26. Juli 1972 (BGHSt 24, 386) entschieden, daß ein Mißbrauch der Scheckkarte durch den Karteninhaber den allgemeinen Betrugstatbestand nach § 263 StGB erfülle. Er hat hierbei darauf abgestellt, daß die Scheckkarte im Scheckverkehr vorgelegt werde und nur den zusätzlichen Nachweis der Einlösegarantie erbringe, während die eigentliche Handlung mit Erklärungswert die Hingabe des Schecks sei. Insoweit bestehe kein wesensmäßiger Unterschied zu der Einlösung eines ungedeckten Schecks ohne Scheckkarte. Diese Rechtsprechung des Bundesgerichtshofs wird vom Schrifttum bis heute mit der Begründung heftig kritisiert, daß sie mit den Gegebenheiten des Scheckkartenverkehrs nicht im Einklang sei. Wie bei der Vorlage einer Kreditkarte brauche der Schecknehmer sich bei der Vorlage der Scheckkarte bis zur garantierten Summe über die Kreditwürdigkeit des Scheckausstellers keine Gedanken zu machen und werde das in der Regel auch nicht tun. Die Voraussetzungen des Betrugstatbestands, nämlich der für die Vermögensverfügungen ursächliche Irrtum, sind deshalb in diesen Fällen nicht gegeben. Angesichts dieser Kritik aus dem Schrifttum ist davon auszugehen, daß die Entscheidung des Bundesgerichtshofs auf Dauer schwerlich Bestand haben werde.

Im Rechtsausschuß ist umstritten, ob der dargestellte Mißbrauch von Scheck- und Kreditkarten strafwürdig ist. Nach Auffassung der Mehrheit weist die dargestellte Tathandlung gegenüber dem geltenden Untreuetatbestand einen ähnlichen sozialschädlichen Kriminalitätsgehalt auf. Der neue Straftatbestand sei zum Schutze der Funktionsfähigkeit des bargeldlosen Zahlungsverkehrs, der eine volkswirtschaftliche Bedeutung erlangt habe, notwendig.

Die Minderheit lehnt die neue Strafvorschrift ab. Sie ist der Auffassung, daß die Verwendung der Scheck-, vor allem der Kreditkarten, allgemein keineswegs so positiv einzuschätzen sei, da das Kredit- und Scheckkartensystem die Gefahr einer Überschuldung der Inhaber in sich berge, wie es sich in den USA gezeigt habe. Vor allem würde mit dem Straftatbestand in systemwidriger Weise die Verletzung von Vertragspflichten strafrechtlich sanktioniert und der notwendige Rechtsschutz sei durch das Zivilrecht gewährleistet. Insbesondere sei es Aufgabe der Kreditinstitute, sich durch eine entsprechende Ausgestaltung der Rechtsbeziehungen zu den Inhabern der Scheckkarten und Kreditkarten und zu den Vertragsfirmen sowie durch eine sorgfältige Prüfung der Kreditwürdigkeit ihrer Kunden zu schützen.

Einigkeit bestand im Ausschuß, daß keine Notwendigkeit besteht, den Tatbestand auf andere Fälle von Mißbräuchen, insbesondere auf den Gebrauch von Scheck- und Kreditkarten durch Nichtberechtigte auszudehnen. Die Anwendung des Betrugstatbestandes reicht hier aus.

Zu der Ausgestaltung der von der Mehrheit beschlossenen Strafvorschrift ist zu bemerken:

Absatz 1 lehnt sich in seiner Einzelausgestaltung eng an den Mißbrauchstatbestand des § 266 StGB (Untreue) an. Durch die Wendung „... die ihm durch die Überlassung einer Scheckkarte oder einer Kreditkarte eingeräumte Möglichkeit, den Aussteller zu einer Zahlung zu veranlassen" wird der Täterkreis auf berechtigte Karteninhaber eingegrenzt und auch die Garantieerklärung, die mit der Überlassung der Karte verbunden ist, beschrieben. Zahlung ist dabei nicht nur im rein technischen Sinne als Hingabe von Bargeld zu verstehen, sondern auch als Geldleistung im Verrechnungswege. Die Begriffe Scheck- und Kreditkarte haben im Wirtschaftsleben einen so feststehenden Bedeutungsinhalt, daß sie als Tatbestandsmerkmale ausreichend bestimmt sind, zumal auf die ihnen notwendigerweise zukommende Garantiefunktion Bezug genommen wird.

Die mit der Überlassung der Scheck- oder Kreditkarte eingeräumte Möglichkeit muß der Täter „mißbrauchen". Das Mißbrauchsmerkmal entspricht dem des § 266 Abs. 1 1. Alternative StGB. Der Täter hält sich dabei nach außen im Rahmen seines rechtlichen Könnens, überschreitet aber im Innenverhältnis zu dem Kartenherausgeber die Grenzen seines rechtlichen Dürfens. Mißbrauch der Scheckkarte liegt z. B. immer dann vor, wenn der Täter einen Scheck hingibt, dessen Einlösung zwar von seinem Kreditinstitut garantiert ist, für den auf seinem Konto aber keine Deckung oder kein ausreichender Kredit vorhanden ist. Bei der Kreditkarte liegt ein Mißbrauch z. B. dann vor, wenn der Täter mit der Verwendung der Karte gegen seine aus dem Kreditkartenvertrag resultierenden Pflichten verstößt, insbesondere, wenn er Verpflichtungen eingeht, obwohl die Einkommens- und Vermögensverhältnisse den Kontoausgleich nicht gestatten oder er selber nicht für ausreichende Deckung Sorge getragen hat.

Wie bei § 266 StGB setzt das Mißbrauchsmerkmal weder generell voraus, daß dem Karteninhaber für einzelne Geschäfte ein Limit gesetzt ist (so in seiner Wirkung die Scheckkartengarantie), noch daß ein zeitabhängiger (etwa monatlicher) Höchstrahmen vorgeschrieben wird, noch daß eine absolute Kreditobergrenze vereinbart ist. Anderenfalls wären Verhaltensweisen, über die der Bundesgerichtshof jüngst zu entscheiden hatte, weiterhin straflos.

Der Mißbrauch der Kreditkarte muß schließlich zu einer Schädigung des Kartenherausgebers führen. Damit soll die Parallele zum Betrugs- und Untreuetatbestand gewahrt werden, da durch den neuen Tatbestand lediglich eine Lücke geschlossen werden soll, die bei der Anwendung dieser Bestimmungen offenbar wurde. Es muß sich daher bei dem Schaden um einen Vermögensschaden handeln. Das Schadenserfordernis engt darüber hinaus das Mißbrauchsmerkmal weiter ein. Ist der Täter anderweitig bereit und in der Lage, die Überziehung sofort oder jedenfalls unverzüglich auszugleichen, so liegt ein Schaden — ebenso wie beim Untreuetatbestand, der dem neuen Tatbestand in diesem Punkt entspricht — nicht vor. Unter diesen Voraussetzungen wird auch der neue Tatbestand des Scheckkartenmißbrauchs nicht anzuwenden sein, wenn der Täter gelegentlich sein Konto durch Begebung von Schecks über die ihm eingeräumte Kreditgrenze hinaus belastet.

Der Täter muß vorsätzlich handeln, der Vorsatz muß sich auf sämtliche Tatbestandsmerkmale beziehen. Derjenige, der bei Scheckausstellung oder Verwendung der Kreditkarte noch nicht weiß, daß er seinen Verpflichtungen später nicht wird nachkommen können, kann daher auch nach dem neuen Tatbestand nicht bestraft werden. Darüber hinaus handelt auch derjenige unter Umständen noch nicht vorsätzlich, der zwar von der Deckungslosigkeit seines Kontos bei Begebung des garantierten Schecks weiß, aber mit Vermögensausgleich in kürzester Zeit rechnet.

Absatz 2 erklärt entsprechend § 266 Abs. 2 StGB § 248a (Antragserfordernis bei geringem Schaden) für entsprechend anwendbar.

Zu Artikel 1 Nr. 6 — § 269 StGB — Fälschung beweiserheblicher Daten

Die Einführung eines besonderen Tatbestandes gegen die Fälschung beweiserheblicher Daten wird vom Ausschuß für notwendig erachtet. Dafür sind die bereits im Regierungsentwurf, in der öffentlichen Anhörung sowie in den Ausschußberatungen vorgebrachten Gesichtspunkte maßgebend. Vom Tatbestand der Urkundenfälschung werden unbefugte Eingaben z. B. von Computerdaten bzw. unbefugte Veränderungen von bereits gespeicherten Daten, die, wenn sie in ein Schriftstück aufgenommen wären, eine Urkundenfälschung darstellen würden, mangels Erkennbarkeit der Erklärung nicht erfaßt. Für die Anwendung des § 267 StGB reicht die leichte Einsehbarkeit in Dateien über Bildschirmterminals alleine nicht aus. Die Urkundeneigenschaft kann auch mangels Ausstellerangabe entfallen. Solchen Daten fehlt daher die von § 267 StGB vorausgesetzte Urkundenqualität. Der Straftatbestand des § 268 StGB (Fälschung technischer Aufzeichnungen) erfaßt nur Teilbereiche. Ohne eine Ergänzung des Strafrechts würde daher die Umstellung verwaltungsmäßigen Handelns auf die Datenverarbeitung den bisher bei Schriftstücken bestehenden strafrechtlichen Urkundenschutz ungerechtfertigt verkürzen. Bei den Verwendungsmöglichkeiten der Datenverarbeitung reicht für einen wirksamen Schutz auch die Tatsache nicht aus, daß Verarbeitungen zu Computerausdrucken führen können, denen Urkundenqualität beizumessen ist und die bei (mittelbarer) Vornahme, z. B. von Eingaben oder nachträglichen Veränderungen durch nicht Berechtigte, deshalb als Urkundenfälschung i. S. von § 267 StGB qualifiziert werden können. In vielen Fällen werden entscheidungserhebliche Daten direkt aus dem Computer zur (maschinellen) Weiterverarbeitung benutzt, wie dies besonders im Bank-, Rechnungs- und Zahlungsverkehr deutlich wird.

„Hacker-Manöver" in Paris

Eine „Nacht der Hacker" ist in der vergangenen Woche von der Pariser Zeitung 'Le Monde' organisiert worden. Zehn junge Informatik fans, so berichtet 'Le Monde' jetzt, seien unter der Aufsicht von drei Experten zwischen Mitternacht und sieben Uhr am frühen Morgen in zwanzig große Datenbanken Europas und der USA eingedrungen so in die des britischen Verteidigungsministeriums.

Aus ähnlichen Erwägungen wie beim Computerbetrug hat sich der Ausschuß gegen den Vorschlag von Haft in der Öffentlichen Anhörung (Prot. Nr. 26, S. 164, Anl. S. 201) ausgesprochen, sich mit einer bloßen Ergänzung des § 267 StGB zu begnügen („Gedankenerklärungen können auch dann Urkunden sein, wenn sie computerlesbar gespeichert sind"). Eine sich nur auf eine Ergänzung des Urkundenbegriffs, sei es in § 267 StGB oder in allen Urkundenstraftatbeständen, beziehende Gleichstellungsvorschrift würde andere Tatbestandsmerkmale unangetastet lassen. Dies würde zu einer unklaren und wenig anschaulichen Tatbestandsumschreibung führen („Wer ... unechte computerlesbar gespeicherte Gedankenerklärungen ... [bzw. Daten ...] speichert ...), die dem Ausschuß nicht akzeptabel erscheint.

Im Hinblick auf die in Absatz 1 gegenüber den Entwürfen vorgeschlagene Erweiterung des Tatbestandes wurde die Überschrift geändert.

Absatz 1 wurde seinem Inhalt und seiner Ausgestaltung nach nicht unwesentlich umgestaltet. Entsprechend der Prüfungsempfehlung des Bundesrates stellt die Neufassung sicher, daß die der Herstellung einer unechten Urkunde entsprechende unzulässige Speicherung beweiserheblicher Daten dem Tatbestand unterfällt. Dem dazu vorgelegten Formulierungsvorschlag der Bundesregierung in ihrer Gegenäußerung zu der Stellungnahme des Bundesrates ist der Ausschuß allerdings nicht gefolgt. Maßgebend dafür war, daß dort zur Abgrenzung von strafbarem und straflosem Verhalten u. a. weiter auf „unbefugtes" Handeln abgestellt wird, dieser Begriff jedoch in seiner Bedeutung nicht völlig klar ist. Darauf hat Haft in der öffentlichen Anhörung zu Recht hingewiesen (Prot. Nr. 26, Anl. S. 210). Die einengende Auslegung, die der Regierungsentwurf diesem Merkmal beilegt, kann im Hinblick auf eine weiterreichende Bedeutung dieses Merkmals in anderen Strafvorschriften nicht als gesichert betrachtet werden. Um zu vermeiden, daß von der neuen Strafvorschrift Verhaltensweisen erfaßt werden, die bei ihrer Vornahme im Zusammenhang mit der Herstellung oder Veränderung eines Schriftstücks nur eine sog. straflose schriftliche Lüge darstellen, hat der Ausschuß die Vorschrift neu gestaltet. Entscheidend ist, daß Daten so (nicht unmittelbar wahrnehmbar) gespeichert oder verändert werden, daß sie, wenn sie als ausgedruckt oder wiedergegeben wahrnehmbar wären, eine Urkundenfälschung i. S. des § 267 StGB darstellen würden. Mit dieser Ausgestaltung wird auch dem Anliegen von Haft, den Tatbestand nicht von der Garantiefunktion, der Ausstellererkennbarkeit zu lösen (Prot. Nr. 26, S. 168, Anl. S. 209 f.), Rechnung getragen. Durch die Konstruktion eines hypothetischen Vergleichs mit Fällen der Urkundenfälschung i. S. des § 267 StGB war es auch nicht mehr notwendig, besonders hervorzuheben, daß vom Tatbestand nur solche Daten erfaßt werden, „die dazu bestimmt sind, bei einer Verarbeitung im Rechtsverkehr als Beweisdaten für rechtlich erhebliche Tatsachen benutzt zu werden" (so die Formulierung der Entwürfe). Der Zusatz „beweiserheblich" gibt in verkürzter Form diese Auslegung wieder. Aus der den Tatbestand des § 267 StGB ergänzenden Funktion des § 269 StGB wie aus seiner Ausgestaltung ergibt sich, daß nur solche beweiserheblichen Daten betroffen sind, die „elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar" gespeichert werden bzw. bei Tatbegehung schon entsprechend gespeichert waren. Wie bei § 263 a StGB wurde auf eine Verweisung auf § 202 a Abs. 2 StGB abgesehen, da § 269 StGB auch Fälle erfaßt, in denen Daten eingegeben werden, also nicht nur an bereits gespeicherten Daten Veränderungen vorgenommen werden (so noch die Entwürfe).

Die *Absätze 2 und 3* wurden unverändert übernommen.

§ 270 StGB — Täuschung im Rechtsverkehr bei Datenverarbeitung —

unverändert

Zu Artikel 1 Nr. 7 und 8 — §§ 271, 273 StGB —

unverändert

Zu Artikel 1 Nr. 9 — § 274 StGB —

Die Vorschrift wurde inhaltlich im wesentlichen unverändert übernommen. Die Änderungen und Ergänzungen sind Folgeänderungen. Der Begriff Daten wird durch Bezugnahme auf § 202 a Abs. 2 StGB in Artikel 1 Nr. 2 b eingegrenzt. Die Verwendung des Merkmals „beweiserheblich" ersetzt die Verweisung auf § 269 StGB. Es ist wie dort zu verstehen (vgl. die Begründung zu Artikel 1 Nr. 6 — § 269 StGB —). Die Ergänzung der Tathandlungen dient der Angleichung an § 303 a StGB (Datenveränderung) in Artikel 1 Nr. 9 b (vgl. die dortigen Erläuterungen). Sie verdeutlicht den in der höheren Strafdrohung sich auswirkenden Vorrang der Nummer 2 gegenüber § 303 a StGB. Auch Tathandlungen, die dem „Beschädigten" in § 274 Abs. 1 Nr. 1 StGB entsprechen, werden nunmehr ausdrücklich erfaßt.

Zu Artikel 1 Nr. 9a und 9b — § 303 Abs. 3, §§ 303 a, 303 b, 303 c StGB —

§ 303 a StGB — Datenveränderung —

Der Ausschuß schlägt die Aufnahme eines in den Entwürfen nicht enthaltenen Tatbestandes gegen „Datenveränderung" vor. Als Daten dargestellte Informationen sollen dagegen geschützt werden, daß ihre Verwendbarkeit beeinträchtigt oder beseitigt wird. Computerdaten können einen hohen wirtschaftlichen Wert haben. Auf Grund der wachsenden Abhängigkeit von ihnen in Wirtschaft und Verwaltung und ihrer starken Komprimierung ist ein zusätzlicher strafrechtlicher Schutz erforderlich. Aufgegriffen werden damit Anregungen aus der öffentlichen Anhörung (vgl. Mohr und Oertel, Prot. Nr. 26 S. 180, 183 f.; Anl. S. 36 ff., 218 f.). Sieber (Prot. S. 177) sah zwar im Moment keine spezifischen Reformbedürfnisse, wies aber selber auf eine mögliche Zunahme solcher Delikte hin (Prot. S. 172). Auch

ausländische Staaten haben vergleichbare Regelungen (USA, Kanada) oder planen solche (Österreich, Schweiz). Das geltende Recht reicht nicht aus. Die Anwendbarkeit des § 303 StGB (Sachbeschädigung) ist umstritten und zumindest nicht in allen Fallgestaltungen gesichert (zweifelnd z. B. Oertel, Prot. S. 183 f., 190). Das Vernichten oder Verändern von Daten während der Übermittlungsphase wird z. B. von § 303 StGB nicht erfaßt.

Der vorgeschlagene Tatbestand lehnt sich in seiner Ausgestaltung weitgehend an § 303 StGB an. Durch Aufnahme verschiedener, sich teilweise überschneidender Tathandlungen soll erreicht werden, daß alle rechtswidrigen Beeinträchtigungen der Verwendbarkeit von Daten erfaßt werden. Dabei kann sich die Rechtswidrigkeit sowohl aus der Verletzung des Verfügungsrechts des Speichernden als auch aus der Verletzung von Interessen des vom Inhalt der Daten Betroffenen (vgl. § 41 BDSG) ergeben.

Absatz 1

Handlungsobjekt sind alle nicht unmittelbar wahrnehmbaren Daten i. S. des § 202 a Abs. 2 StGB. Das „Löschen" von Daten, das dem Zerstören einer Sache in § 303 StGB entspricht, macht diese unwiederbringlich vollständig unkenntlich (vgl. § 2 Abs. 1 Nr. 4 BDSG). Ein „Unterdrücken" von Daten liegt vor, wenn diese dem Zugriff Berechtigter entzogen und deshalb nicht mehr verwendet werden können; insoweit geht § 303 a StGB über § 303 StGB hinaus. „Unbrauchbar" sind Daten, wenn sie (z. B. durch zusätzliche Einfügungen, so Sieber in der veröffentlichten erweiterten Fassung seines Gutachtens) so in ihrer Gebrauchsfähigkeit beeinträchtigt werden, daß sie nicht mehr ordnungsgemäß verwendet werden können und damit ihren Zweck nicht mehr erfüllen können. Das „Verändern" von Daten erfaßt Funktionsbeeinträchtigungen wie das in § 2 Abs. 1 Nr. 3 BDSG genannte inhaltliche Umgestalten, durch das ihr Informationsgehalt bzw. Aussagewert geändert wird.

Absatz 2

In Parallele zu § 303 StGB wird auch der Versuch für strafbar erklärt.

§ 303 b StGB — Computersabotage —

Der Ausschuß schlägt die Aufnahme eines in den Entwürfen nicht enthaltenen Tatbestandes gegen „Computersabotage" vor, der Störungen der Datenverarbeitung in Wirtschaft und Verwaltung durch Eingriffe in Daten oder Sabotagehandlungen gegen Datenträger oder Datenverarbeitungshandlungen dann unter Strafe stellt, wenn die gestörte Datenverarbeitung für den Geschädigten von wesentlicher Bedeutung ist. Die zunehmende Bedeutung und Abhängigkeit von Wirtschaft und Verwaltung von einem störungsfreien Funktionieren der Datenverarbeitung, insbesondere in Rechenzentren, rechtfertigt die Einführung eines Tatbestandes gegen eine besonders gefährliche Form der Wirtschaftssabotage. Werden z. B. Buchführung und Lohnabrechnung in Rechenzentren lahmgelegt, so kann dies nicht nur zum wirtschaftlichen Ruin des Rechenzentrumsbetreibers, sondern auch der mit diesem zusammenarbeitenden Unternehmen führen (Mohr, DATEV, Prot. Nr. 26, S. 181). Dabei ist auch auf die Möglichkeit des unbefugten Eindringens Außenstehender hinzuweisen, die u. U. auch zu erheblichen Störungen führen kann.

In der öffentlichen Anhörung ist das geltende Recht (§ 303 StGB) und die in den Entwürfen vorgeschlagene sich auf Beweisdaten beschränkende Änderung des § 274 StGB als unzureichend kritisiert worden; dies gilt insbesondere für den Strafrahmen des § 303 StGB (vgl. Mohr und Oertel, Prot. S. 179 ff., 182 ff.; Anl. S. 36 ff., 218 ff.), welchem derjenige des § 303 a StGB entspricht (Freiheitsstrafe bis zu zwei Jahren). Mit diesen Tatbeständen kann den Auswirkungen einer Computersabotage auf Unternehmen und Behörden (trotz § 46 StGB) nicht hinreichend Rechnung getragen werden. Sieber (Prot. S. 177) hat zwar im Moment kein spezifisches Reformbedürfnis gesehen, aber selber eingeräumt, daß bei Störungen der Datenübertragung, bei Fehlbedienungen der Computerhardware und sonstigen Eingriffen in betriebliche Abläufe der Tatbestand der Sachbeschädigung bei der Erfassung der Betriebssabotage auf Schwierigkeiten stößt (Prot. Anl. S. 272).

Bei der Entscheidung für einen Sondertatbestand der Computersabotage hat der Ausschuß die Forderungen nach einem weitergehenden strafrechtlichen Schutz hochwertiger Wirtschafts- und Industriegüter vor Sabotage durch einen Straftatbestand gegen Betriebssabotage nicht übersehen. Abgesehen von der Schwierigkeit, einen praktikablen und ausreichend bestimmten Straftatbestand der Betriebssabotage zu bilden (vgl. auch den Hinweis von Sieber, Prot. Anl. S. 273), ist nach Ansicht des Ausschusses das derzeitige Bedürfnis für die Bildung eines Sondertatbestandes der Computersabotage stärker als das für die Einführung eines allgemeinen Sabotagetatbestandes.

Angesichts der bei schweren Fällen von Computersabotage leicht vorstellbaren hohen Schäden hält der Ausschuß es für notwendig, eine Höchststrafe von fünf Jahren Freiheitsstrafe vorzusehen.

Im einzelnen ist folgendes zu bemerken:

Absatz 1

Strafbar macht sich, wer eine für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde wesentliche Datenverarbeitung durch die in Nummern 1 und 2 genannten konkreten Angriffshandlungen stört. Der Begriff „Datenverarbeitung" ist dabei weit auszulegen. Er umfaßt nicht nur den einzelnen Datenverarbeitungsvorgang, sondern auch den weiteren Umgang mit Daten und deren Verwertung. Eingeschränkt wird der Tatbestand dadurch, daß die Datenverarbeitung „von wesentlicher Bedeutung" sein muß. Damit sind unter anderem Angriffe auf Daten (einschließlich ihrer Verarbeitung) erfaßt, die in den Rechenzentren von Groß-

unternehmen bzw. in Anlagen (einschließlich Datenträgern) gespeichert sind, welche die für die Funktionsfähigkeit von Unternehmen bzw. Behörden zentralen Informationen enthalten. Sabotageakte von untergeordneter Bedeutung fallen hierdurch bereits von vornherein nicht unter den Tatbestand; Beeinträchtigungen der Funktionsfähigkeit von elektronischen Schreibmaschinen oder Taschenrechnern werden dadurch ausgeschieden. Für die Anwendung des Tatbestandes ist eine bloße Gefährdung der Datenverarbeitung nicht ausreichend; vorliegen muß vielmehr eine nicht unerhebliche Beeinträchtigung des reibungslosen Ablaufs der genannten wesentlichen Datenverarbeitung. Eine Störung des Betriebes wie in § 316 b StGB wird jedoch nicht gefordert; eine zu starke Einengung des Tatbestandes soll dadurch vermieden werden. Nicht strafbar macht sich nach § 303b StGB derjenige, welcher durch Handlungen nach Nummern 1 oder 2 nur seine eigene Datenverarbeitung stört. Greift er hierbei in fremde Rechte ein, kann er insoweit nach § 303 bzw. 303 a StGB bestraft werden.

Hinsichtlich der einzelnen Angriffsmittel unterscheidet Absatz 1 zwischen verschiedenen Tatobjekten.

Nummer 1 nennt als Sabotagehandlung eine rechtswidrige Datenveränderung i. S. von § 303 a Abs. 1 StGB. Eine Tat nach Absatz 1 Nr. 1 stellt insoweit eine Qualifikation zu § 303 a StGB dar.

Nummer 2 knüpft bei der Nennung weiterer an Datenverarbeitungsanlagen oder Datenträgern begangenen Sabotagehandlungen am Tatbestand der Sachbeschädigung (§ 303 StGB) und an Sabotagestraftatbestände des Strafgesetzbuches an (§ 87 Abs. 2 Nr. 2; § 109 e Abs. 1; § 145 Abs. 2 Nr. 2; §§ 316 b, 317), womit auch eine Angleichung an Nummer 1 i. V. m. den in § 303 a StGB genannten Tathandlungen erfolgt. Die Begriffe „Zerstören" und „Beschädigen" decken sich mit denen des § 303 StGB. Die genannten Gegenstände sind „beseitigt", wenn sie aus dem Verfügungs- oder Gebrauchsbereich des Berechtigten entfernt sind. Sie sind „unbrauchbar", wenn ihre Gebrauchsfähigkeit so stark beeinträchtigt wird, daß sie nicht mehr ordnungsgemäß verwendet werden können, und „verändert", wenn ein vom bisherigen abweichender Zustand herbeigeführt wird. Der Ausschuß hat sich dafür entschieden, die Nummer 2 nicht nur als qualifizierte Sachbeschädigung auszugestalten. Auch dann, wenn sich die einzelnen Tathandlungen gegen eigene Sachen richten, soll die Nummer 2 anwendbar sein, wenn dadurch die wesentliche Datenverarbeitung eines dem Täter nicht gehörenden Unternehmens oder einer Behörde gestört wird. Für die Nummer 1 lassen sich ähnliche Ergebnisse durch eine entsprechende Auslegung des § 303 a StGB erreichen.

Absatz 2

Wie bei den §§ 303, 303 a StGB und den Sabotagetatbeständen der §§ 316 b, 317 StGB wird der Versuch für strafbar erklärt.

FEUER | NOTRUF

§ 303 Abs. 3; § 303 c StGB — Strafantrag —

Wie der bisherige § 303 StGB werden die §§ 303 a und 303 b StGB grundsätzlich als Antragsdelikt ausgestaltet. Ausnahmsweise kann in Fällen besonderen öffentlichen Interesses ein Strafverfahren auch ohne Strafantrag durchgeführt werden. Die Identität der Regelung für die §§ 303 bis 303 b StGB hat den Ausschuß bewogen, diese im Anschluß daran in einen neuen § 303 c StGB aufzunehmen (vgl. als Parallele § 205 StGB). Die Aufhebung des § 303 Abs. 3 StGB stellt dazu eine Folgeänderung dar.

Kurzmeldungen

Kurzmeldungen Kurzmeldungen

(Bild: Harald, aus taz)

Atom-Kataster

Ein störsicheres Strahlungsmeßprogramm auf Heimcomputern wie VC20 und C64 fahren mehrere Bürgerinitiativen. Derzeit werden erst ein paar der bundesdeutschen Atomkraftwerke überwacht.

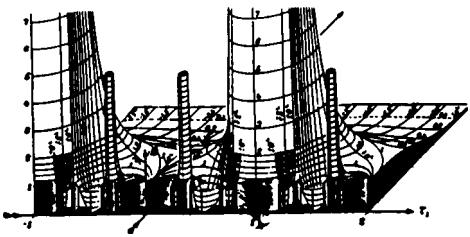
Vor Tschernobyl wurden diese mit Computern arbeitenden Initiativen oft genauso argwöhnisch betrachtet wie die Atomkraftwerke. Jetzt ist das Verhältnis entspannt.
Als Hardware vor Ort dient ein VC20 mit Datasette, Drucker, Echtzeituhr, Netz- und Batteriebetrieb.
Am Userport hängen Meßfühler für Wind, Wetter und Strahlung.
Ein C64 bildet das örtliche Kleinarchiv, eine 520er Aufrüstung teils in Planung.
Zum mobilen Meßkit gehört Kompaß mit Visiereinrichtung auf Kamerastativ: Kühlturm bekannten Formats anpeilen, dann Standortbestimmung auf Meßtischblatt.
Wettermessung ist eine wichtige Voraussetzung für verläßliche Strahlungsdaten. Feinmechaniker stellten benötigte Präzisionsteile bei befreundeten Firmen her.
Der Batteriebetrieb ermöglicht nahezu störungsfreien Betrieb auch bei Ausfällen des Stromnetzes.
Meßdaten werden archiviert und bundesweit ausgewertet.
Derzeit bilden sich an verschiedenen anderen Standorten der Kernspaltung in den Bürgerinitiativen weitere Meß-Initiativen mit dem Ziel, ein bundesweites öffentliches Atomkataster zu erstellen. (crd8606291700)

_____ dsPE	2,50 DM	___'__	Probeexemplar ds-aktuell
			Ein Abo bringt Unbekanntes öfter!
_____ dsL1	999,99 DM	___'__	Lebensabo ds (wer oder was lebt länger?)
_____ dsF1	ab 100 DM	___'__	Förderabo 8 Ausgaben
_____ dsN1	60,00 DM	___'__	Jahresabo 8 A. Normalverdiener
_____ dsS1	30,00 DM	___'__	Sonderabo 8 A. NUR Schüler u.a.!!!
_____ dsH0	60,00 DM	___'__	Sonderabo und Hackerbibel Teil 1
			dsPE-dsH0 jeweils inkl. Porto/Verp.

13

(Bild umgesägter E-Mast)
Stillstand nach Stromausfall

"Sägende Sofortabschalter", die - abgesehen von der Gesetzeslage - teilweise ziemlich leichtsinnig Strommasten umlegen (immerhin AKW-Notabschalttest, dazu zehntausende Volt Schrittspannung) veranlaßten kürzlich einige Hamburger Großrechenzentren, ihre Wiederanlauffähigkeit nach Kurzzeitstromausfall zu testen. Bei zumindest zwei Rechenzentren erwies sich das System als verbesserungsbedürftig. (crd8606291702)



Reliefdarstellung der elliptischen Modulfunktion

Fünf Jahre Chaos - Ende offen

Vor genau 5 Jahren (11./12. September 1981) fand in Berlin das erste Treffen des CCC statt. "Mißtraut Aktentaschen und Kartons" war die Überschrift einer Berliner Tageszeitung damals.

Seit Frühjahr 1984 gibt es die datenschleuder. Angefangen hat es mit vier Seiten A4, die jetzige Ausgabe umfaßt immerhin 16 Seiten. Die kleine Schrift (dichtgepackte Information) brachte Gerüchte, wir würden vom Optikerverband unterstützt. Das regelmäßige Erscheinen wurde trotz guter Vorsätze bisher nicht erreicht, gelegentlich wurde die ds schon totgeglaubt.

Eintreffende Briefe mit bösen Forderungen und Drohungen zB wegen "Nichtlieferung" von Abo usw. werden mit Verweis auf das Chaos und Rückerstattung beantwortet. Die ds erscheint öfter, wenn konstruktivere Textbeiträge hier eingehen. Wir tun unser bestes, auch wenn es manchen nicht reicht. Finanzielle Bereicherung, wie Unwissende unterstellen, liegt nicht vor. Wir brauchen im Gegenteil Spenden. Es gibt kaum noch Zeitschriften, die nicht von Werbung abhängig sind.

Die datenschleuder ist von Lesern abhängig und freuen uns über jede Unterstützung.

ds-red.

NUI OFF

Welcher Kopplerbesitzer hat noch nicht mit dem Gedanken gespielt sich auch einmal im Datex P-Netz der Deutschen Bundespost zu versuchen ?! So auch ich. Also nichts wie ran ans Telefon, Fernmeldeamt angerufen und ein Antragsformular für eine Network-User-Identifikation (NUI) beantragt. Nach zwei falschen Antragsformularen kam dann auch nach ca. 10 tagen daß heißersehnte Papier. Ausfüllen und wieder abschicken wurde auf der Stelle erledigt. Als die NUI dann nach einiger Zeit per Einschreiben zugestellt wurde, konnte ich es gar nicht abwarten den Rechner einzuschalten. Kurz nochmal die mitgespeicherte Datex P-Anleitung einer der Mailboxen 'durchgelesen, ein paar NUA's (Network-User-Adress) aus derselben Mailbox notiert, und dann gings los. Doch was ist das ?? Da will doch dieser blöde Rechner, der in diesem Fall in England stand, auch noch einen Usernamen und ein Passwort wissen. Nach einigen Fehlversuchen probierte ich es in den USA, aber die wollten ihre Daten auch nicht kostenlos herausgeben. Da stand ich nun mit meinem Latein und meiner NUI. Da meine Englischkenntnisse auch nicht gerade die eines Engländers waren, gab ich es erstmal wieder auf. Ich sagte mir, die 15 DM im Monat werd ich auch noch verkraften, vielleicht lern ich in sachen Datex ja nochmal was dazu, und dann könnte ich die NUI sicher nochmal gebrauchen. Als ich nun nach zwei Monaten immer noch keine Gebührenabrechnung vom Fernmeldeamt bekommen hatte, wunderte ich mich zwar, dachte mir aber nichts dabei. Der große Schock kam erst nach gut drei Monaten. Und zwar in Form einer Fernmelderechnung über 1090.13 DM. Da mußte ich erstmal schlucken. Als sich die ersten Schluckkrämpfe gelegt hatten rief ich natürlich sofort bei der Fernmelderechnungsstelle an um die Rechnung überprüfen zu lassen. Die Dame am Telefon wusste allerdings nichts von so einer Rechnungssumme. Lediglich eine Summe von ca. 80.- DM sei ihr bekannt. Nun, das hörte sich ja schon ganz gut an, mit etwa so einer Summe hatte ich auch gerechnet. Doch plötzlich verwandelte sich meine Erleichterung in die bekannten Schluckstörungen. Die freundliche Dame teilte mir mit daß da nachträglich noch etwas 'von Hand' auf meiner Rechnung geändert worden wäre (was immer das auch heißen mochte). Sie verwies mich dann an die zuständige Stelle für Datex-P. Die konnten mir aber leider auch nicht helfen, wollten aber, wenn ich gleich vorbeikommen würde, meine NUI noch am selben Tag sperren. Ich also hin, NUI zu sofort gekündigt und gefragt was ich denn nun machen könne. Man sagte mir daß man versuchen wollte die Gebühren zu überprüfen. Mit der Versicherung daß die NUI noch am gleichen Tag gesperrt würde fuhr ich also wieder nach Hause. Als ich nach etwa einer Woche immer noch nichts vom Fernmeldeamt gehört hatte kam mir Samstagnachmittag beim Frühstücken der Gedanke mal den Pad anzurufen und die NUI auszuprobieren. Ich dachte mich tritt ein Pferd.: Teilnehmerkennung DTAMMANY aktiv !!! Daraufhin probierte ich natürlich noch mehrere Male und bekam bis Montagmorgen noch die Aktivmeldung. Auf den sofortigen Anruf beim Fernmeldeamt wurde mir geantwortet daß man NUI's nur von Sonntag auf Montag sperren könne und am letzten Sonntag die dafür benötigten 'Speicherplätze' schon belegt gewesen wären.... Nach ca. vier Wochen bekam ich dann einen Anruf vom Fernmeldeamt in dem man mir mitteilte daß mir die Gebührenaufstellung die ich beantragt hatte nicht zustellen könne, mir bliebe aber freigestellt die Aufstellung im Amt einzusehen. Jenes würde aber nochmal zwei wochen dauern, da die Aufstellung noch nicht da sei. Nach abermals drei Wochen klingelte dann endlich das Telefon. Ziemlich kleinlaut erklärte mir die Dame am Apparat daß man angewiesen worden wäre mir 990.- DM zu erstatten, da im Datex-System ein Softwarefehler gewesen wäre. Was das nun ist wußte sie natürlich nicht und sie hatte von Datex-P natürlich auch keine Ahnung, da müßte ich mich schon an die dafür zuständige Stelle wenden..... Ich legte dann auf und dachte darüber nach was wohl einige größere Firmen gemacht haben die diesem 'Softwarefehler' zum Opfer fielen ? So ein Fehler tritt ja nicht nur bei einem auf. Ich nehme an sie haben ihren Mitarbeitern gesagt sie sollen nicht soviel telefonieren (wenn ihnen die erhöhte Summe überhaupt aufgefallen ist) und haben ohne zu zögern die Rechnung bezahlt.

nuioff.ws 19860416 1900 SSB/Sy

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club

Datenschleuder

Chaos Communication Center — Fragen & Antworten

Wie komme ich auf die CCC-Mailbox?

— nur als Mitglied
— durch Antrag (siehe rechts)
— ich brauche ein Girokonto

Wie werde ich Mitglied?

— Durch Antrag (siehe rechts)

Was wollt ihr?

— aktive Mitarbeit und/oder Unterstützung
— zwanzig Mark Aufnahmegebühr (Verwaltung)
— von Schülern und Studenten sechzig Mark im Jahr
— von anderen einhundertzwanzig Mark im Jahr

Warum brauche ich ein Girokonto?

Die Abrechnung der Mailboxkosten geschieht im Einzugsverfahren. Anders ist die Verwaltungsarbeit für uns zu kompliziert. Viele „Kreditinstitute führen kostenfreie Schülergirokonten (meist ohne Magnetkarte), sollten Euch eure Lehrnmittelgeldverwalter nicht fördern.

Was kostet die CCC-Mailbox?

Grundgebühr inklusive 47 Freiminuten monatlich DM 8,-. Die werden jeden Monat eingezogen.
Die Bank erhält eine Floppy von uns.

Dazu kommen bei Bedarf:

jede weitere Anschaltminute	15 Pfg
je versendete Nachricht im CCC-System	7 Pfg
je Telefonalarm (BRD)	80 Pfg

desweiteren leider nach Geldbeutel:

— Datenbankgebühren je nach Datenbankabfrage
— Telex, Telexgebühren plus geringer Zeitgebühr
— Nachrichten in andere Systeme, Datex-P Zuschlag.

Hääää?

Ihr erreicht das CCC-System über einen Telefonport (Bremen) oder mehrere Datex-P Zugänge. Für DM 8,- habt ihr einen Eintrag auf dem CCC-System. Die Nutzungsgebühren innerhalb des Systems sind preiswert. Teurer werden Datenbankdienste, Telex und Intermailverbindungen zu anderen Mailboxsystemen. Die werden je nach Aufwand weiterberechnet.

Was verdient der CCC daran?

Nix.
Die Mailboxgebühren werden ohne Aufschlag weitergegeben.

Was habe ich zu beachten?

Für die Mailbox wird derzeit die Nutzungsordnung vom Chaos Computer Club erstellt. Sie regelt das Teilnehmerverhältnis entsprechend den Vertragsbedingungen für die Benutzung des INFEX-Systemes. Wesentliche Punkte enthält dieser Beitrag.

Was passiert nun?

1. Ich fülle den Antrag rechts kräftig aus!
2. Wir stimmen meist zu.
3. Der Beitrag wird überwiesen, eingezogen oder gebracht.
4. Liegt eine Einzugsermächtigung vor, stellen wir auf Wunsch einen Eintrag im CCC-System zur Verfügung.
5. Weitere Leistungen für Mitglieder können nicht ausgeschlossen werden und sind beabsichtigt.

Wie komme ich wieder raus?

Aus dem CCC nur einmal im Jahr mit dreimonatiger Vorwarnung. Aus der Mailbox mit drei Monaten Kündigungszeit.

CHAOS-TEAM

Chaos Communication Congress 1986

28. + 29. Dezember

Durch das verlängerte Weihnachtswochendende ergibt sich diesmal kein Wochenendtermin. Die Aufbauarbeiten in den Räumen des Eidelstedter Bürgerhauses beginnen am Samstag dem 27. Dezember. Ab Sonntag können Arbeitsgruppen, Hilfskräfte und Teilnehmer anreisen. Übernachtungsmöglichkeiten werden vom Sonntag bis Dienstag bereitgehalten.
Der Congress wird am Montag um 10 Uhr eröffnet und endet Dienstag gegen 22 Uhr.
Anregungen für Themenbereiche, sowie Referenten sind willkommen (Fernmündlich 040/483752 Leitstelle 23 — da meldet sich ein MENSCH!). Weitere Informationen sowie die Teilnahmebedingungen werden zum August in der *datenschleuder* bekanntgegeben.

ls23

DV-unterstützter Informationsaustausch

Auf der Basis der Erfahrung mit Mailbox-Systemen in den USA, die dort grenzüberschreitend Informationsaustausch für Oppositionsgruppen betreiben, sollen diese auch in Deutschland verstärkt genutzt werden. ***Insbesondere die Koordinationserfahrungen, die man mit der Datenkommunikation in den USA für Besetzungsplanung von öffentlichen Gebäuden*** in über 30 Städten gewonnen hatte, hat die linke Szene in der Bundesrepublik aufmerken lassen. Auf schnellstem Wege hatten bei dieser spektakulären Aktion die Besetzer untereinander Informationen austauschen können und ihr Verhalten gegenüber den Sicherheitsbehörden koordiniert.

Aus: SICHERHEITS-BERATER, S.133 (Handelsblattverlach)

Chaos Communication Center — Hintergrundinfo

Der CCC schafft einen elektronischen Treffpunkt als Forum für seine Mitglieder und wählte als Werkzeug GeoNet, das derzeit ausgereifteste Mailboxsystem in Europa. Als Betreiber machte die Bremer Infex GmbH das beste Angebot.
Die Infex GmbH stellt dem CCC Systemanteile auf einem nur von Vereinen genutztem Mailboxsystem zur Verfügung. Die Einzelabrechnungen der Teilnehmer werden nicht vom Betreiber (Infex), sondern vom CCC durchgeführt. So ist es möglich, kostengünstig ein GeoNet-Mailboxsystem im Rahmen der CCC Mitarbeit zu gebrauchen.
Die GeoNet Mailboxsysteme werden derzeit in der Bundesrepublik neben der Infex auch von der Deutschen Mailbox kommerziell betrieben. Die Österreichische Post hat sich, im Gegensatz zur Bundespost, für ein GeoNet Mailboxsystem entschieden. Durch die relativ hohe Kostenschranke von ca. DM 40,- Grundgebühr konnten sich bisher nur Firmen den Komfort eines solchen Systems leisten.
Der CCC ermöglicht bei Mindestnutzung des Systems für Mitglieder Nutzungskosten von DM 8,- im Monat.
"Die im GeoMail-Verbund jetzt zusammenarbeitenden mehreren Tausend Benutzer repräsentieren eine sehr heterogene und internationale Leserschaft mit Querverbindungen zu vielen anderen elektronischen Medien und damit zu einer **Grass Root Population** (elektronische Eingeborene) von aufgeschlossenen Menschen, die nicht nur passiv Nachrichten konsumieren, sondern sie dank des Mediums MAILBOX *aktiv und aufwandsarm kommentieren können. Es ist diese neue Fähigkeit, die Mailbox-Systeme so grundlegend anders machen, als traditionelle Kommunikations-Medien"* (Günter Leue, GeoNet)

Grundsätzliche Merkmale des CCC-Systems

— Zugriff über das Ferngespräch (1 Port / 37n1d)
— Zugriff über das Datex-P Netz (7 Ports)

— mehrsprachige befehlsorientierte Dialogführung
— gleichzeitiger Zugriff durch 8 Hacker
— zeitgesteuerte Verwaltung von 23 persönlichen Bitbergen
— Schwarze Bretter, themenbezogene Infosammelplätze
— clubbezogen und zu allgemeinen Interessen
— Nachrichtenaustausch mit Teilnehmern oder Schwarzen Brettern in anderen GeoNet-Systemem im In- und Ausland
— Dialogmöglichkeit anwesender Teilnehmer
— Findefunktionen für Nachrichten und Verzeichnisse
— Telefonsklave zur Alarmierung von Teilnehmern bei wichtiger Post

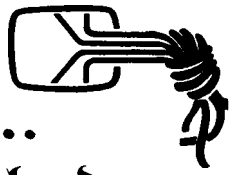
— Versand und Erhalt von Telexen (derzeit nur weltweit)
— Zugriff auf Datenbanken, Presseagenturen. . .

Neben dem CCC werden zwei weitere Vereine und einige Wissenschaftlergruppen gemeinsam, in einem Mailbox-Gremium, das System gestalten.
Der CCC wird die Clubarbeit und den Kontakt unter den Mitgliedern aus aller Welt auf seinem elektronischem Clubcenter, dem **CHAOS COMMUNICATION CENTER,** abwickeln.

ev2.txt

Für die Teilnahme am *Chaos Communication Center*
Ich/Wir wollen Teilnehmer auf dem Chaos Communication Center, der Club-Mailbox, werden. (nur mit Einzugsermächtigung)
Benutzername: ..... (max. 15 Stellen, nur A—Z als erstes Zeichen, danach Telexzeichenvorrat ohne Umlaute).
Kennwort zur Einrichtung: ..... (mindestens 6 Stellen)
Bei Teilnahme erkenne ich die Nutzungsbedingungen für das Chaos Communication Center an. Die Nutzungsgebühren von mindestens DM 8,— werden monatlich abgebucht.

.....
Unterschrift, bei Minderjährigen die des gesetzlichen Vertreters



Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club

Verlangen nach Mitgliedschaft im Chaos Computer Club e.V.

An Leitstelle eVA, Schwenckestraße 85, D—2000 Hamburg 20
Ich verlange Mitglied im © © © eV zu werden.

Vor/Zuname: .....
Hilfszeile: .....
Straße/POB: .....
LKZ—PLZ Ort: .....
Telefon/Mbx: .....

- Ich bin Schüler, Student oder einkommensgleichgestellt und steuere die Entwicklung durch einen Beitrag von DM 60,— jährlich.
- Ich steuere die Entwicklung mit 120,— DM jährlich.
- Wir möchten (förderndes) Mitglied werden. Bei Körperschaften stimmberechtigte Kontaktperson: .....
  Rufnummer: .....

Für Mitglieder (oder welche, die es werden möchten)

- Ich möchte einen Erfa-Kreis bilden.
  Thema: .....
  .....
- Bitte sendet mir die *datenschleuder*
- Ich bin *datenschleuder*-Abonnent
- Ich wünsche mir einen maschinenschreibbaren Mitglieds ausweis (vorgesehen)

Angaben zur Verwaltung
Ich zahle meine Mitgliedsbeiträge als Scheck, bar oder via Überweisung *nur* Postgiro Hmbg BLZ 200 100 20 Kto. .....
☐ jährlich ☐ halbjährlich

Ihr dürft die Mitgliedsbeiträge abbuchen,
☐ jährlich ☐ halbjährlich

Die Satzung des CCC erkenne ich an. Die Aufnahmegebühr von DM 20,— habe ich beigefügt (Bearbeitung sonst nicht möglich).

.....
Unterschrift, bei Minderjährigen die des gesetzlichen Vertreters

Einzugsermächtigung. Das Mitglied ermächtigt den CCC eV widerruflich, die Mitgliedsbeiträge jährlich oder halbjährlich sowie die Nutzungsgebühren für das Chaos Communication Center monatlich abbuchen zu lassen.

Postleitzahl, Ort, Datum

Datenschutzhinweis: Die Daten werden während der Mitgliedschaft zur maschinellen eV-Verarbeitung gespeichert.

Name de/r/s Chaos Teilnehmer/in/s von nachstehend angegebenem Konto einzuziehen beim Postgiroamt

Einzugsermächtigung

A 2 ZA Postgirokonto-Nr. —

B 3 ZA Girokonto-Nr. Bankleitzahl des Kreditinstituts

Name und Anschrift des Kreditinstitutes

Das Konto wird beim Geldinstitut unter folgender Bezeichnung geführt (Name des Kontoinhabers)

Von den Hinweisen der Deutschen Bundespost für die Teilnahme am Lastschrifteinzug habe ich Kenntnis genommen.

Wird vom Amt für Chaos geprüft

ggf. SA 80 geprüft	SA 00 geprüft

Unterschrift de/r/s Kontoinhaber/in/s

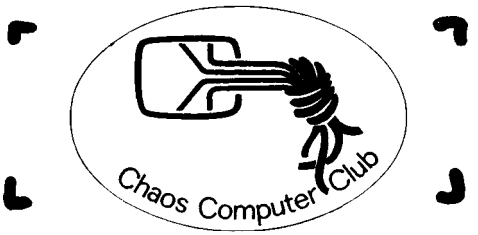
Datenschleuder

Wenn unzustellbar. Anschriftenausschnitt bitte mit neuer Adresse zurück

D-2000 Hamburg 20
Schwenckestraße 85

Geonet: Geo1:Chaos-Team
Btx: *655321#

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club



Chaos Computer Club
Partner auf dem Weg zur Informationsgesellschaft.

Mit Wirkung vom 14. April 1986 wurde der Chaos Computer Club e.V. unter der Nummer 10940 beim Amtsgericht Hamburg in das Vereinsregister eingetragen.

Es begann 1981! mit einem Treffen von Computerfreaks in Berlin. Die ersten Personal Computer eroberten die Büros und waren zu erschwinglichen Preisen im Handel.

Man wollte Informationen tauschen, doch gab es damals kaum Möglichkeiten dafür. Die Bundesrepublik war auf diesem Gebiet ein Entwicklungsland.

Im Februar 1984 erschien die *datenschleuder* mit Informationen für die Szene, die sich als "wissenschaftlich" bezeichnet, für die aber auch Bezeichnungen wie "Underground-Postille" und "Hackerschmierblatt" verwendet werden: *das* Fachblatt für Datenreisende.

Seitdem bemüht sich ein offener Kreis von Leuten darum, Informationen über die Verwendung der Technik — insbesondere Neuer Medien — zu sammeln und zugänglich zu machen: **Bürgerhilfe im Technikdschungel.**

Durch die spektakuläre Btx-Aktion des CCC im September '84 (Verbraucherschutzaktion 134.000,- bei der Haspa) erregte der Club bundesweites Aufsehen.

Leider sind wesentliche Aktivitäten des CCC im Medientrubel untergangen oder wurden fälschlich dargestellt.

Teile der Presse schreiben **"Hacker"** in Gänsefüßchen und verkaufen sie als Computerterroristen und gefährliche Datenräuber. Während mit einer Hacker-Panik noch Zeitschriftenumsätze geschürt werden und ängstliche Anwender von cleveren "Beratern" die bedenklichsten Sicherungssysteme aufgedrückt bekommen, und viele den Computer verteufeln, zieht die Informationsgesellschaft kaum bemerkt in unsere Kinderzimmer ein.

Hacker sind neugierige Reisende im modernen Alltag. Forscher und Menschen, die sehr bewußt — und offen — mit Neuen Technologien umgehen.

Computerkriminelle haben im Gegensatz dazu Geheimhaltungsprobleme und Bereicherungsabsichten.

Die Gesetzgebung zur Computerkriminalität trägt dem auch Rechnung.

Die Älteren und die deutsche Industrie betrachten erstaunt die Entwicklung, manche fassungs- und tatenlos. Andere begreifen, was los ist. **Insgesamt wächst das Bewußtsein um Daten**un**sicherheit** ***stetig, aber langsam.***

Zum Herbst '85 stellte der CCC sein **Wissen in der Hackerbibel** Teil 1 zusammen (Die Hackerbibel ISBN 3-922708-98-6). Das 256 Seiten umfassende Werk wurde bisher über 3500 mal zu einem "sozialem" Preis von ca. 13 Pfennig die A4-Seite vertrieben.

Zweimal bisher, jeweils zum Jahreswechsel, veranstaltete der CCC den Chaos Communication Congress. Das jährliche internationale Treffen von über 400 Datenreisenden führte interessierte Menschen zusammen und verdeutlichte die Lage: Wenig Informationen, kaum technologische Förderung der Jugend, keine Erfahrung über die **Sozialverträglichkeit** neuer Technologien.

Darin spiegelt sich auch die **Rasanz der Entwicklung.**

Modernes Opfer

dpa Heilbronn **Die Verwechslung zweier Adapterstecker hat in der Heilbronner Kinderklinik zum Tod eines 16 Monate alten Mädchens geführt. Eine Krankenschwester hatte Meßelektroden eines Gerätes, das das Herz überwacht, an einen Infusomaten angeschlossen. Das Baby bekam einen Stromschlag von 220 Volt.** *(Hmb. Abdbl. 2.5.86)*

"Die Informationsgesellschaft unserer Tage ist ohne Computer nicht mehr denkbar. Die Einsatzmöglichkeiten der automatisierten Datenverarbeitung und Datenübermittlung bergen Chancen, aber auch Gefahren für den Einzelnen und für die Gesellschaft. (Präambel der CCC Satzung)

Das große Informationsbedürfnis in der Bevölkerung überflutete das Chaos-Team mit Bergen von Anfragen, aber auch Verwaltungsarbeiten. Die Aboabteilung der Datenschleuder erwies sich als ein kraftsaugendes schwarzes Loch. Dem CCC fehlt es an einem tatkräftigen Sekretariat plus Computern. Auch die Clubräume in Hamburg (Anlaufadressse, Redaktionsräume und Tagung von Erfahrungsaustauschkreisen) stellen den Club vor finanzielle, organisatorische und rechtliche Probleme.

Zahlreiche Anfragen, zur Teilnahme an öffentlichen Informationsveranstaltungen rund um Informations- und Kommunikationstechniken, Verbraucherschutz sowie den Einsatz sozialverträglicher Technologien drohten die Kapazitäten der hamburger Gruppe zu sprengen.

Einziger Ausweg ist die Offensive, die Gründung eines Vereines. Dadurch ist es dem CCC möglich, jedem Mitglied die Nutzung eines Mailbox- und Informationssystemes zugänglich zu machen. Der CCC bietet ein Forum zum elektronischem Informationsaustausch auf internationaler Ebene.

„Nach uns die Zukunft: vielfältig uns abwechslungsreich durch Ausbildung und Praxis im richtigem Umgang mit Computern. Wir verwirklichen soweit wie möglich das NEUE Menschenrecht auf zumindest weltweiten freien, unbehinderten und nicht kontrollierbaren Informationsaustausch unter ausnahmslos allen Lebewesen.

Computer sind dabei eine nicht wieder abschaffbare Voraussetzung. **Computer sind Spiel-, Werk-, und Denk-Zeug; vor allem aber: "das wichtigste neue Medium".** Zur Erklärung: Jahrhunderte nach den "Print"-Medien wie Bücher, Zeitschriften und Zeitungen enstanden Medien zur globalen Verbreitung von Bild und Ton; also Foto, Film, Radio und Fernsehen. Das entscheidenste heutige neue Medium ist der Computer. Mit seiner Hilfe lassen sich **Informationen "über alles denkbare" in dieser Galaxis** übermitteln und — kraft des Verstandes — wird neues geschaffen." (Aus der Datenschleuder 1, Februar 1984).

Bildschirmtext hat gezeigt, daß man ein 2-Klassen-System (Anbieter und Abrufer) keinem bewußtem Menschen zumuten kann. Mailbox-Systeme kennen nur eine Klasse. Jeder Teilnehmer kann Informationen abrufen, kommentieren oder selber welche über die Schwarzen Bretter anbieten.

Eine Mitgliedschaft im CCC e.V. ermöglicht die Teilnahme am Nachrichtenverkehr auf einem **Geonet-System** zu Preisen der **Wunschmaschine** Bildschirmtext. Alle **Mailbox-Teilnehmer sind gleichberechtigte** Informationsanbieter in einem Informationsbasar rund um Wissenschaft, Technik und alles was Spaß macht und wenig kostet. *Kommerzielle Aktivitäten der Mitglieder sind dort unerwünscht.*

"Der Chaos Computer Club ist eine galaktische Gemeinschaft von Lebewesen, unabhängig von Alter, Geschlecht und Rasse sowie gesellschaftlicher Stellung, die sich grenzüberschreitend für Informationsfreiheit einsetzt und mit den Auswirkungen von Technologien auf die Gesellschaft sowie das einzelne Lebewesen beschäftigt und das Wissen um diese Entwicklung fördert." (CCC-Satzung).

Der CCC behält seine offene Struktur. Er bietet Interessierten mehr als ein Forum: *Mit uns die Zukunft!*