ISSN 0930-1054

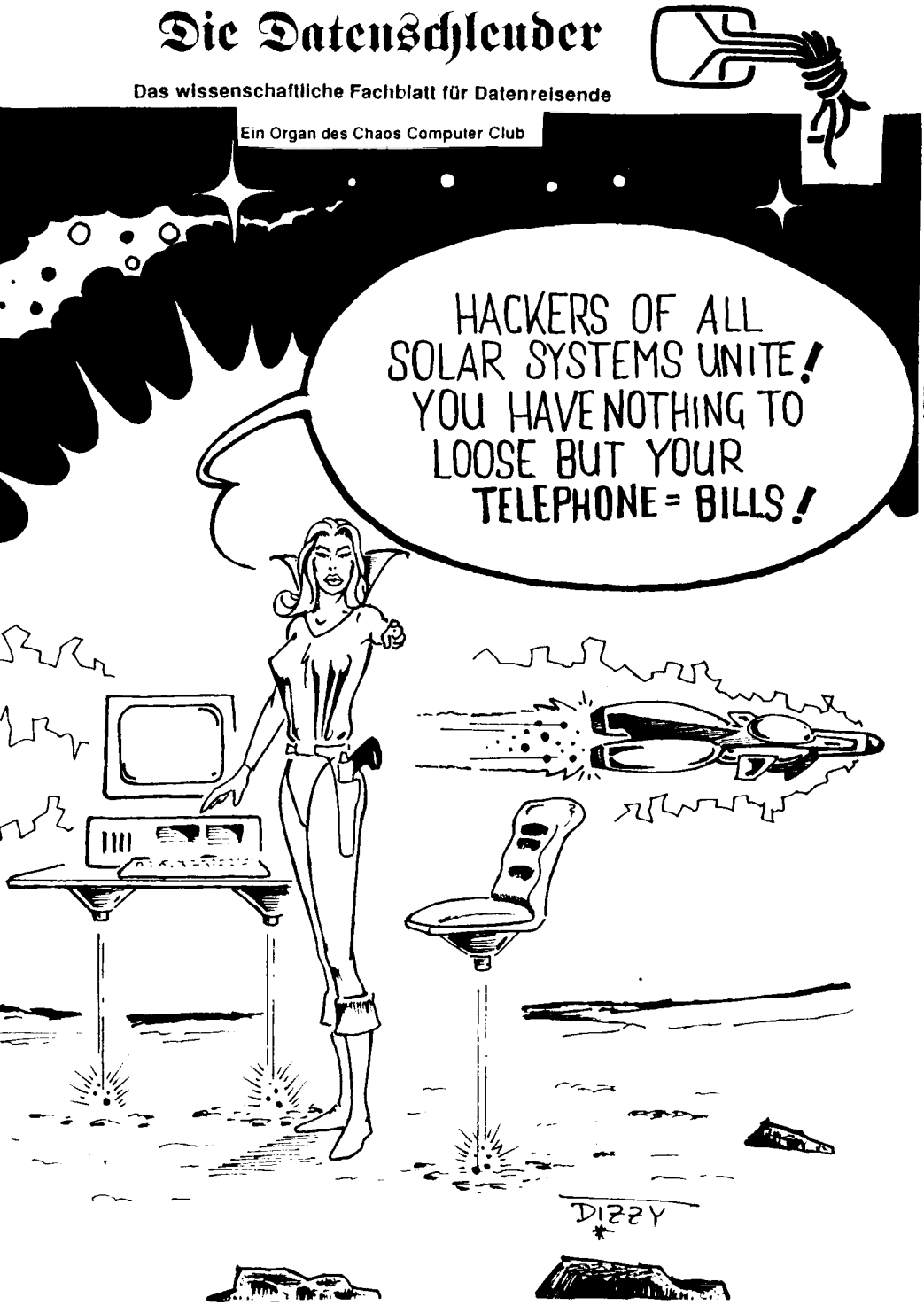
KOSTAQUANTA: DREIFUFFZICH

Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende

Ein Organ des Chaos Computer Club

NUMMER 31, NOVEMBER/DEZEMBER 1989



ADRESSEN:

HOTLIST

BHP - Die Bayrische Hackerpost. Treffen sich immernoch irgendwann irgendwo in wohl mehr oder weniger regelmaessigen Abstaenden in Muenchen.
Briefpost: BHP, c/o Basis, Adalbertstr. 41b, 8000 Muenchen 40

CHAOS-HH - Chaos Computer Club Hamburg. Treffen woechentlich Dienstags 19 Uhr Mailbox CHAOS-HH unter 040 4911085 (12/24 8N1). Voice 490 37 57.
Briefpost: CCC-HH, Schwenckestrasse 85, 2000 Hamburg 20

CHAOS-HL - Chaos Computer Club Luebeck. Treffs jeweils am ersten und dritten Freitag im Monat 19 Uhr in der Roehre (gerade Querstrasse, geht von der Mengstr. ab). Erreichbar ueber die MAFIA(.ZER) Mailbox. (0451 31642 / 3/12/24 8N1): CCC-HL. Voice 0451 865571.
Briefpost: CHAOS-HL, Lachswehrallee 31, 2400 Luebeck

CHAOS-RN - Chaos Computer Club Rhein-Neckar. Treffen unklar. Telefonnumer auch. Existenz inzwischen zu 42.23% gewiss. Mailbox CHAOS-RN, Rufnummer unklar.
Briefpost: CCC-RN, Postfach 104027, 6900 Heidelberg

Aufklärung in letzter Sekunde:
CHAOS-RN Treffen Dienstags 19 Uhr im Hookemann, Heidelberg-Fischmarkt.

FOEBUD-BI - Verein zur Foerderung des oeffentlichen bewegten und unbewegten Datenverkehrs e.V. Bielefeld. Tel.: 0521 175254 di-fr 14-18 h. Treffen Dienstags 19 Uhr im EXTRA, Siekerstr. 20. Mailbox BIONIC (0521 171188 / 12/24 8N1). Monatliche "Public Domain" Veranstal- tung jew. am 1 Sonntag i.M. im Bunker Ulmenwall, Kreuzstr. 0, 48 Bl 1. Termine siehe BIONIC.
Briefpost: FoeBud e.V. / c/o art d'Ameublement, Marktstr. 18, 48 Bielefeld 1

SUECRATES-S - Stuttgarter Computerrunde mit Zeitschrift d'Hacketse. Garantiert keine Satzungsdebatten - Mitglied im Bundesverband gegen Vereinsmeierei e.V.
Kontakt/Info: C.PANTLE, SYSOP@CACHE.ZER, oder per Briefpost: SUECRATES, c/o K.Raatz, Schuetzenstr. 39, 7000 Stuttgart 1 (GEO.: /LINKE: K.RAATZ). D'hacketse: Einzelpreis 3.-. Abo fuer acht Ausgaben 25.- DM

LABOR-HH - Zeitschrift fuer Worldprocessing. Chaos kompatibel. Treffen jew. am 1. Donnerstag im Monat - oder auch nicht. Erreichbar ueber labor@winsch.UUCP / LABOR@CHAOS-HH.ZER. Einzelpreise verschieden. Abo fuer 8 Ausgaben 42.- DM.
Offener Redaktionstreff und Briefpostadresse: LABOR, c/o Glaser, Hospitalstr. 61, 2000 Hamburg 50

Die Datenschleuder Nummer 31
- November/Dezember 1989
Das wissenschaftliche Fachblatt für Datenreisende.

Wir organisieren uns dezentral oder auch nicht, möglichst Kontakt mit lokalen Gruppen knüpfen. Mehroderweniger offizielle Redaktions-Anschrift: Redaktion DS, Schwenckestrasse 85, D-2000 Hamburg 20, Telefon 040 490 37 57, Geol/Ifx1/Mbk1: CHAOS-TEAM, DS-RED@CHAOS-HH.ZER, ccc@mcshh.UUCP, Btx *CHAOS*

IDAMTEPNSRCHELESUDSERUM

VisdP: Frank Simon

Mitarbeiter dieser Ausgabe in alphabetischer Reihenfolge: Alf, Andy, Cash, Henne, JWI, Nikolaus, Rowue, Tori, Terra sowie wie immer der unbekannte / vergessene Redakteur.

Nachdruck fuer **nichtgewerbliche** Zwecke bei Quellenangabe erlaubt.

EDITORIAL

Liebe DatenschleuderleserInnen,

Pannenberichterstattung faellt wegen Ueberreichlichkeit aus. Im Vergleich zum Erscheinen der letzten Aussabe ergibt sich eine realsozialistische Verdoppelung des Umfanges verbunden mit weit mehr als gleichzeitiger Viertelung des Produktionszeitraumes. Derartiges haelt auf Dauer keiner durch.

Die Zeit der Rauhnaechte naht und damit der chaostypische nachweihnachtliche Chaos Communication Congress. Mehr dazu in dieser Aussabe. Die naechste DS-Aussabe wird wohl wieder auf dem Kongress fertig werden. Wer aktiv wissen will, wie so eine Redaktion funktioniert, kann es bei der Kongressredaktion versuchen.

Die Kongressgaeste moegen die postamtlichen regionalen Telefonsebuehrenverzeichnisse mit Nah- und Fernzonenlisten mitbringen, damit eine BRD-Gesamtuebersicht (wichtig fuer kostensuenstige Vernetzung) auf Datentraeger erstellt werden kann.

Zudem wird der Chaos-Archivdienst zum Kongress eingehende (mitgebrachte) Dokumente umgehend ins Archiv integrieren und zum Kopieren bereitstellen.

Nachdem wieder verschiedene Universitaetsbibliotheken der DDR die Hackerbibel bestellt haben, meinen wir, diese KnowHow-Sammlung sollte auch in oeffentlichen Buechereien der DDR leihbar sein ebenso wie die Studie ber Computereinsatz bei den Gruenen. Die DS-Redaktion empfiehlt, das am besten selber zu organisieren ueber eigene Beziehungen/Buecherspenden in die DDR.

Die DDR-Besucher werden gebeten, technische Informationen und Dokumente ueber das DDR-Telefonsystem mitzubringen. Erste Kontakte zu Computerfreaks in der DDR bahnen sich an - und sollen schliesslich zu Netzwerkverbindungen fuehren.

read inhaltsverzeichniss : goto nextpage

Andy / Wau

Inhaltsverzeichniss

Mailboxen unter Kontrolle der Geheimdienste

Die Telekommunikationsanbieter sollen zum verlängerten Arm von Polizei und Geheimdiensten gemacht werden. Mit der Verabschiedung des Poststrukturgesetzes wurden - von der Öffentlichkeit kaum bemerkt - die Überwachungsmöglichkeiten durch Polizei und Geheimdienste bei Telekommunikationsdiensten erheblich erweitert.

Zur Abwehr von drohenden Gefahren für die freiheitlich demokratische Grundordnung dürfen die Verfassungsschutzbehörden (VS), der Militärische Abschirmdienst (MAD) und der Bundesnachrichtendienst (BND) den Tele kommunikationsverkehr überwachen und in beliebiger Form mit beliebigen Medien aufzeichnen und in beliebiger Form mit beliebigen Medien aufzeichnen (1). Dasselbe dürfen jetzt die Strafverfolgungsbehörden im strafrechtlicher Ermittlungen gem. Par. 100 a und 100 b StPO. Bislang durften der Fernmeldeverkehr nur auf Tonträger aufgenommen werden.

Damit sind die rechtlichen Voraussetzungen zur Anwendung jeder beliebigen Speicherungs- und Auswertungstechnik von Sprache und Daten durch die Geheimdienste und Strafverfolgungsbehörden geschaffen worden. Diese Techniken sind für die effektivere Überwachung digitalisierter Netze, insbesondere der Kommunikation im ISDN für die Geheimdienste von besonderem Interesse.

Bestimmte Überwachungsmethoden können eine neue Qualität erreichen. Bereits 1978 hat der Bundesnachrichtendienst einen bestimmten Prozentsatz des Post- und Fernmeldeverkehrs in die DDR mit folgendem Verfahren überwacht (2). Es werden regelmäaig computergesteuert Gespräche mitgeschnitten, in denen bestimmte Begriffe oder Silben enthalten sind. Diese Auswertungen sind nach einem Urteil des BVerfG von 1985 (3) nur verfassungsmäßig, weil es sich gem. § 3 G 10 um eine strategische Überwachung handele, die Sach- und nicht personenbezogen sei.

Die Partner der Gespräche blieben unbekannt, weil es im Fernsprechverkehr in der Regel technisch nicht möglich sei, die Gesprächspartner zu identifizieren, wenn sie nicht selbst, was selten genug der Fall sei, sich im Verlauf des Gespräches über ihre Identität äußern (4), so das BVerfG Im ISDN ist dies vermutlich nicht mehr der Fall, falls die Geheimdienste ihre Überwachungsmaßnahmen in den Vermittlungstellen durchführen. Zumindest sind über das Gesprächsende die Vermittlungsdaten rekonstruierbar. Die Gesprächs partner lassen sich über die Verbindungsdaten in den Vermittlungstellen identifizieren. Die strategische Überwachung gem. § 3 G 10 wäre im ISDN personenbeziehbar.

Mit den neuen Dienstleistungsangeboten wie TEMEX, Mailboxen, Pressedienste, elektronischen Bestellungen usw. auf der einen Seite und der Speicherung der Verbindungsdaten im Netz selbst durch die Post auf der anderen Seite, entstehen für automatisierte Überwachungsverfahren ganz neue Möglichkeiten.

Zudem muß jeder Telekommunikationsanbieter jetzt für die Geheimdienste tätig werden. Auf Anordnung des Innenminsters oder der zuständigen Länderbehörden müssen Telekommunikationsanbieter den Geheimdiensten und Strafverfolgungsbehörden Auskunft über den durchgeführten Fernmelde- und Datenverkehr erteilen, Sendungen die ihnen zur Übermittlung auf Telekommunikationsnetzen anvertraut worden sind, aushändigen und die Überwachung und Aufzeichnung des Telekommunikationsverkehrs ermöglichen (5).

Für die Durchführung muß jeder Telekommunikationsanbieter derartiger Maß nahmen Personal bereithalten, daß nach den Bestimmungen des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes vom Verfassungschutz überprüft ist und zum Zugang zu Verschlußsachen des jeweiligen Geheimhaltungsgrades ermächtigt ist (6). Damit muß jeder Telekommunikationsanbieter (z.B. Mailboxbetreiber) dem Verfassungsschutz mindestens eine Person zu nennen, die vom Verfassungsschutz sicherheitsüber prüft wird und aufgrund dieser Überprüfung die Berechtigung zum Zugang zu Verschlußsachen hat. Wer derartiges Personal nicht bereitstellt, kann mit einer Geldbuße bis zu 30.000.- DM bestraft werden (7). Jeder Telekommunikationsanbieter ist verpflichtet, dem Verfas-

sungschutz MitarbeiterInnen zu nennen, die dieser im Rahmen einer Sicherheitsüberprüfung ausschnüffeln darf und die für die Überwachungsmaßnahmen der Geheimdienste zur Verfügung stehen. Bei Anbietern, die Telekommunikationsdienstleistungen alleine oder zu zweit an bieten, kommt dies einer generellen Sicherheitsüberprüfung von Telekommunikationsanbietern durch den Verfassungsschutz gleich. Zudem können die zuständigen Stellen natürlich jederzeit die Überwachungsmaßnahmen mit eigenen Mitarbeitern durchführen.

Nach dieser Änderung des G 10 muß jeder Telekommunikationsanbieter und jeder Nutzer damit rechnen, daß die Geheimdienste auch rückwirkend sowohl die Herausgabe von Daten über Verbindungen, als auch den Inhalt z.B. von elektronischen Fächern in Mailboxen, verlangen können. Maßgeblich für die rückwirkende Herausgabe, ist der Zeitpunkt der Anordnung. Sie ergeht schriftlich und ist dem Telekommunikationsanbieter mitzuteilen. Sie sollte sich jeder Betroffene vorlegen lassen. Andernfalls ist weder Herausgabe noch Überwachung zulässig. Weiterhin muß jeder Telekommunikationsanbieter Überwachungs maßnahmen für die Zukunft bei Vorliegen einer Anordnung dulden. Diese ist auf höchstens drei Monate befristet und darf jeweils nur um drei Monate ver längert werden, falls die Vorraussetzungen der Anordnung fortbestehen.

Die vom Gesetz intendierten Überwachungsmaßnahmen richten sich dabei nicht primär gegen den Telekommunikationsanbieter, sondern gegen die Nutzer der Telekommunikationsdienste. Der Telekommunikationsanbieter wird im Falle von Überwachungsmaßnahmen einer besonderen Schweigepflicht unterworfen (8). Teilt er einem anderen die Tatsache der Überwachung mit, so kann mit Freiheitstrafe bis zu zwei Jahren bestraft werden.

Ein zynischer Wermutstropfen: Die Geheimdienste bezahlen alle Leistungen, die für sie im Rahmen von Überwachungsmaßnahmen erbracht werden (9).

(1) § 1 Abs. 1 G 10
(2) Vgl. Der Spiegel Nr. 47, 1978 S. 25
(3) BVerfGE 67, S.157.
(4) Vgl. BVerfGE 67, S.157 ff.
(5) § 1 Abs. 2 G 10.
(6) § 1 Abs. 2 G 10.
(7) § 11 Abs. 2 G 10.
(8) § 10 Abs.1 G 10.
(9) § 13 G 10.

Jochen Riess / Institut für Informatios- und Kommunikationsökologie

■■■ GESETZE

Postministerium: Neuregelung des Fernmeldegeheimnis gilt nicht für Mailbox-Systeme. Ausdehnung der Überwachungsmöglichkeit auf private Netzbetreiber stösst auf Kritik.

Hamburg/Bonn (emp/mik) - Die im Zuge der Postreform auf private Betreiber von Vermittlungseinrichtungen ausgedehnten Beschränkungen des Fernmeldegeheimnisses gelten nach Auskunft des Bundespostministeriums nicht für Mailbox-Systeme. Dies teilte das Ministerium der Oberpostdirektion Bremen auf Anfrage mit, nachdem verschiedene Bremer Mailbox-Betreiber ihr zuständiges Fernmeldeamt über die neue Rechtslage befragt hatten. Nach der Neufassung des Gesetzes zur Beschränkung des Fernmeldegeheimnisses, die seit dem 1. Juli 1989 gilt, ist nicht nur die Deutsche Bundespost, sondern auch jeder andere Betreiber öffentlicher Vermittlungseinrichtungen gesetzlich verpflichtet, den staatlichen Sicherheitsorganen die ihm anvertrauten Briefsendungen auszuhändigen und die Überwachung des Fernmeldeverkehrs zuzulassen. Private Kommunikations-Dienstleister müssen zudem Mitarbeiter benennen, die mit den Sicherheitsbehörden zusammenarbeiten und Verschlusssachen auf Anordnung aushändigen.

Nach allem was man weiss, so das Ministerium, fallen die Mailboxen nicht unter die Anmeldepflicht. Man habe weder Formulare für Mailboxen, noch gehe man davon aus, dass man die vielen Mailbox-Systeme überhaupt verwaltungstechnisch registrieren könnte - selbst wenn man wollte. Ferner sei der Begriff "Fernmeldeanlage" im Gesetz technisch und formal zu verstehen. Gemeint seien Vermittlungseinrichtungen. Zwar fallen Mailboxen auch unter Fernmeldeanlagen oder Fernmeldedienstleistungen, nicht aber unter den technischen Begriff der "Vermittlungseinrichtung". Dies gelte auch für vernetzte Mailbox-Systeme. Sollte sich an dieser Interpretation etwas ändern, werde das Ministerium darüber umgehend informieren.

weiter auf nächster Seite

Nach dem Gesetz droht dem Betreiber einer Vermittlungseinrichtung ein Bussgeld bis zu dreissigtausend Mark, wenn er sich weigert, mit Geheimdiensten und staatlichen Sicherheitsbehörden zusammenzuarbeiten. Als Weigerung wird angesehen, wenn Sendungen nicht aushändigt oder das Überwachen des Fernmeldeverkehrs nicht ermöglicht werden. Gleiches gilt für Betreiber, die keine Mitarbeiter stellen, die mit staatlichen Geheimdiensten zusammenarbeiten. Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe werden dem angedroht, der eine angeordnete Überwachung des Fernmeldeverkehrs anderen mitteilt.

Als "masslose Selbstüberschätzung" bezeichneten Bonner Rechtsexperten die Auffassung politischer Beobachter, die in der Neufassung des Gesetzes einen gezielten Seitenhieb auf den E-Mail-Bereich oder gar einzelne Nutzergruppen wie Umweltschützer oder linke Gruppen sehen wollen. In diesem Sinne hatte die Illustrierte Stern das Thema aufgegriffen. Das Blatt sprach von "Spitzeln in der Mailbox" und einer Reaktion bundesdeutscher Geheimdienste, denen die Mailbox-Szene "schon lange ein Dorn im Auge" gewesen sei. Wie das Bundespostministerium auf Anfrage erklärte, sei die Ausdehnung der Überwachungsmöglichkeiten auf private Betreiber eine Konsequenz der Poststrukturreform. Ohne die Neufassung wäre eine Situation entstanden, bei der nur die Deutsche Bundespost zur Offenlegung der Daten gegenüber Geheimdiensten verpflichtet wäre.

In einer von der GeoNet Mailbox Services GmbH Haunetal in Auftrag gegebenen Kurz-Analyse der neuen Bestimmungen heisst es unter anderem, dass die Verfasser des Gesetzes irrigerweise davon ausgegangen seien, dass künftig nur grosse, institutionalisierte Anbieter in Konkurrenz zur Bundespost treten würden. Dies beweise insbesondere die Tatsache, "dass das Nichtvorhalten überprüften Personals mit einer nicht unbeträchtlichen Geldstrafe bedroht wird". Darüber hinaus sei es kaum gelungen, eine geeignete Definition anzubieten, welche tatsächlich alle Dienstleitungstypen abdecke. So könne man das Gesetz auch so auslegen, dass Stand-Alone-Mailbox-Systeme nicht unter diese Vorschrift subsumiert werden können. Dies alles ändere jedoch nichts daran, dass die E-Mail-Branche mit diesem Gesetz zu leben habe. Im Sinne der Benutzer sei es deshalb sinnvoll, Nachrichten künftig verschlüsselt abzuspeichern, wodurch sich auch eine Reihe datenschutzrechtlicher Probleme elegant lösen liessen.

Weitere Informationen erteilt:

Pressereferat Bundespostministerium
Heinrich-von Stephan-Strasse 1:
5300 Bonn 1: Tel.: 0228/149921

cmp: E-Mail-Press
Tel: 040/27 51 86, MIK-Magazin

Schnelle und einfache Verbindung

USADIRECT Service ist eine Dienstleistung von AT&T im Rahmen des International Long Distance Service, der dem Anrufer eine schnelle und bequeme Möglichkeit bietet, in die USA zu telefonieren. Diese Dienstleistung wird in mehr als 50 Ländern angeboten und kann mit der AT&T Card oder als R-Gespräch geführt werden.

Der Geschäftsreisende wird zunächst mit dem AT&T-Operator in den USA verbunden, der den Anruf dann innerhalb der USA (außer Alaska) weitervermittelt. Der Operatorplatz ist immer besetzt und kann zu jeder Zeit angerufen werden.

Die Kosten für ein Gespräch über USADIRECT sind die gleichen wie bei einem normalen handvermittelten AT&T-Auslandsgespräch. Es gibt keine zusätzlichen Gebühren, der Anrufer bezahlt mit der AT&T Card oder der Angerufene trägt die Kosten.

Australien	Direktwahl (0014-881-011)
Bahamas♦	Direktwahl (1-800-872-2881)
Belgien+	Direktwahl (110010)
Brasilien♦	Direktwahl (000-8010)
Britische Jungferninseln	Direktwahl (1-800-872-2881)
Bundesrepublik Deutschland+	Direktwahl (0130-0010)

In mehr als 50 Ländern verfügbar

Der AT&T USADIRECT Service kann kostenfrei von praktisch jedem Telefon in vielen Ländern in Anspruch genommen werden. In manchen Ländern oder Gebieten ist der Service über bestimmte, entsprechend gekennzeichnete Telefone erreichbar, die sich zum Beispiel in großen Hotels, Telefonzentren, Häfen, Flughäfen und an vielen anderen öffentlichen Orten überall auf der Welt befinden.

Zusammen mit den nationalen Postverwaltungen bietet AT&T den USADIRECT Service in über 50 Ländern und Regionen an:

* Zweiten Wählton abwarten
\+ Öffentliche Telefone: Münze oder Telefonkarte erforderlich
♦ nur begrenzt verfügbar

DOKUMENTATION

Artikel 10
(Brief-, Post und Fernmeldegeheimnis)

(1) Das Briefgeheimniss sowie das Post- und Fernmeldegeheimniss sind unverletzlich.

...allerdings...

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, dass sie dem Betroffenen nicht mitgeteilt wird und dass an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
Gesetz zu Artikel 10 Grundgesetz

G10 § 12
Fassung: 1989-06-08

(1) Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird durch dieses Gesetz eingeschränkt.

(2) Die auf Grund anderer Gesetze zulässigen Beschränkungen dieses Grundrechts bleiben unberührt.

G10 § 1
Fassung: 1989-06-08

(1) Zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschliesslich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages oder der im Land Berlin anwesenden Truppen einer der Drei Mächte sind die Verfassungsschutzbehörden des Bundes und der Länder, das Amt für den militärischen Abschirmdienst und der Bundesnachrichtendienst berechtigt, dem Brief-, Post- oder Fernmeldegeheimnis unterliegende Sendungen zu öffnen und einzusehen sowie den Fernmeldeverkehr zu überwachen und aufzuzeichnen.

(2) Die Deutsche Bundespost hat der berechtigten Stelle auf Anordnung Auskunft über den Postverkehr zu erteilen und Sendungen, die ihr zur Übermittlung auf dem Postweg anvertraut sind, auszuhändigen. Die Deutsche Bundespost und jeder andere Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, haben der berechtigten Stelle auf Anordnung Auskunft über den nach Wirksamwerden der Anordnung durchgeführten Fernmeldeverkehr zu erteilen, Sendungen, die ihnen zur Übermittlung auf dem Fernmeldeweg anvertraut sind, auszuhändigen sowie die Überwachung und Aufzeichnung des Fernmeldeverkehrs zu ermöglichen. Sie haben für die Durchführung der vorstehend genannten Anordnungen das erforderliche Personal bereitzuhalten, das gemäss § 3 Abs. 2 Nr. 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes überprüft und zum Zugang zu Verschlusssachen des jeweiligen Geheimhaltungsgrades ermächtigt ist.

G10 § 2
Fassung: 1978-09-13

(1) Beschränkungen nach § 1 dürfen unter den dort bezeichneten Voraussetzungen angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand

1. Straftaten des Friedensverrats oder des Hochverrats (§§ 80, 80a, 81, 82 und 83 des Strafgesetzbuches),
2. Straftaten der Gefährdung des demokratischen Rechtsstaates (§§ 84, 85, 86, 87, 88, 89 des Strafgesetzbuches, § 20 Abs. 1 Nr. 1, 2, 3 und 4 des Vereinsgesetzes),
3. Straftaten des Landesverrats und der Gefährdung der äusseren Sicherheit (§§ 94, 95, 96, 97a, 97b, 98, 99, 100, 100a des Strafgesetz-

buches),

4. Straftaten gegen die Landesverteidigung (§§ 109e, 109f, 109g des Strafgesetzbuches),
5. Straftaten gegen die Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantik-Vertrages oder der im Land Berlin anwesenden Truppen einer der Drei Mächte (§§ 87, 89, 94, 95, 96, 98, 99, 100, 109e, 109f, 109g des Strafgesetzbuches in Verbindung mit Artikel 7 des Vierten Strafrechtsänderungsgesetzes vom 11. Juni 1957 in der Fassung des Achten Strafrechtsänderungsgesetzes),
6. Straftaten nach § 129a des Strafgesetzbuches oder
7. Straftaten nach § 47 Abs. 1 Nr. 7 des Ausländergesetzes plant, begeht oder begangen hat.

(2) Eine Anordnung nach Absatz 1 ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Sie darf sich nur gegen den Verdächtigen oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt.

G10 § 3
Fassung: 1968-08-13

(1) Ausser in den Fällen des § 2 dürfen Beschränkungen nach § 1 für Post- und Fernmeldeverkehrsbeziehungen angeordnet werden, die der nach § 5 zuständige Bundesminister mit Zustimmung des Abgeordnetengremiums gemäss § 9 bestimmt. Sie sind nur zulässig zur Sammlung von Nachrichten über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen.

(2) Die durch Massnahmen nach Absatz 1 erlangten Kenntnisse und Unterlagen dürfen nicht zum Nachteil von Personen verwendet werden. Dies gilt nicht, wenn gegen die Person eine Beschränkung nach § 2 angeordnet ist oder wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der in § 2 dieses Gesetzes oder eine andere in § 138 des Strafgesetzbuches genannte Handlung plant, begeht oder begangen hat.

G10 § 4
Fassung: 1989-06-08

(1) Beschränkungen nach § 1 dürfen nur auf Antrag angeordnet werden.

(2) Antragsberechtigt sind im Rahmen ihres Geschäftsbereichs

1. in den Fällen des § 2
   a) das Bundesamt für Verfassungsschutz durch seinen Präsidenten oder dessen Stellvertreter,
   b) die Verfassungsschutzbehörden der Länder durch ihre Leiter oder deren Stellvertreter,
   c) bei Handlungen gegen die Bundeswehr das Amt für den militärischen Abschirmdienst durch seinen Leiter oder dessen Stellvertreter,
   d) bei Handlungen gegen den Bundesnachrichtendienst dieser durch seinen Präsidenten oder dessen Stellvertreter,
2. in den Fällen des § 3 der Bundesnachrichtendienst durch seinen Präsidenten oder dessen Stellvertreter.

(3) Der Antrag ist unter Angabe von Art, Umfang und Dauer der beantragten Beschränkungsmassnahme schriftlich zu stellen und zu begründen. Der Antragsteller hat darin darzulegen, dass die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

G10 § 5
Fassung: 1989-06-08

(1) Zuständig für die Anordnung nach § 1 ist bei Anträgen der Verfassungsschutzbehörden der Länder die zuständige oberste Landesbehörde, im übrigen ein vom Bundeskanzler beauftragter Bundesminister.

(2) Die Anordnung ergeht schriftlich; sie ist dem Antragsteller und der Deutschen Bundespost oder dem anderen Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, mitzuteilen. In ihr sind Art, Umfang und Dauer der Massnahme zu bestimmen und die zur Überwachung berechtigte Stelle anzugeben.

(3) Die Anordnung ist auf höchstens drei Monate zu befristen. Verlängerungen um jeweils nicht mehr als drei weitere Monate sind auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen.

(4) Das Bundesamt für Verfassungsschutz unterrichtet das jeweilige Landesamt für Verfassungs-

schutz über die in dessen Bereich getroffenen Beschränkungsanordnungen. Die Landesämter für Verfassungsschutz teilen dem Bundesamt für Verfassungsschutz die ihnen übertragenen Beschränkungsmassnahmen mit.

(5) Beschränkungsmassnahmen sind den Betroffenen nach ihrer Einstellung mitzuteilen, wenn eine Gefährdung des Zwecks der Beschränkung ausgeschlossen werden kann. Lässt sich in diesem Zeitpunkt noch nicht abschliessend beurteilen, ob diese Voraussetzung vorliegt, ist die Mitteilung vorzunehmen, sobald eine Gefährdung des Zwecks der Beschränkung ausgeschlossen werden kann. Einer Mitteilung bedarf es nicht, wenn diese Voraussetzung auch nach fünf Jahren noch nicht eingetreten ist. Nach der Mitteilung steht den Betroffenen der Rechtsweg offen; § 9 Abs. 6 findet keine Anwendung.

"Den Verfassungsschutzbehörden fällt es jedoch schwer, ihre Auskunftspraxis diesen rechtsstaatlichen Vorgaben anzupassen."

"...bevor eine Petentin informiert werden durfte, dass über sie keine Informationen gespeichert sind. Sie war irrtümlich in den Verdacht extremistischer Bestrebungen geraten und musste deshalb die Überwachung ihres Post- und Fernmeldeverkehrs erdulden."

Der Hamburger Datenschutzbeauftragte

G10 § 6
Fassung: 1968-08-13

(1) In den Fällen des § 2 muss die Anordnung denjenigen bezeichnen, gegen den sich die Beschränkungsmassnahme richtet.

(2) Soweit sich in diesen Fällen Massnahmen nach § 1 auf Sendungen beziehen, sind sie nur hinsichtlich solcher Sendungen zulässig, bei denen Tatsachen vorliegen, aus welchen zu schliessen ist, dass sie von dem, gegen den sich die Anordnung richtet, herrühren oder für ihn bestimmt sind.

G10 § 7
Fassung: 1989-06-08

(1) Die aus der Anordnung sich ergebenden Massnahmen nach § 1 Abs. 1 sind unter Verantwortung der antragsberechtigten Stelle und unter Aufsicht eines Bediensteten vorzunehmen, der die Befähigung zum Richteramt hat.

(2) Liegen die Voraussetzungen der Anordnung nicht mehr vor oder sind die sich aus der Anordnung ergebenden Massnahmen nicht mehr erforderlich, so sind sie unverzüglich zu beenden. Die Beendigung ist der Stelle, die die Anordnung getroffen hat, und der Deutschen Bundespost oder dem anderen Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, mitzuteilen.

(3) Die durch die Massnahmen erlangten Kenntnisse und Unterlagen dürfen nicht zur Erforschung und Verfolgung anderer als der in § 2 genannten Handlungen benutzt werden, es sei denn, dass sich aus ihnen tatsächliche Anhaltspunkte ergeben, dass jemand eine andere in § 138 des Strafgesetzbuches genannte Straftat zu begehen vorhat, begeht oder begangen hat.

(4) Sind die durch die Massnahmen erlangten Unterlagen über einen am Post- und Fernmeldeverkehr Beteiligten zu dem in Absatz 3 genannten Zweck nicht mehr erforderlich, so sind sie unter Aufsicht eines der in Absatz 1 genannten Bediensteten zu vernichten. Über die Vernichtung ist eine Niederschrift anzufertigen.

G10 § 8
Fassung: 1968-08-13

(1) Sendungen des Postverkehrs, die zur Öffnung und Einsichtnahme der berechtigten Stelle ausgehändigt worden sind, sind unverzüglich dem Postverkehr wieder zuzuführen. Telegramme dürfen dem Postverkehr nicht entzogen werden. Der zur Einsichtnahme berechtigten Stelle ist eine Abschrift des Telegramms zu übergeben.

(2) Die Vorschriften der Strafprozessordnung über die Beschlagnahme von Sendungen des Postverkehrs bleiben unberührt.

G10 § 9
Fassung: 1978-09-13

(1) Der nach § 5 Abs. 1 für die Anordnung von Beschränkungsmassnahmen zuständige Bundesminister unterrichtet in Abständen von höchstens sechs Monaten ein Gremium, das aus fünf vom Bundestag bestimmten Abgeordneten besteht, über die Durchführung dieses Gesetzes.

(2) Der zuständige Bundesminister unterrichtet

monatlich eine Kommission über die von ihm angeordneten Beschränkungsmassnahmen vor deren Vollzug. Bei Gefahr im Verzug kann er den Vollzug der Beschränkungsmassnahmen auch bereits vor der Unterrichtung der Kommission anordnen. Die Kommission entscheidet von Amts wegen oder auf Grund von Beschwerden über die Zulässigkeit und Notwendigkeit von Beschränkungsmassnahmen. Anordnungen, die die Kommission für unzulässig oder nicht notwendig erklärt, hat der zuständige Bundesminister unverzüglich aufzuheben.

(3) Der zuständige Bundesminister unterrichtet monatlich die Kommission über von ihm vorgenommene Mitteilungen an Betroffene (§ 5 Abs. 5) oder über die Gründe, die einer Mitteilung entgegenstehen. In den Fällen des § 5 Abs. 5 Satz 3 unterrichtet er die Kommission spätestens fünf Jahre nach Einstellung der Beschränkungsmassnahmen über seine abschliessende Entscheidung. Hält die Kommission eine Mitteilung für geboten, hat der zuständige Bundesminister diese unverzüglich zu veranlassen.

(4) Die Kommission besteht aus dem Vorsitzenden, der die Befähigung zum Richteramt besitzen muss, und zwei Beisitzern. Die Mitglieder der Kommission sind in ihrer Amtsführung unabhängig und Weisungen nicht unterworfen. Sie werden von dem in Absatz 1 genannten Gremium nach Anhörung der Bundesregierung für die Dauer einer Wahlperiode des Bundestages mit der Massgabe bestellt, dass ihre Amtszeit erst mit der Neubestimmung der Mitglieder der Kommission, spätestens jedoch drei Monate nach Ablauf der Wahlperiode endet. Die Kommission gibt sich eine Geschäftsordnung, die der Zustimmung des in Absatz 1 genannten Gremiums bedarf. Vor der Zustimmung ist die Bundesregierung zu hören.

(5) Durch den Landesgesetzgeber wird die parlamentarische Kontrolle der nach § 5 Abs. 1 für die Anordnung von Beschränkungsmassnahmen zuständigen obersten Landesbehörden und die Überprüfung der von ihnen angeordneten Beschränkungsmassnahmen geregelt.

(6) Im übrigen ist gegen die Anordnung von Beschränkungsmassnahmen und ihren Vollzug der Rechtsweg nicht zulässig.

G10 § 10
Fassung: 1968-08-13

(1) Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) wird durch dieses Gesetz eingeschränkt.

(2) Die auf Grund anderer Gesetze zulässigen Beschränkungen dieses Grundrechts bleiben unberührt.

G10 § 11
Fassung: 1968-08-13

Die nach diesem Gesetz berechtigten Stellen haben die Leistungen der Deutschen Bundespost abzugelten.

G10 § 13
Fassung: 1989-06-08

Die nach diesem Gesetz berechtigten Stellen haben die Leistungen der Deutschen Bundespost oder anderer Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, abzugelten.

G10 § 14
Fassung: 1989-06-08

Artikel 2 und 3 dieses Gesetzes mit Ausnahme des Artikels 2 Nr. 2, § 100a Nr. 1 Buchstaben b und d, gelten nach Massgabe des § 13 Abs. 1 des Dritten Überleitungsgesetzes vom 4. Januar 1952 (Bundesgesetzbl. I S. 1) auch im Land Berlin.

G10 § 15
Fassung: 1989-06-08

Dieses Gesetz tritt mit Ausnahme des § 9 Abs. /× 4, ×/ der am Tage nach der Verkündung in Kraft tritt, am ersten Tag des auf die Verkündung folgenden dritten Kalendermonats in Kraft.

"Es mag bereits zweifelhaft sein, ob neue TK-Dienste, insbesondere Mehrwertdienste, überhaupt voll in den Schutzbereich des Art. 10 GG fallen... Damit ist die Überwachung von in digitaler Form übertragener Daten nicht gestattet."

Der Hamburger Datenschutzbeauftragte 1988

LICH ... DEMOKRATISCH ... FREIHEITLICH ...

Artikel 3

ÄNDERUNG DES GESETZES ÜBER FERNMELDEANLAGEN

...

15. Es wird folgendes § 26 angefügt:

§ 26 Betreiber von Fernmeldeanlagen, die Telekommunikationstdienstleistungen gemäss § 1 Abs. 4 für andere am 1. Juli 1989 erbringen, müssen den Betrieb bis zum 1. Januar 1990 beim Bundesminister für Post und Telekommunikation schriftlich anzeigen."

§ 10

(1) Wird der Fernmeldeverkehr nach Artikel 1 dieses Gesetzes oder nach den §§ 100a, 100b der Strafprozessordnung überwacht, so darf diese Tatsache von Personen, die eine für den öffentlichen Verkehr bestimmte, nicht von der Deutschen Bundespost betriebene Fernmeldeanlage betreiben, beaufsichtigen, bedienen oder bei deren Betrieb tätig sind, anderen nicht mitgeteilt werden.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer entgegen Absatz 1 die Tatsache der Überwachung des Fernmeldeverkehrs einem anderen mitteilt.

§11

(1) Ordnungswiedrig handelt, wer als Betreiber einer für den öffentlichen Verkehr bestimmten, nicht von der Deutschen Bundespost betriebenen Fernmeldeanlage entgegen

1. Artikel 1 § 1 Abs. 2 Satz 2 eine Auskunft nicht erteilt, Sendungen nicht aushändigt oder das Überwachen des Fernmeldeverkehrs nicht ermöglicht oder
2. Artikel 1 § 1 Abs. 2 Satz 3 das erforderliche überprüfte und zum Zugang zu Verschlussachen des jeweiligen Geheimhaltungsgrades ermächtigte Personal nicht bereithält.

(2) Die Ordnungswidrigkeit kann mit einer Geldbusse bis zu dreissigtausend Deutsche Mark geahndet werden.

Quellen: - *Bundesgesetzblatt, Jahrgang 1989, Teil 1 Nr. 25 - Tag der Ausgabe: Bonn, den 14. Juni 1989 Seite 1049 1050*
- *Jahresbericht des Hamburger Datenschutzbeauftragten, 1988*

Chaos Communication Congress 1989

Was Wann Wo: **6. Chaos Communication Congress, vom 27. bis 29.Dezember 1989 im Eidelstedter Bürgerhaus, Elbgaustr. 12, D-2000 Hamburg 54**

Themen[u.a.]: **Mailboxnetze und öffentliche Datenbanken**
Telefonnetz der DDR und Planung von Datenreisemöglichkeiten
Freedom of Information Act und Copyright
Feminines Computerhandling
Cyberpunk, Viren, Würmer, Wanzen,
Datenschutz, Postreform
Zu den Diskussionen wurden kompetente in- und ausländische Gäste eingeladen.

EUnet

European Unix network

"Das EUnet ist ein kooperatives, nichtkommerzielles Netz von Unixrechnern in Europa, das seinen Teilnehmern eine schnelle und guenstige Kommunikation per Electronic Mail - national und international - sowie Informationen ueber das weltweite Computerkonferenzsystem der "News" ermoeglichen will. Technisch baut das Rechnernetz auf dem Kommunikationsprotokoll UUCP (Unix-to-Unix-Copy) bzw. TCP/IP sowie einem Mail-Programm auf. Zur Verbindung der Rechner werden je nach den Erfordernissen entweder Standleitungen, Datex-P oder Telefonleitungen benutzt.

Organisatorisch steht das EUnet zum einen unter dem Verwaltungs-Dach der European Unix systems Users Group und deren nationalen Vertretungen. Andererseits laeuft der groesste Teil der Organisation, Beratung und Hilfe fuer die Teilnehmer an den nationalen Zentralstellen der sogenannten "Backbone-Rechner" zusammen. In Deutschland wird dieser Backbone-Rechner "unido.uucp" an der Informatik Rechnerbetriebsgruppe der Universitaet Dortmund von einem Team von Studenten aufrechterhalten.

History-weit weit zurueck in den 83ern

Damit waere im Prinzip das Wichtigste ueber das EUnet schon festgestellt. Bliebe noch zu sagen, dass die Philosophie des Unix-Netzes historisch einen gewissen Benutzereinfluss, Pragmatismus, Unabhaengigkeit wo noetig und Kooperation, wo moeglich, fuer sich beansprucht. Historisch war diese Entwicklung deshalb so, weil das Netz aus der Initiative von europaeischen Unix-Anwendern hervorgegangen ist, die etwa 1983 eigentlich nur ihre Arbeit am allgemein wenig bekannten Unix-System verbessern wollten. Man sah hinueber in das Unix-Stammland USA und wollte untereinander und mit dem amerikanischen Unix-Netz Informationen und Programme austauschen.

Der pragmatische Ansatz lag nun darin, das zu benutzen, was an Kommunikationsmoeglichkeiten im Unix-System schon existierte - naemlich UUCP und mail - und so einige Rechner an den wenigen europaeischen Forschungsinstituten mit Unixabteilungen zu verbinden. Von den Unternehmen waren nur wenige gewillt, Unix oder gar ein Rechner offen zu unterstuetzen. So konnte man sich die eigene Unabhaengigkeit von Unternehmen bewahren. Gleichzeitig muessen alle Leistungen des Netzes durch die Gelder der Benutzer selbst finanziert und durch Kooperation mit anderen Netzen so effizient wie moeglich gestaltet. Im amerikanischen Usenet dagegen wird die Infrastruktur fuer grosse Weitverkehrsstrecken stark durch die Backbones bei einigen Firmen wie DEC, HP, AT&T oder finanziell starken Forschungsinstitutionen getragen, wenn auch nicht verwaltet, so dass dort die Struktur nur chaotisch zu nennen ist. Bis heute wird das nichtkommerzielle EUet in seiner Struktur und Verwaltung mit viel ideellem Einsatz an den Backbone- Institutionen eher "nebenbei" aufrecht erhalten.

Gewachsene Strukturen und Organisation: T-Bones und Backbones bilden das Skelett Datenfernverbindungen innerhalb Europas waren und sind, teuer, so dass in jedem Land moeglichst nur ein Rechner zentral die entsprechende technische Infrastruktur fuer groessere Datenmengen aufbauen sollte, um diese dann kostenguenstig an mehrere Organisationen im Land zu verteilen. Diese sternfoermige Struktur des Netzes wird besonders durch die hohen Kosten fuer die Megabyte an "News"-Artikeln be-

dingt. Diese kommen zentral beim Centrum voor Wiskunde en Informatica (CWI) in Amsterdam an, um dann mehrfach kopiert und an die nationalen Backbone-Rechner verteilt zu werden. Dieses Prinzip der moeglichst kostenguenstigen Teilung von Kosten setzt sich in den nationalen Netzen weiter fort.

Fuer die E-Mailverbindungen sieht die Struktur anders aus, dezentraler. Die Backbone-Rechner der 19 beteiligten Laendern tauschen etwa alle halbe Stunde anfallende E-Mail aus und bilden damit ein eng vermaschtes Netz. Gateways und schnelle Verbindungen in nationale oder internationale Forschungsnetze laufen wenn moeglich von den einzelnen Backbone-Rechnern direkt. So koennen EUnetter heute ihre elektronische Post ueber ihren Backbone-Rechner etwa ins EARN/Bitnet, das amerikanische Arpa/Internet oder das ehemalige CSnet, japanischen "Junet"tern, australischen "ACSnet"tern oder auch in X.400-Netze wie das DFN schicken. Allein im amerikanischen Unix-Mutternetz umfasst die Zahl der erreichbaren Endbenutzer etwa 1 Million ... Damit sind ueber das EUnet heute die meisten Teilnehmer an den wichtigsten internationalen Forschungsnetzen erreichbar.

Ganz nebenbei ist das EUnet durch seine Unabhaengigkeit von Forschung und Unternehmen auch eines der wenigen Computernetze, die Organisationen aus Forschung *und* Unternehmen teilnehmen lassen. Warum eigentlich nur Organisationen? koennte man an dieser Stelle fragen. Warum keine Privatpersonen? Verschiedene Gruende spielen da eine Rolle: Zum einen sind die urspruenglichen Teilnehmer des EUnet die Mitglieder"organisationen" der Unix User Groups. Zum anderen gehoerten Unixrechner bis vor kurzem noch nicht gerade zum Privatbesitz einer einzelnen Person, sondern standen ueblicherweise in den Raeumen irgendeiner Organisation. Nicht zuletzt verlangt die Aufrechterhaltung des Netzanschluseses fuer eine Einzelperson allein einen nicht unerheblichen Aufwand. In einer Firma oder Universitaet lohnt sich diese Muehe eher, weil der lokale Systemadministrator, im Unix-Netz der "Postmaster", mit seinem Wissen und der technischen Infrastruktur einer groeseeren Gruppe von Nutzern dient.

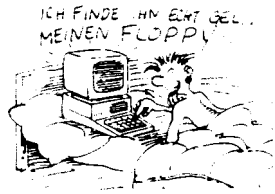
Auserdem wuerde eine Vielzahl von einzelnen kleinen Rechnern, die sich direkt am Service-Rechner ihres Backbones anschlieseen wollten, den Zentralrechner und das dortige Postmaster-Team uebermaesseig belasten. Die optimale Netzstruktur musste die Last nach unten auf die Zwischenrechner oder T-Bone-Rechner verteilen, die wiederum mehrere Endknoten bedienen koennen. In einigen Teilen des EUnets, wie in Holland oder England, laeuft eine solche Dezentralisierung relativ gut, in anderen - wie in Deutschland - laeuft dies ziemlich schlecht. Offiziell gibt es nur in Berlin mit der Technischen Universitaet Berlin und der Siemens AG fuer den Muenchner Raum Zwischenrechner, die sowohl Rechnerkapazitaet als auch Verwaltungs- und Beratungsarbeit fuer das Netz uebernehmen.

Was sind die News?

Sinnvoll wird eine Dezentralisierung insbesondere, um grosse Datenmengen wie die "News" nur *ein* Mal vom zentralen Backbone in einen Grossraum, wie etwa Frankfurt, zu uebertragen und diese zum lokalen Telefontarif dann an

Dänemark + ... Direktwahl (0430-0010) Finnland + ... Direktwahl (9800 10010)

mehrere Interessierte weiter zu verteilen. Was sind denn nun diese imaginaeren "News", denen im EUnet so grosse Aufmerksamkeit und so viel Datenvolumen gewidmet wird? Die News kann man sich als ein Schwarzes-Brett-System von ueber 350 Themengruppen vorstellen, auf denen Fragen und Antworten der Teilnehmer ein intensives Diskussions- und Informationsforum in einem weltweiten Netz ermoeglichen. Die nach Europa transferierten internationalen Gruppen sind ueberwiegend aus dem Umfeld der Computer, Wissenschaft und Technik. Die Spannbreite geht da von "alt.aquaria" fuer die alternative Gruppe der Aquariums-Fischfreunde unter uns, ueber die Bionet-Informationen zum Public-Domain-Vertrieb z.B. in comp.unix.sources (GNU, PC-Software, etc.) oder in die auf Europa oder Deutschland begrenzten EUnet- bzw. Dnet-Hierarchien. Der Informationen werden jedoch auch ueber wissenschaftlichen Felder wie etwa sci.med.aids ausgetauscht. Oder es gibt die gesellschaftlichen Foren wie soc.culture.china oder Freizeitthemen a la rec.arts.books, oder nicht endenwollenden Diskussionen ueber Computerspiele, oder, oder. Also an Themen ist kein Mangel. Der prinzipielle Vorteile des Newssystems gegenueber aehnlich aussehenden Mailboxen ist das Vorhandensein der Daten auf dem eigenen Rechner, so dass man ohne zusaetzliche Kosten die "eigenen" abonnierten Newsgruppen auf dem eigenen Rechner in aller Gemuetsruhe lesen kann. Das Newssystem setzt mit dem Programm "Readnews" in der Gestaltung der News-Artikel und deren Verwaltung unmittelbar auf dem Mail-System auf. Der News-Leser hat es durch die News-Oberflaeche einfach, Texte oder Dateien in und aus seinem Homedirectory aus direkt zu speichern, auszudrucken oder automatisch auf Anfragen zu antworten. Entweder erfolgt dies fuer die Gruppe sichtbar, wenn es von allgemeinem Interesse ist, oder direkt an den Anfrager. Das News-Programm selbst, derzeit Version 2.11, ist ein Public Domain Produkt. Ab Sommer 1989 wird es in der Version 3.0 auch vom Unido-Backbone zu erhalten sein.



Wie laeuft das in Deutschland

Ach ja, dieser Unido-Backbone. Ein halbes Dutzend Studenten der Informatik Rechnerbetriebsgruppe der Universitaet Dortmund pflegen den Zentralrechner Unido, ein MX500 und die notwendigen Peripheriegeraete. Mehr Zeit als fuer die Technik wird jedoch fuer die Beratung und Information der angeschlossenen ueber 180 Teilnehmerorganisationen und deren Systemadministratoren und Benutzer verwandt. Nachdem die Rechner mit ihrem UUCP-Namen in die weltweite Adressdatenbank der "Maps" aufgenommen worden ist, muss eine funktionierende UUCP-Verbindung zu Unido hergestellt werden, um die Daten austauschen zu koennen. Danach kommt die Hilfestellung bei der Konfiguration des notwendigen "Message Transport Agents" als dem Programm, das lokal die Post der Benutzer weiterleiten muss. Die genaue Versendung wird den Teilnehmerorganisationen vom nationalen Backbone-Rechner abgenommen, der jede Mail nach seinem letzten aktuellen Informationen auf den richtigen Weg routet. Dies schliesst ein aktives Routing durch den einzelnen Benutzer aus, der sich im Normalfall nicht um den genauen Weg kuemmern kann und kuemmern muss.

(Zur Erklaerung fuer Nicht-Unix-Kenner: Das Unix-to-Unix-CoPy verlangte urspruenglich eine Adressierung ueber jeden Rechner, der zur Uebertragung beitrag. Also ungefaehr so:

!Rechner1!Rechner2!Rechner3!
Endrechner!Empfaenger

Man kann sich vorstellen, dass dies bei einer Mail nach Kalifornien zum Beispiel einige Zeilen fuellen kann, die anfaellig fuer Tippfehler und unnoetige Umwege sind. Deshalb koennen heute alle in der "Map" mit ihren Zugangsmoeglichkeiten registrierten Unix-Rechner ueber eine Adresse wie Benutzer@Rechnerxy.uucp erreicht werden. Darueberhinaus gibt es noch so etwas wie eine netzunabhaengige, sogenannte Domainadresse, die in Deutschland zum Beispiel in der Form

Benutzer@Rechner.Abt.Organisation.de

eine logische Adressierung entsprechend der Organisationsaufbau ermoeglichen soll. Dies erfordert jedoch nicht weniger, sondern Mehraufwand und wird fuer Deutschland vom EUnet-Backbone koordiniert.)

Die Vereinfachung der Rechneradressierung erfordert jedoch natuerlich einen gewissen Verwaltungsaufwand beim Backbone und von der Benutzerorganisation einen gewissen Beitrag, um vom EUnet-Backbone registriert zu werden. Letzeres fuehrt immer wieder zu einem gewissen Unmut bei den Benutzern, die diese Kostenbeitraege fuer zu hoch halten. Nun denn, so sieht die Beitragstabelle im deutschen EUnet im Juni 1989 aus:

Grundbeitrag fuer Mailanschluse inklusive europaeischer News und unbegrenzt Mail innerhalb Deutschlands: 80,- DM

Ein Kilobyte Mail weltweit: 1,- DM Ein Kilobyte innerhalb Europas: 0,30 DM

Von dem pauschalen News-Gebuehren ist das Unido-Team im April 89 angegangen, um auch Interessenten fuer nur wenige Gruppen einen Zugang zu den internationalen News zu ermoeglichen. Seitdem wird entsprechend dem Anteil an den Gesamtkosten der News volumenmaessig abgerechnet. Die monatlichen Beitraege fuer die internationalen News fangen mit zusaetzlichen 40,- DM bei bis zu 10 Prozent des Gesamtvolumens an und reichen bis zu 220,- DM fuer das gesamte Volumen der internationalen News (Juni 89 etwa 100 Mb monatlich).

Schoene "Zukunfts"-Aussichten

Mit dem weiteren Wachstum des EUnet ist eine weitere Verringerung der Beitraege zu erwarten, weil die gemeinsame Infrastruktur durch mehr Teilnehmer getragen wird. Im deutschen EUnet ist mit dem Uebergang auf eine Standleitung zur europaeischen Zentrale in Amsterdam auch mit einer weiteren Kostendaempfung zu rechnen.

Weitere zukuenftige Projekte im EUnet sind etwa ein Netz von dezentralisierten Archivservern ueber ganz Europa hinweg, die Moeglichkeit, ISO-Anwendungen ueber das EUnet hinweg zu benutzen oder der Aufbau eines europaeischen IP-Netzes (Internet-Protocol). Alle diese Dienste haengen jedoch noch vom Interesse und der Beteiligung der EUnetter ab. Wie bei allen anderen Services muessen auch hier jeweils die Benutzer entsprechend finanziell und inhaltlich beteiligt sein.

Wer jetzt immer noch am EUnet interessiert ist, kann sich an das Postmaster-Team an der Uni Dortmund wenden.

EUnet Postmaster-Office
Universitaet Dortmund - IRB
Postfach 500 500
4600 Dortmund 50
Tel.: 0231 / 755 - 24 44
postmaster@unido.uucp
Anke Goos (ag@unido.uucp)

Frankreich ..... Direktwahl (19*-0011) Gambia ..... Direktwahl (001 199-220-0010)

Schwarze Magie, weisse Magie, Netzmagie?

Irgendwo in den Tiefen Nordrhein Westfalens, hinter dem sieben Bergen, bei den sieben Zwergen, gibt es ein Netz. Allerdings nicht für die Zwerge, sondern für den normalen Menschen. Das MagicNet ist ein kleines, derzeit weitgehend noch auf NW begrenztes Netz. Allerdings gibt es auch die ersten Magicnet-Boxen in Hamburg und Paderborn. Ähnlich wie im Zerberusnetz gibt es eine Serverstruktur, derzeit sind dies die MILLIWAYS und die LOS. Die (derzeit) restlichen 31 Rechner sind an einer dieser beider Server angeschlossen. Die verwendete Software wurde von Ingo Richards entwickelt. Dabei handelt es sich um ein compiliertes Basicprogramm. Allerdings gibt es die Software nur für PC's unter MS-DOS. Eine ST-Version soll geplant sein, wer genaueres wissen will, muß schon fragen. Für einen vernüftigen Betrieb sollte man schon einen PC mit 8Mhz haben. Der Vertrieb wurde inzwischen von einer Firma übernommen. Das eigentliche Mailboxprogramm, muss man sich für 350 DM kaufen. Eine Singe-User-Version für den Terminalbetrieb (Point genannt) kostet 30 DM. Zusätzlich gibt es eine Demoversion. Wegen Software kann man sich an MILLIWAYS:SPHINKS wenden. Bei der Installation soll es wenig Probleme geben und ausserdem ist die Software voll fernwartungsfähig, also braucht die Mailbox nicht umbedingt zuhause zu stehen. Nachdem ein Benutzer in der Box war, wird der Rechner resetet. Das hat den Vorteil das die Box nicht nach stundenlangen Betrieb eventuell in einem desolaten Zustand ist. Dafür braucht der Rechner aber eine Weile, bis die Box wieder online ist. Bei der Benutzungsoberfläche handelt es sich um eine geo-ähnliche Shell. Zusätzliche Features sind das Austragen aus bestehende Gruppen, damit man sich auf die für einen interessanten Gruppen beschränken kann. Ausserdem kann man sein Bezugsdatum ändern und damit seine Systemumgebung auf ein anderes 'Lastlog'-Datum ändern. Neben den lokalen Brettern gibt es Netzbretter, z.B. zu Themen wie Musik, Programmiersprachen und Private Kleinanzeigen.

Durchschnittlich werden täglich 50 Nachrichten in den Netzbrettern ausgetauscht. Ausserdem gibt es geschlossene Benutzergruppen. Diese sind entweder vom Benutzerlevel abhängig, von einem Brettpasswort abhängig oder werden durch eine Zugangsliste unterschieden.

Die Zugangskontrollevel für ein Brett kann für Lesen, Schreiben und Inhalt verschiedenen gegeben werden. Neben den Brettern gibt es noch eine PD-Softwarebank. Diese sind wie Bretter in den MagicNet Mailboxen orientiert. Zum uploaded kann man X-,Y- und Z-Modem verwenden. Unter anderem sind 10-15 MB an IBM Software abrufbar. Allerdings kann man keine Binärnachrichten über das Netz verschicken. Der Level wird von 0 bis 9 unterschieden, wobei 3 der Normalzustand sein sollte. Zeitlimit ist 30 Minuten. Kosten für verschickte Nachrichten entstehen in der Regel nicht. Nur für Eilnachrichten werden Gebühren erhoben. Da aber bei der derzeit geringen Ausbreitung des Netzes

jede normale Nachricht innerhalb von 24 Std. ankommt, sind diese auch nicht notwendig. Vom MagicNet aus, gibt es praktisch keine Verbindungen (Gateways) in andere Netzwerke. Es gab zwar mal ein Zerberus-Gateway, aber irgendwie kam man mit der Verwaltung durch die verschiedenen Kostenstrukturen nicht klar. Für die Zukunft sind andere Gateways geplant. Probleme gibt es auch, wenn man eigene MagicNet Software programmieren will. An die Spezifikationen z.B. der Protokolle oder Einloggsequenzen ist nicht ranzukommen. Ähnlich wie beim Zerberus wird dadurch (in Verbindung mit dem Mailbox-Preis) eine stärkere Verbreitung, wie z.B. bei UUCP, verhindert.

Autoren: Diverse Sysops und User des MagicNets

Eventuelle Fragen können z.B. an LOS:ROLAND gestellt werden. Die Nummer ist 0214/94738 8N1.

DECnet

DECnet ist ein Netz fuer Rechner von Digital Equipment Corporation (:= DEC), bzw. fuer Rechner, die die DECnet-software besitzen. DECnet gibt's fuer die Betriebsysteme VMS (1), RSX (2), ULTRIX bzw. Unix (3), und mit Einschraenkungen fuer DECnet-DOS, das eine DEC-Variante von MS-DOS darstellt und auf IBM-kompatiblen Muehlen laeuft. Die physikalische Grundlage von DECnet ist Ethernet, sowohl als Koax als auch neuerdings vermehrt Glasfaser. Die kleinste Uebertragungsgeschwindigkeit betraegt 9600 kBaud, die Groesste 10 MBaud.

DECnet war ursprünglich nur als reines lokales Netz geplant, wird inzwischen aber auch vermehrt als WAN (Wide Area Network) eingesetzt, zum Teil ganze Kontinente umspannend.

Es gibt aber nicht nur ein DECnet, so wie es z.B. nur ein Fidonet gibt, sondern sehr viele in der ganzen Welt mit sehr unterschiedlichen Groessen. Diese diversen DECnets sind teilweise miteinander verbunden und haben Gateways zu anderen Netzen.

Betrieben werden die DECnets meistens von Unis, Instituten und aehnlichem, aber auch Firmen haben welche, bzw. lassen sich dran anschliessen. Die meisten DECnet-Installationen enthalten zu 90% VAXen unter VMS und haben damit eine sehr homogene Benutzeroberflaeche.

Die Adresse eines Rechners im DECnet lautet 'nodename::username', wobei node sein kann:

1) ein logical (4)
2) eine Zahl zwischen
   2.1) 0 und 1023; damit werden lokale Rechner angesprochen.
   2.2) zwischen 1024 und 64512 (=2**16-2**10)

Großbritannien + ... Direktwahl (0800-89-0011) Italien + ... Direktwahl (172-1011)

In den folgenden Ausführungen werde ich mich auf VMS beschraenken.

Netzwerkfunktionen

Remote Login: mit dem Befehl 'set host ‹node›' kann man sich auf einem weiteren Rechner einloggen.
Beispiel: set host netvax

Remote command: einen Befehl an einen anderen node schicken.
Beispiel: NETDCL.COM (siehe unten)

Remote job entry: einen task auf einem anderen node starten.
Beispiel: NETDCL.COM (siehe unten)

Task-to-Task-communication: Prozesse auf verschiedenen Rechnern tauschen Daten untereinander aus.

File Transfer: ein Filetransfer ist in beiden Richtungen moeglich.
Entweder mit:
copy source node"user password"::destination
oder: copy node"user password"::source destination
Beispiel:
copy test.txt netvax"framstag geheim"::disk3:‹users.framstag›

Mail: Jeder User hat in VMS seine eigene mailbox. Wobei mailbox woertlich zu nehmen ist:
ein Briefkasten in den der Postbote (=DECnet) Briefe einwirft oder man selbst Briefe an andere User aufgibt. Angekommene mails werden innerhalb der mailbox gespeichert und beim einloggen wird angezeigt, ob und wieviel mail man bekommen hat. Diese mails koennen dann in normale files umkopiert oder ausgedruckt werden. Beim mail-Aufruf kann entweder ein vorher erstelltes (Text-) File angegeben und abgeschickt werden, oder mail fragt nach dem Text interaktiv.
Ist der Adressent ein geloggt, bekommt er die Nachricht, dass er soeben post erhalten hat.
Beispiel:
mail/subject="neues vom CCC!" test.txt netvax::framstag

Phone: Das ist die Facility zum chatten! PHONE ist eine interaktive Kommunikation zwischen Usern und entspricht dem TALK bei UNIX oder einem "deluxe-"CHAT bei VM/CMS. Der Bildschirm wird in 2 Teile gesplittet, wobei die obere Haelfte einem selber gehoert, die untere dem Telefonpartner. Nun kann munter drauflosgetippt werden, wobei jeder Buchstabe sofort uebermittelt wird und nicht erst der ganze Satz nach ‹return›. Bei Bedarf kann auch ein Konferenzphone geschaltet werden: der Bildschirm wird dann in x User aufgesplittet... und alle koennen gleichzeitig tippen (*wahnsinnschaos*).
Um sich vor einem moeglichen Telefonterror zu schuetzen gibt's die Moeglichkeit sein phone abzuklemmen:
set broadcast=nophone, Beispiel: phone 45152::framstag

Wie weiss ich nun welche VAXen in meinem DECnet drin sind?
Da gibt's die schoene Utility ncp (Network Control Programm), die einem mit 'mcr ncp show known nodes' ... was wohl zeigt?
Dieses NCP bietet aber noch wesentlich mehr Möglichkeiten, von denen ich hier nur eine Übersicht aufliste (siehe Kasten auf der nächsten Seite).

Tja, und wie komm ich nun an die User?
1. Man kennt diesen kommunikationswilligen User. prima, alles paletti
3. Mit 'phone dir node' bekommt man eine Liste der user auf der 'node'-VAX
2. Falls 2. nicht klappen sollte: NETDCL.COM (7)
'NETDCL.COM' muss im aktuellen Directory gespeichert sein. Der Aufruf erfolgt dann mit: @netdcl
Vorausgesetzt die ZielVAX laesst einen herein, ist man als User DECNET drin. Nun schauen wir uns mit 'show user' um, ob jemand bekanntes da ist und phonen oder mailen ihn an (nach logout vom netdcl).
Aber Vorsicht: es koennte auch ein Prof oder Sysop dahinter stecken, der gerade beschaeftigt ist. Aber da kann man sich ja noch herausreden mit: "Ihr phone war nicht abgestellt und da dachte ich mir, ruf doch mal an...."
Wie komme ich nun in's DECnet?
1. remote login
1.1 Man ist schon drin. Die meisten Unirechenzentren vergeben Accounts auch an Studenten.

$ mcr ncp help commands

SET	Change parameters in the volatile database
DEFINE	Change parameters in the permanent database
CLEAR	Remove components or
PURGE	parameters from the volatile or permanent databases
SHOW	Display information about
LIST	components in the volatile or permanent databases
CONNECT	Connect local terminal to remote node console interface
DISCONNECT	Disconnect logical links with processes
COPY	Copy one node database to another
LOOP	Test lines or connections to nodes
LOAD	Downline load nodes
TRIGGER	inmitiate bootstrap sequence of a node
TELL	Establish temporary executor node
ZERO	Zero counters for the specified entity

1.2 Ueber einen oeffentlichen Account; leider gibt's da sehr sehr wenige...und es werden immer weniger. Das liegt an dem unkollegialen Verhalten einiger 'Mithacker', die solange keine Ruhe geben, bis sie Systemprivilegien besitzen und die VAX zum Absturz bringen. Spaetestens dann gibt's einen oeffentlichen Account weniger. Also, liebe Leut, diese oeffentlichen Accounts sind extra FUER UNS eingerichtet worden! Die Uni braucht so was nicht! Missbraucht diese Gastfreundschaft nicht! Einen Tip habe ich: die VAX der FH der Post in Berlin laesst guest herein, erlaubt ihm aber dann keinen set host (:= remote login). NUA: 45300090864
...und wenn jemand mal im BELWUE ist: 59184::boerse ist eine offene Mailbox.
2. mail geht eigentlich nur, wenn der Betreffende node noch andere mail-software fachrt - und entsprechend verkabelt ist. z.B.: JNET fuer EARN/bitnet-mail oder EAN fuer x.400-mail
Mail direkt an einen nur-DECnet-Knoten zu schicken geht von aussen nicht.
Was kann ich mit DECnet anfangen?
Im allgemeinen: fast gar nichts, wenn ich vom User ausgehe, der von aussen ins DECnet moechte. Der Grund: DECnets sind im Prinzip nicht fuer den oeffentlichen Zugang ausgelegt. DECnet lohnt sich eigentlich nur fuer den authorisierten User, sei es nun Universitaetsangehoeriger, Student, Betreiber etc... und latuernich fuer den Hacker :-)
Es gibt keine Standard-mailboxen, -server, oder andere nuetzliche Dinge. Der Betreiber des jeweiligen DECnets muss das schon selber einrichten - und die meisten tun es leider nicht.
Gateways (falls vorhanden) aus DECnet heraus zu anderen Netzen: Mit FTP oder TELNET ueber TCP/IP in Arpa/Internet-aehnliche Netze, wie das

Hongkong +.....Direktwahl (008-1111) Jamaica +.....Direktwahl (1-0-800-872-2881)

BELWUE (6), mit JNET ins EARN/ bitnet, mit gMAIL (PD-SW) ins usenet und dessen Derivate, mit EAN ins DFN und andere x.400-Netze oder mit psi ins datex-p.
Beispiel eines DECnet(8): Das DECnet im BELWUE. Es enthaelt zur Zeit ca 300 nodes und ist noch im Aufbau begriffen. Vernetzt sind alle Unis in Baden-Wuertemberg, viele Institute und einige Firmen.
Zum Schluss noch eine Story, direkt aus dem Leben eines DECnet-Users gegriffen:
Es folgt nun die unblaubliche Maer wie man aus User Hacker macht:

Auf jeder VAX gibt es einen Standard-Account DECNET mit pw:= DECNET, der aber NICHT mit remote login erreicht werden kann. Dieser Account ist fuer verschiedene DECnet-Utilities und als Pseudo-Gast-Account vorgesehen. Dieser DECNET-Account hat sehr eingeschraenkte Rechte, so ist z.B. ein editieren oder ein weiterer Netzwerkzugriff nicht moeglich. Das HELP-Menue wird vom System eingerichtet und entspricht dem MAN bei UNIX.

Hier an der Uni Ulm gibt es ein *unglaublich* unwissendes Rechenzentrum, mit einem noch groesseren Mangel an Literatur (mal abgesehen von den 80 kg VAX/VMS- Manuals). Der aktive User darf sich seine Information, die ueber "run", "FORTRAN" oder "logout" hinausgehen, selbst suchen. Gut, dass ich im BELWUE- DECnet noch andere Accounts besitze, wo mehr Informationen fuer den User angeboten werden. In einem Tuebinger Rechner fand ich im HELP-Menue die Erklaerung zur Prozedur NETDCL.COM, die Kommandos an den DECNET-Account anderer VAXen schickt und dort ausfuehren laesst (remote command). Die Anleitung im HELP- Menue war Idiotensicher - also auch fuer mich :-)

Mit "$ mcr ncp show known nodes" bekommt man ja bekanntlich die aktiven VAXen im DECnet und so probierte ich mal der Reihe nach alle durch, um zu sehen, wo es noch mehr Infos fuer einen wissensdurstigen User gibt. Mit "help", "dir" und aehnlichen Befehlen schaute ich mich dann um. Leider haben 2/3 aller VAXen den DECNET-Account fuer das NETDCL.COM gesperrt , wahrscheinlich aus Angst vor unberechtigten Zugriff, wie auch immer der ausschen mag.

Von manchen Systemmanagern kam dann auch ab und zu eine mail an mich, in der sie sich bei mir erkundigten, ob sie mir weiter helfen koennten bzw. einer schickte mir eine NETDCL.COM -Version fuer ULTRIX.

Dann, nach einem Monat kam das *GRAUEN* in Form folgender mail von meinem Systemmanager:

From: TUEBINGEN::SYSTEM
31-MAY-1989 15:31:11.38
To: FRAMSTAG
CC:
Subj: mach bloss kein scheiss sonst fliegst du raus
From: ITTGPX::SYSTEM
29-MAY-1989 16:46
To: TUEBINGEN::SYSTEM
Subj: Systemeinbruch am 01-May-1989

An den Systemmanager des Rechners TUEBINGEN, wir hatten am 01-May-1989 ueber den DECnet-Account einen Systemeinbruch, der von Ihrer Maschine ausging. Ueber unser Accounting konnten wir feststellen, dass Ihr User mit dem Namen FRAMSTAG ueber das "trojanische Pferd" NETDCL.COM auf unserem Brueckenrechner und auf jedem Rechner unseres VAXclusters einen interaktiven Login emuliert hat. Nennen Sie uns Namen und Adresse dieses

Users und klaeren Sie den Vorgang vollstaendig auf. Wir weisen Sie darauf hin, dass sich der User durch diesen Vorgang strafbar gemacht hat. Sollte sich dies wiederholen, so sehen wir uns gezwungen entsprechende Gegenmassnahmen einzuleiten. Wir werden ueberpruefen, ob an unserem System Schaden entstanden ist. Sollte dies nicht der Fall sein, so werden wir von Massnahmen diesmal absehen. Teilen Sie uns ueber DECnet die Ergebnisse Ihrer Recherchen mit - wir sind ueber die Knotennummer 1084::System zu erreichen.

Dipl.-Ing. [redacted]

Mein Systemmanager drohte mir meinen Account zu loeschen, falls ich nicht augenblicklich die Sache klaeren wuerde. *schluck* Ich war mir meiner Unschuld absolut gewiss; nur - wie sag ich's den anderen? Ich erklaerte klitzeklein alles meinem Systemmanager, was er dann auch geblickt hat, aber die Strafandrohung schwebte immer noch... Also schnell zur Tastatur gegriffen, eine Erklaerungsfile verfasst und abgeschickt an diesen wuetenden Systemmanager in Stuttgart.
Leider war's nichts damit: Er hatte keinen Speicherplatz mehr und meine Erklaerungsmail landete im Nirwana:

```
$ mail erklaerung
  To:   1084::system
%MAIL-E, error sending to user SYSTEM at 1084
%MAIL-E-OPENOUT, error opening
     SYS$SYSROOT:[SYSMGR]MAIL$00040092594FD194.MAI;
 as output
-RMS-E-CRE, ACP file create failed
-SYSTEM-F-EXDISKQUOTA, disk quota exceeded
```

Auch der Versuch ihn ueber PHONE zu erreichen lief schief: er hatte in seiner Hacker-Paranoia auch noch sein PHONE abgklemmt...und nirgendwo gibt's eine Liste in der die REAL-Adressen von den DECnet-Adressen stehen.

Nun stand ich mit dem Brandzeichen "GEFAEHRLICHER HACKER" da und konnte mich nicht rechtfertigen. Ich klagte mein Leid bei einem Bekannten, der Sysop im RZ in Freiburg ist - der fragte bei weiteren ihm bekannten Sysops in Stuttgart nach. Irgendjemand hatte dann 3 Telefonnummern gefunden. Eine davon war tatsaechlich richtig.

Ich bekam auch dann diesen [redacted] ans Telefon und erzaehlte ihm, was ich denn auf seinem DECnet-Account gemacht hatte. Er nahm dann auch prompt seine Vorwuerfe zurueck (von Entschuldigung aber keine Spur). Ich bat ihn schnellstmoeglichst meinen Systemmanager in Tuebingen Entwarnung zu geben, sonst wuerde mir noch mein Account geloescht, wie es in einem aehnlichen Fall einem Komilitonen von mir schon passiert war (auch hier war [redacted] dran schuld). Er sagte mir zu, dass er sofort seine Vorwuerfe offiziell zurueckziehen wuerde. Nach ueber einer Woche ist dies immer noch nicht geschehen (Ich durfte trotzdem meinen Account behalten); dafuer kam folgende mail an mich (an einen dritten Account von mir):

From: 1084::[redacted] 1-JUN-1989 12:51
To: 50180::STUD-11
Subj: Systemeinbruch

An den User STUD-11 des Rechners mit der Knotennummer 50180,

Sie haben am 01-Jun-1989 ab 12:29 auf mindestens einem unserer institutseigenen VAXen einen Systemeinbruch begangen. Wir konnten diesen Vorgang mitprotokollieren. Wir fordern Sie hiermit auf, Rechenschaft ueber diesen Vorgang

Direktwahl (171-499) ..... Ungarn ++ ..... Direktwahl (0039-111) ..... Japan ++

abzulegen.
Sollten wir bis zum 09-Jun-1989 keine lueckenlose Aufklaerung ueber den Vorfall von Ihnen erhalten sehen wir uns gezwungen, weitere Massnahmen zu ergreifen. Die dadurch entstehenden Kosten wuerden wir selbstverstaendlich Ihnen auferlegen. Eine Aufklaerung ist somit in Ihrem eigenen Interesse. Sie koennen uns ueber DECnet-Mail mit der Adresse 1084::[redacted]
oder ueber unten olgende Adresse erreichen.

Institut fuer Technische Thermodynamik und Thermische Verfahrenstechnik
Dipl.-Ing. [redacted] Tel.: [redacted]
Dipl.-Ing. [redacted] Tel.: [redacted]
Pfaffenwaldring 9/10-1 7000 Stuttgart-80
[redacted]

Das war, weil ich "S PHONE 1084::SYSTEM" gemacht hatte. Auf diese Mail habe ich nicht mehr geantwortet. Ich hab keine Lust mehr.

Anhang: NETDCL.COM

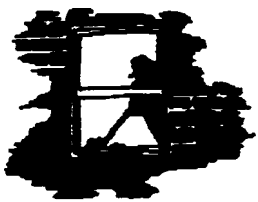
```
$ IF fSmodc() .EQS. "NETWORK" THEN GOTO network
$ IF p1 .EQS. "" THEN READ/PROMPT="-Node: " sys$command p1
$ nodespec = p1 - "::"
$ nodename = fSextract(0,fSlocate("""",nodespec),nodespec)
$ nodespec = nodespec+"""decnet decnet"""
$ ON WARNING THEN CONTINUE
$ CLOSE/ERR=open-server dcl-server
$open-server:
$ OPEN/READ/WRITE dcl-server 'nodespec'::"TASK=NETDCL"/ERROR=open-failure
$ ON WARNING THEN GOTO exit
$flush-output:
$ READ dcl-server record
$ IF record .EQS. "SEND-ME-A-COMMAND" - THEN GOTO send-command
$ WRITE sys$output record
$ GOTO flush-output
$send-command:
$ IF p2 .NES. "" THEN GOTO single-command
$ READ sys$command record /PROMPT=""nodename') " /END=exit
$ record := 'record
$ IF record .EQS. "EXIT" THEN GOTO exit
$ WRITE dcl-server record
$ GOTO flush-output
$single-command:
$ command := 'p2' 'p3' 'p4' 'p5' 'p6' 'p7' 'p8'
$ WRITE dcl-server command
$single-flush:
$ READ dcl-server record
$ IF record .EQS. "SEND-ME-A-COMMAND"- THEN GOTO exit
$ WRITE sys$output record
$ GOTO single-flush
$open-failure:
$ ON WARNING THEN EXIT
$ ON error then copy/log netdcl.com 'nodespec'::
$ COPY/LOG Netdcl.Com 'nodespec'::
$ WAIT 0:0:1
$ OPEN/READ/WRITE dcl-server 'nodespec'::"TASK=NETDCL"
$ ON WARNING THEN GOTO exit
$ GOTO flush-output
$exit:
$ CLOSE dcl-server
$ EXIT
```

```
$network:
$ OPEN/READ/WRITE dcl-link sys$net
$ SET NOON
$ dcl-verify = 'f$verify(0)'
$ DEFINE sys$output dcl-link:
$server-loop:
$ WRITE dcl-link "SEND-ME-A-COMMAND"
$ READ dcl-link dcl-string /END-OF-FILE=server-exit /
ERROR=server-exit
$ 'dcl-string'
$  GOTO server-loop
$server-exit:
$ IF dcl-verify THEN set verify
$ CLOSE dcl-link
$ DEASSIGN sys$output
$ EXIT
```

(1) VMS ist das Standardbetriebsystem fuer die VAX
(2) RSX ist das Echtzeitbetriebsystem fuer die PDP 11
(3) ULTRIX ist UNIX fuer VAX
(4) ein logical ist eine (System- oder Prozess-weit verfuegbare) Variable
(5) source und destination sind VMS-Pfad und -Filebezeichnungen, allgemeine Form: disk:<directory.subdir>name.extension wobei es latuernich mehrere verschachtelte subdirs geben kann.
(6) BELWUE := Baden-Wuerttembergs Extended LAN
(7) Vorsicht mit NETDCL.COM! Ich hafte nicht fuer die Anwendung
(8) siehe auch der SPAN-Artikel von Stephan Stahl im "Das Chaos Computer Buch"

Als weiterfuehrende Literatur kann eigentlich nur das DECnet Manual von DEC empfohlen werden.

Framstag asta@dulruu51.bitnet
asta@rz.uni-ulm.dbp.de
50177::asta (im BELWUE)



Das Z-NETZ

Das Z-NETZ besteht aus mehreren vernetzten Mailboxen, die hauptsächlich mit dem Zerberus-Mailboxprogramm betrieben werden. Im Gegensatz zu anderen Netzwerken liegt im Z-NETZ der Schwerpunkt eher auf den inhaltlichen Bereichen wie z.B. Politik, Umweltschutz, usw., obwohl es auch viele Rechnerbretter für Amiga, Atari, IBM, Mac, usw. gibt. Sehr interessant für Datenreisende sind die Spionage-, Telecom- und G10-Bretter. Diese und viele andere Bretter gehören zum Stammbestand des Z-NETZes, den jede angeschlossene Box führen sollte. Entgegen vielen anderslautenden Stimmen ist das Z-NETZ nicht rechtsradikal. Wenn es auch einige rechte, ziemlich laute Stimmen gibt, die auch nach 100 flames nicht aufgeben, überwiegt doch das das bunte Gemisch der Meinungsvielfalt, wie es in einem richtigen "Bürgernetz" auch sein sollte.

Die Bedienung einer Z-NETZ Mailbox ist denkbar einfach. Schließlich sollte sie auch von Nicht-Computerfreaks (z.B. Umweltgruppen, Parteien, usw.) genutzt werden. Daher wird der recht schnell zu lernende und effektive GeoNet-Standard (BRETT, LESEN, INHALT, SENDEN, usw.) in einer erweiterten Version (mit Unterverzeichnissen wie z.B. /Z-NETZ/ATARI/PROGRAMMIEREN) verwendet. Mit "HILFE *" bekommt man eine ellenlange Anleitung. Auch für Profis bietet die Mailbox Entfaltungsmöglichkeiten: Die Box ist mittels Batch-Dateien programmierbar, so daß sich jeder selbst seine Mini-Shell für die Box basteln kann oder automatisch alle neuen, für ihn interessanten, Nachrichten absaugen kann.

Auch die Editoren sind recht komfortabel: Neben einem Zeileneditor, der in einigen Boxen sogar DES-Verschlüsselung erlaubt, steht der populäre Mi-

Niederlande + ...Direktwahl (06*-022-9111) Norwegen + ...Direktwahl (050 12011)

croEmacs zu Verfügung.

Vergleich zu anderen Netzwerken

Im Z-NETZ muß man nicht in allen Boxen seinen richtigen Namen verwenden. Im Z-NETZ sind Eilmails möglich. Das heißt, daß eine eilige Nachricht zu einer anderen Box nicht, wie sonst bei anderen Netzwerken üblich, über einen vereinbarten Pfad von Box zu Box bis zum Empfänger weitergereicht (geroutet) wird, sondern daß die Stammbox des Absenders direkt die Box des Empfängers anruft. Der Nachteil dieses Systems ist, daß jede Z-NETZ Box mit jeder anderen Z-NETZ Box ein Passwort und ein Übertragungsprotokoll (X-, Z- oder neuerdings auch Bi-Modem) abmachen muß, was manchmal zu etwas Chaos führt. Chaos ist sowieso Trumpf im Z-NETZ: Im Gegensatz zu z.B. Fido kann man bei Zerberus die Serverstruktur komplett selbst bestimmen (nach Absprache mit dem Z-NETZ Koordinator, wenn man es nicht vergißt). In der Praxis heißt das: von Box A holt man sich drei Bretter, von Box B sechs andere, usw. Auch die persönlichen Nachrichten können je nach Lage des Empfängersystems und nach bestehenden Routwegen in alle Himmelsrichtungen verschickt werden. Um dabei Rekursionen zu vermeiden, hat jede Nachricht eine Message-ID. Wenn eine Message-ID doppelt auftaucht, wandert die Datei in Ablage "P".

Die selbst regelbare Serverstruktur erlaubt es auch, neue Subnetze aufzubauen. So gibt es z.B. auf der Basis des Z-NETZes Subnetze wie das "LINK-SYS" des Sozialistischen Computerclubs oder das C-NET des uns wohlbekannten Chaos Computer Clubs. Dort werden alle Clubaktivitäten organisiert, Infos herausgegeben und die neue Datenschleuder geplant.

Weil sich das Z-NETZ immer größerer Beliebtheit erfreut, sind schon über achtzig Mailboxen in Deutschland, der Schweiz, Österreich und Luxemburg angeschlossen. Eine aktuelle Mailboxliste aller Z-NETZ Systeme findet man in jeder Z-NETZ Box im Brett /Z-NETZ/ SYSTEMINFO. Bestimmt ist auch eine in Deiner Nähe dabei. Inzwischen wurden diverse Gateways zu anderen Netzwerken programmiert, um die Kommunikation perfekt zu machen. Man kann Nachrichten an MagicNet-Systeme, Fido und Geonet schicken. Über das neue BtxNet, das von Steffen und Hacko entwickelt wurde, kann man Nachrichten an Btx-Teilnehmer, BtxNet-Teilnehmer, Geo, Bitnet, uucp und sogar Telex- und demnächst auch Telefaxteilnehmer schicken. Wenn man sich eine Terminalversion (Mailboxprogramm für eine Person, das auf dem heimischen Rechner läuft) bei sich installiert, hat man somit eine komplette Nachrichtenzentrale auf dem Tisch stehen. Da kann die gute alte Briefpost nicht mithalten.

Es gibt das Zerberus-Programm als Atari ST- und als MS-DOS Version. Aber auch eine unabhängig entwickelte Amiga-Version gibt es bereits. Für die Zukunft ist eine neue Version des Zerberus-Programms vorgesehen, die ganz in C geschrieben (bisher noch Turbo Basic), multiuserfähig (echt notwendig, einige Boxen sind generell besetzt, weil zu gut besucht) und erheblich komfortabler sein soll.

Wer nun gleich eine Z-NETZ Box besuchen will, kann eine der folgenden

Nummern anrufen. Ich habe eine Box aus je einem Vorwahlbereich ausgewählt, die erfahrungsgemäß sehr stabil läuft und daher leicht erreichbar ist:

0202/473086	TTB
030/4926643	TELEMAIL
040/7019502	ANM
0521/171188	BIONIC
06103/45287	BITMAIL
07762/3144	LINK-LOE
089/656632	INFINET
0911/538985	PARABOL

Alle bieten 300/1200/2400 bps, 8n1

- Henne (SYSOP@MAFIA.ZER) -

EARN (Teil 2)

Ein außerirdisches Datennetz

In DS 25 gab es den ersten Teil des Artikels zum EARN. Erstmal die Berichtigungen zu diesem ersten Teil: Also. Das US-Gegenstück zum EARN heisst natürlich NICHT Bitnic, sondern Bitnet. Bitnic ist der zentrale Knoten in New York, der die Verwaltung für alle Bitnet-Knoten und angeschlossenen Netze (EARN,GuldNet) übernimmt.

Die Nodes im EARN haben meistens ein System in ihrem Namen. Zum Beispiel bedeutet DOLUNI1 nichts weiteres als:

D Deutschland (Land)

OL Oldenburg (Fahrzeugkennzeichnen)

UNI Universität (Organisation)

1 VM/CMS (Betriebsystem)

Ist also ziemlich klar. Andere Kennzahlen für das Betriebssystem sind unter anderem: 0-Cypher, 4-BS3000, 5-VAX/VMS, 6-Unix. Leider wird diese sinnvolle Einteilung nur in Europa eingesetzt. Namen wie WEIZMANN, SUNRISE, etc wird man aber nach längerer Nutzung vom EARN/Bitnet von selbst kennenlernen.

Jedes Zentralnode eines Landes bieten zwei Informationsdienste an. Das eine ist der NETSERV@‹centralnode› Das andere ist der LISTSERV@‹centralnode› Beim Netserver kann man sich Hilfsprogramme zum chatten (z.B. CHAT für VM/SP oder XYZZY für VAX/VMS) schicken lassen. Ausserdem bekommt man dort verschiedene Informationen über die einzelnen Nodes bzw. User. Der Listserver ist da etwas anders. Man kann sich in Listen für bestimmte Themen eintragen: UNIX, ATARI XL, Psychologie des Hundes, usw. Dann bekommt man zu diesen Themen immer das neuste zugeschickt. Aber es gibt auch mehrere E-Mail Zeitschriften wie z.B. BITMONTH. In dieser Zeitschrift wird monatlich alles wissenswerte über das Bitnet veröffentlicht. Bei den Listservern gibt es auch geschlossene Gruppen, die nur fuer bestimmte Leute (z.B. Systemer, Node Admin,etc.) zugaenglich sind. Sinnvolle Kommandos fuer solche Listserver sind z.B. HELP, GET BITEARN NODES (Liste der erreichbaren Nodes) oder GET BITNET SERVERS (Liste der erreichbaren Servern auf dem Bitnet).

Dominica .....Direktwahl (1-800-872-2881) Dominikanische Republik .....Direktwahl (1-800-872-2881)

Dann gibt es noch private Server wie UH-INFO oder TRICKLE DB0TUI11. Diese werden von Firmen oder Universitäten betrieben. Von dieser Art von Server gibt es etwa 200 auf EARN. Dann gibt es auch noch Mailboxen Systeme, da aber auf EARN selten Computerfreaks zu finden sind, haben Mailboxen Seltenheitswert. Es gibt auf der ganzen Welt nur drei Mailboxen, die auch so funktionieren, wie man es von einer anstaendigen Box gewoehnt ist.

UMNEWS@MAINE

Mailbox für Informatiker

COMSERVE@RPICGIGE

Mailbox von Psychologiestudenten

HIPPARCO@ESTEC

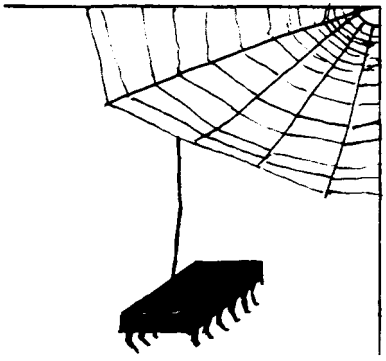
ESA-Mailbox fuer das Hipparco-Projekt

107633@DOLUNI1

Eigenname: Chamas (Möchte nicht viel dazu sagen, da es Werbung wäre: Ist nämlich meine eigene.)

Die Hipparco und die Chamas verwenden eine geoachnliche Benutzungsoberflaeche, soweit dies auf einem Netz wie EARN moeglich ist.

Ein anderer Dienst von EARN sind die Gateways zu anderen Netzen. Dadurch sind bequem andere Netze wie EuNet/UUCP, Janet/UUCP, DFN/X.400 (EAN), Arpa-Inter-Net leicht erreichbar. Auf VM/CMS Systemen gibt es entweder



ein Programm namens CROSSNET oder namens MAIL. Mit diesen kann man in andere Netze Nachrichten verschicken, da diese Programme die entsprechenden Envelopes (Mailformate) automatischen bilden kann. Auf VAX/VMS gibt es ein Kommando namens gMAIL. Dieses muss aber nicht umbedingt vorhanden sein. Wenn man Pech hat, muss man sich seinen Envelope selbst basteln. Die dazu notwendigen Formate sind bekannt unter dem Namen BSMTP und RFC822. Die Beschreibungen für diese Umschläge sind auf allen Servern der Zentralknoten (in Deutschland DEARN) zu bekommen. Diese Abkürzungen hören sich schlimm an, beschreiben aber im Endeffekt nur paar Zeilen vor und nach der eigentlichen Nachricht. Auch für andere Netze wie z.B. EuNet oder UseNet sind diese Formate interessant. Wenn man mit diesen Formaten umgehen kann, sind auch Mailboxen und Server auf dem InterNet erreichbar. Beispielsweise gibt es einen Server atari@terminator.cc.umich.edu. Dort kann man Massen von Atarisoftware abfordern. Dafür muss man nur den Befehl INDEX oder HELP in der Subject-Zeile (auswaerts fuer Betreff) angeben. Natürlich kann man auch von anderen Netzen aus ins Bitnet senden. Das geht z.B. vom UUCP aus mit dem Path: ..!tmpmbx!<node>BITNET!<userid> oder auch ..!unido!<node>BITNET!<user>. Man sollte aber immer dran denken, dass das senden in andere Netze Probleme bringen kann, da es auf diesen Netzen vielleicht andere Topologien, Organisationen und Kostenstrukturen gibt. Im Zweifelsfall sollte man immer einen SysOp oder Postmaster fragen. Das verwendete Protokoll auf den EARN/Bitnet ist NJE. Dies steht für Network Job Entry und ist ein Produkt von IBM. Bis heute habe ich noch keine vernüftige Beschreibung für dieses Protokoll ge-

funden, da es sich um 'restricted documents' handelt. Ein beliebtes Hobby von Firmen wie IBM und DEC. Die Verbindung unter dem Nodes wird mit einem Softwareprogramm namens RSCS aufrecht gehalten. Dieses RSCS ist eine Art Pseudo-User und ist daher auch ansprechbar. Man kann ihm unter anderen Kommandos schicken.

Wichtige Befehle des RSCS sind z.B.

CMD ‹node1› q ‹node2› s
Welcher Status hat der Link zwischen Node1 und Node2 (Aktiv?, Files queued, usw.)

CMD ‹node› CPQ N
Wer ist alles am Node1 eingeloggt?

CMD ‹node› ‹userid› CPQ T ‹text›
Text an User Userid in Node schicken.

CMD ‹node2› CMD ‹node3› ‹rscs kommando›
Es wird nicht der vorgegebene Link von Startnode über Node1 nach Node3 genommen, sondern ein Umweg über Node2. Bei LF sehr sinnvoll.

CMD ‹node› CPQ U ‹userid›
Ist User ‹userid› eingeloggt?

CMD ‹node1› q ‹node2›
Welche Dateien warten darauf, gesendet zu werden?

Leider haben viele RSCS eine Sperre drin, die die Befehl CPQ N und CPQ U, oder sogar noch mehr sperren. RSCS gibt es an sich nur auf VM/CMS Maschinen. Allerdings werden diese Kommandos in der Regel auf von JNET (VAX/VMS) und ähnlichen Kommunikationsservern verstanden. Unterschiede gibt es zum Beispiel bei JES3 (für BS3000). Dort ist der Befehl '$D,u "‹userid›"' mit dem Befehl 'CPQ U ‹user›' auf RSCS gleichzusetzen. Auf UREP (für UNIX) lautet der gleiche Befehl finger ‹userid›.

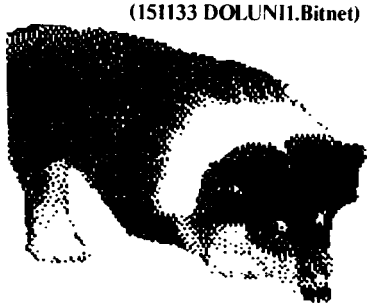
Das Backbonenetz von EARN wurde bis Ende 1987 von IBM finanziert. Seit dem wird es vom Bundesministerium für Forschung und Technologie bezahlt. Die Finanzierung läuft Ende 1989 aus. Das hätte normalerweise das Ende von EARN in Deutschland bedeutet, wenn nicht IBM gesagt hätte, das sie die Finanzierung eventuell wieder übernehmen. Man könnte jetzt meinen, das die Universitäten dahinterher sein müßten, EARN attraktiv zumachen, um durch hohe Benutzerzahlen IBM endgültig eine Zusage abzuringen. Im Gegenteil: In letzter Zeit wird der Zugang immer schwieriger. Stattdessen will man sich an das DFN (Deutsches Forschungsnetz) hängen. Dieses (auf X.400 basierende) Netz läuft über Latex. Als Begründung wird angeführt, das man nicht von einer Firma (IBM) abhängig sein will. Das hört sich gut an. Bei DFN wäre man ja nur von der Bundespest abhängig. Und... DFN müßte sicher für die Allgemeinheit gesperrt werden. Das Uebertrgungsmedium ist ja Datex-L. Das ist teuer und ziemlich unsicher (wenigstens im Vergleich zu EARN). Außerdem bietet DFN weder Server, noch Messages, noch Relays. Allerdings ist das Thema Netze der Universitäten noch nicht entschieden. Das letzten Reste von EARN werden wohl im naechsten Jahr in das AGFNet integriert. Das AGFNet ist das Netz der 'Arbeitsgemeinschaft Grossforschungseinrichtungen'. An dieses AGFNet wollen sich jetzt auch paar Universitäten anschliessen, um die Leistungen vom Bitnet weiter direkt nutzen zu können. AGFNet bietet sogar weitergehende Leistungen wie Remote Login. Außerdem hat die Post angeboten ein wissenschaftliches

Schweden + ... Direktwahl (020-795-611) ..... Schweiz + ... Direktwahl (046-05-0011)

Datennetz für die Universitäten einzurichten. Dieses ist praktisch Datex-P wird aber von den Universitäten pauschal bezahlt, also nicht nach Volumen. In wie weit Studenten diese Netze nutzen können, werden die einzelnen Rechenzentren entscheiden müssen. Inzwischen hat sich unter anderem die Universitäten in Niedersachsen entschlossen auch über das Jahr 1990 hinaus am EARN/Bitnet angeschlossen zu bleiben. Als Übertragungsmedium wird ebenfalls das wissenschaftliche Hochschulnetz dienen, da auch der deutsche Betreiber (Gesellschaft fuer Mathematik und Datentechnik) inzwischen versichert hat, den deutschen Zentralknoten DEARN weiter zubetrieben.

In Deutschland kann man weitergehende Informationen über EARN/Bitnet von IBM Heidelberg, von der GMD in Darmstadt oder Bonn oder aber von mir bekommen.

Terra
(151133 DOLUN11.Bitnet)



FIDO - weltweite Kommunikation im Namen des Hundes

1. Allgemeines

Als freakige Alternative zu den damals gerade entstehenden kommerziellen Rechnerverbunden enstand FidoNet aus der Unzufriedenheit der Standalone-Mailboxuser in den USA Anfang der 80er Jahre. Mittlerweile sind weltweit ueber 5000 Systeme dem Netzwerk angeschlossen. Sie stehen in den USA, in Europa und Asien, sowie Australien. In der Bundesrepublik Deutschland sind ueber 50 Mailboxen angeschlossen. Die International FidoNet Association (IFNA) wurde vor einigen Jahren gegruendet. Ihre Aufgabe ist die Koordinierung allgemeiner Netzwerkangelegenheiten. Die IFNA gibt eine Gazette heraus, schlaegt Normen fuer Uebertragungsprotokolle vor und sorgt fuer ein woechentliches Update der 'World-Nodelist', dem Verzeichnis aller Netzknoten. Benutzt und betrieben wird das Netz von Privatleuten. Kommerz gibt es in der Fido-Philosophie nicht. Wer als Systembetreiber etwas an seiner Mailbox verdient, ist angewiesen, einen bestimmten Geldbetrag dem 'Shanty-Project', einer AIDS-Initiative in San Franzisko, zu spenden. Firmen haben aus Prinzip keinen Zugang zu FidoNet. Gebuehren, die von den Usern gezahlt werden, um die Betriebskosten zu decken, sind aber erlaubt. Den Benutzern ist nicht gestattet, Pseudonyme zu benutzen. Eingetragen werden duerfen nur die Realnamen, und obligatorischerweise ist es verboten, 'Raubkopien' anzubieten, oder hochzuladen. Ansonsten wird immer wieder betont, dass jeder SysOp die Regeln seiner Mailbox selbst bestimmen kann.

Der Service besteht im FidoNet aus E-Mail (persoenliche Nachrichten) und die 'Echomail Conference' - lokale oder regionale Diskussionsforen zu verschiedenen auch nichttechnischen Themen.

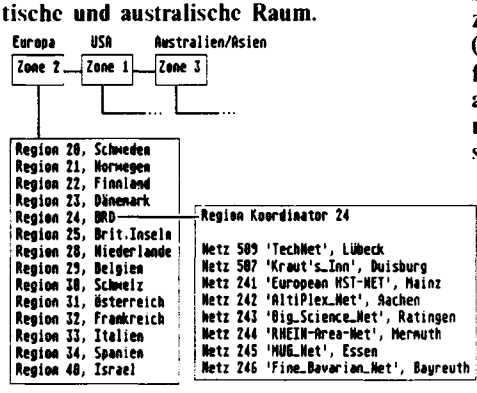
Zwischen den Nodes werden die Nachrichten wachrend des 'Mailslots' (Briefschlitz) ausgetauscht. Der 'Mailslot' ist eine weltweit einheitliche Uhrzeit, die mit 02:30 Uhr bis 03:30 Uhr GMT angegeben wird. In Deutschland ist das bei mitteleuropaeischer Sommerzeit von 04:30 Uhr bis 05:30 Uhr MEZ, in der Winterzeit verschiebt es sich auf 03:30 Uhr bis 04:30 Uhr MEZ.

Eine besondere Option in FidoNet ist der 'Point'. Ein User kann dabei eine Point-Nummer bekommen und bildet so

einen eigenen Privat- Node. Anders als normale User laesst dieser seinen Computer selber 'pollen', um die neuen Nachrichten als Paket abzuholen. Offline koennen diese dann in Ruhe gelesen und ggfs. kommentiert werden. Auf diese Weise lassen sich Telefoneinheiten sparen, die online sonst durch Nachdenken oder Einfinger-Adler-Suchstrategie verloren gehen. Die Moeglichkeit kann auch von FidoNet-Mailboxen genutzt werden, die sich nicht an den regulaeren Mailslot halten koennen oder wollen.

2. Netzstruktur

Einzelne Nodes sind zu Unter-Netzwerken zusammengeschlossen, die von einem Koordinator betreut werden. Diese 'Netzwerke' ergeben zusammen mit unabhaengigen Nodes 'Regionen', die wiederum zusammengefasst 'Zonen' bilden. Zur Zeit existieren drei Zonen, die auch geographisch auseinander gehalten werden koennen: Zone 1 bedeutet USA, Zone 2 Europa, Zone 3 ist der asiatische und australische Raum.



Zone 2 (Europa) besteht aus 13 zusammengefassten Regionen. Die Bundesrepublik ist mit Region Nr.24 vertreten. Diese wird aus acht 'Netzwerken' gebildet, an denen jeweils unterschiedlich viele Einzelsysteme angeschlossen sind. Die Staedtenamen hinter den Netzwerkbezeichnungen geben den Standort der einzelnen Netzwerk-Koordinatoren an. Koordinator der gesamten Region Nr.24 ist der Netzwerk-Koordinator von Nr.509 (Snoopy's BBS, Luebeck). Alle Klarheiten beseitigt? Adressiert werden E-Mails mit dem Empfaengernamen, sowie der Netzadresse, die sich wie folgt zusammensetzt:

zone:netzwerk/node

z.B.: 2:509/1 ('Snoopy's BBS', Luebeck)
er 3:700/88 ('Executive Board', Hongkong)

3. Ich will Fido...

Wer mit seiner Mailbox an das FidoNet gehen will, sollte am besten einen 16Bit-Rechner mit Festplatte und als Betriebssystem wenigstens MS-DOS benutzen. Implementationen gibt es auch schon auf Atari ST. Ein schnelles Modem von mindestens 1200bps ist natuerlich wichtig. Ausserhalb Europas sind Geschwindigkeiten von 9600bps ja schon lange keine Seltenheit mehr. Eine FidoNet-Mailbox sollte in der Lage sein, sowohl Anrufe von anderen Systemen zur Datenuebertragung anzunehmen ('PICK UP'), als auch selber anzurufen ('POLL'). In der Praxis sollte das allerdings mit dem SysOp des naechstgelegenen Fido-Nodes abgesprochen werden können.

Welche Netz-Software?

Es gibt zwei Programmpakete, die voll auf FidoNet ausgerichtet sind. Das eine heisst - man glaubt es nicht - 'FIDO' und kann fuer Geld gekauft werden. Das andere heisst OPUS, ist inklusive einiger Zusatzprogramme und Dokumentation Public Domain und am meisten verbreitet. Die Benutzeroberflaeche ist amerikanisch-menueorientiert. Wer auf seine gewohnte Shell nicht verzichten will oder eine andere fuer sinnvoller haelt und ausserdem nicht schlecht programmieren kann, hat auch die Moeglichkeit, seine eigene Implementation zu bauen. Zur Hilfe kann

Cayman Inseln ..... Direktwahl (1872) St. Kitts ..... Direktwahl (1-800-872-2881)

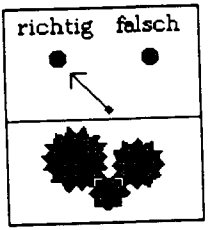
dazu die Fido-Dokumentation 'FSC001 A Basic FidoNet(tm) Technical Standart' genommen werden, in dem die FidoNet-Datenformate und Protokolle definiert sind. Ausserdem sollte auch das Dokument 'FSC002' besorgt werden. Darin wird das Format der IFNA-Nodelist beschrieben. Ist es irgendwann endlich geschafft, kann der erste Testbetrieb am Netz stattfinden. Die endgueltige 'Aufnahmepruefung' eines werdenden Fido-Nodes besteht darin, eine Nachricht an den jeweiligen Netzwerk-Koordinator zu senden. Wenn das gut geht und eine Antwort zurueckkommt, wird die Mailbox in die Nodelist aufgenommen.

Soweit eine oberflaechige Beschreibung von FidoNet.

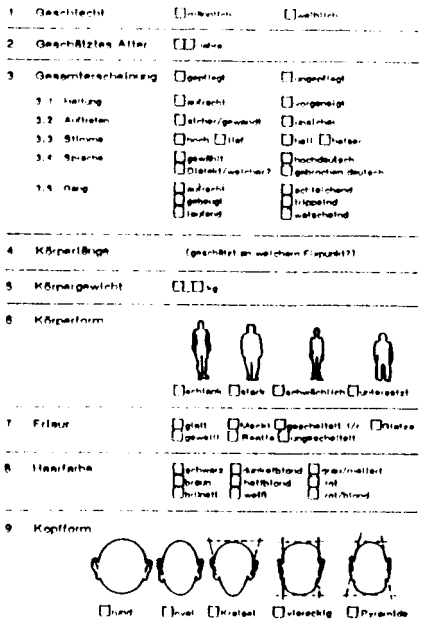
Weitere Informationen:

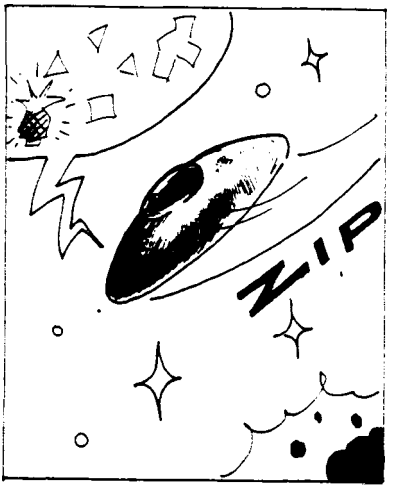
'FSC001 A Basic FidoNet (tm) Technical Standart' 'FSC002' Nodelist-Dokumentation 'FidoNet Policy' Grundsaetzliche Rgeln des Netzes Diese Files koennen in der Regel von den Netzwerk-Koordinatoren bezogen werden. Z.B. Netzwerk 509: Snoopy's BBS, Luebeck, 0451/493920

Bo-Chen Lo (china@subetha.UUCP oder FIDO 2:509/1)



Personenbeschreibung





Chaos Computer Club e.V. Redaktion Datenschleuder
Schwenckestrasse 85 D-2000 Hamburg 20 Telefon 040 - 490 37 57
Mbx (12/24 8N1): 040 - 491 10 85 / BTX: *CHAOS* / Geo1/Ifxl/Mbkl: Chaos-Team

Bestellfetzen 198911/08

Mitgliedschaft im CCC e.V. *

Schliesst ein Abo der Datenschleuder u.a. mit ein.

—— evvw	20.00	(D)M	Einmalige Verwaltungsgebuehr bei Eintritt.
—— evnm	120.00	(D)M	Normalmitgliedschaft Jahresbeitrag
—— evsoz	60.00	(D)M	Sozialmitgliedschaft Jahresbeitrag (f. Schueler, Studenten, Arbeitslose u.ae.)
—— ifxinf	2.00	(D)M	Information / Antrag zur Teilnahme auf dem Chaos Communication Center auf der Infex-Mailbox

Reine Datenschleuder Abo's *

Ein Abo gilt fuer ein Chaos-Jahr, garantiert aber 8 Ausgaben.

—— nabo	60.00	(D)M	Normalabo der Datenschleuder
—— sabo	30.00	(D)M	Soz. Abo (s.o.)

Sonstige Literatur

—— habil	33.33	DM	Die Hackerbibel, Teil 1 (260 S. A4)
—— habi2	33.33	DM	Die Hackerbibel, Teil 2 (260 S. A4)
—— wund	28.00	DM	Das Chaos Computer Buch (250 S. A5)
—— stud	7.50	DM	Studie fuer die Gruenen ueber politischen Computereinsatz im Bundestag - und ueberhaupt
—— mutst	10.00	DM	Mensch-Umwelt-Technik Studie: Elektronische Informationssysteme fuer den Umweltschutz
—— kamj	10.00	DM	Der elektronische Kammerjaeger / Ueber Wanzen, Abhoermethoden und Erkennung dergleichen.
—— mosk	26.00	DM	Hacker fuer Moskau / Hintergruende d. KGB-Story (unzensierte 1. Auflage) (224 S. A5)

Infopakete / Software & Co

—— vir	25.00	DM	Infopaket Computerviren (inkl. MS-DOS Demovirus)
—— pcd	25.00	DM	PC-DES (f. MS-DOS): Verschluesselung von (Text-) Dateien fuer jedermann/frau.

Backer

—— 3ks	3.33	DM	3 Aufkleber "Kabelsalat ist gesund" + Chaos Knoten (wassergeschuetzt)
—— ah	3.33	DM	Bogen mit 64 Aufkleber "Achtung Abhoergefahr" in postgelb zum selberausschneiden
—— pvt	??.??	DM	Porto / Verpackung / Trinkgeld / Spende (Zutreffendes bitte streicheln)

BE
STELL
FET
ZEN

* Mitgliedschaften und Abo's für DDR-Bürger 1:1 in OstMark, möglichst in DDR-Briefmarken zahlen.

Summe: ——.—— DM (Versand erfolgt fruehestens nach Geldeingang)

Zahlweise (bitte bekreuzigen oder so):
- Bar — V-Scheck — Rostwertzeichen (nicht groesser als 1.-)
- Ueberweisung (Postgirosamt HH / BLZ 20010020 / Kto. 599090-201)

Name : ————————————
Vorname : ————————————
Strasse : ————————————
Ort : ————————————
Telefon : ————————————

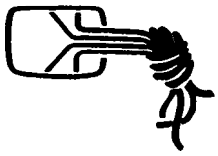
————————————
Datum, Unterschrift

(** nur b. Mitgliedschaft notw.)

Nur fuer Chaos-Verwaltungszwecke:

Eingang _____ Betrag erhalten _____ Erledigt _____

6. C h a o s Communication C o n g r e s s 1989



DAS Treffen für Datenreisende, Hacker, Häcksen und Netzwerker!
Aktive Workshops, Video- & Papercopiers.

TERMINHINWEIS

WAS WANN WO:
6. Chaos Communication Congress, **vom 27. bis 29. Dezember 1989** im Eidelstedter Bürgerhaus, Elbgaustr. 12, D-2000 Hamburg 54

TEILNAHME:

CCC Mitglieder	23,- DM
Private Teilnehmer	33,- DM
Kommerzielle Teilnehmer	103,- DM
Presse	53,- DM

DDR-Bürger können unter Vorlage gültiger Reisedokumente Eintritt und Kaffee 1:1 in Ost-Mark zahlen.
Die Teilnahmegebühr gilt für alle Congresstage und Veranstaltungen. Nur Pressevertreter benötigen ein Passfoto!
TV-Teams mögen sich bitte anmelden.

VORANMELDUNG:
Durch Überweisung auf
Konto Nr. 59 90 90 - 201
des Chaos Computer Club beim Postgirosamt Hamburg (BLZ 200 100 20). Einzahlungsbeleg dient als Quittung für die Teilnahme (also bitte mitbringen).

Knackplätze: Auf Anfrage (Geschäftsstelle, Dienstag Abends)

VOR ORT:
Ab dem 27. Dezember, 14 Uhr sind wir auf dem Congress erreichbar.

Projektleitung/Zentrale	040 570 - 8228
Pressestelle	- 3664
Fax	- 6765

Ab dem 1. Dezember ist (hoffentlich) das Konferenzsystem des Congresses erreichbar.

Chaos	(=300 Bps)	040 570 - 2911
Communication	(=300 Bps)	- 3424
Center		- 4445 / -7488

Während des Congresses sind über diese Rufnummern die vor Ort betriebenen Mailboxsysteme erreichbar.

Wir danken der Dr. Neuhaus Gruppe für die pestgeprüften Datenmodems zum Konferenzsystem.

VORBEREITUNG:

CCC Geschäftsstelle (Di+Do Nachm)		040 4903757 Q
Pressearbeit	(J.Wieckmann)	040 275186
Organisation	(S.Wernery)	040 483752 Q
Fax		040 4803181

MITARBEIT:
Wie in den vergangenen Jahren auch, werden dieses Jahr zahlreiche Chaos-Engel zur Gewährleistung des Congress- ablaufs gesucht. Aufbau, Abbau und Betriebshelfer sollten frühzeitig anreisen.

Am Montag dem 25. Dezember gegen 12 Uhr werden die Räumlichkeiten im Eidelstedter Bürgerhaus bezogen. Nach Abschluss der Kabelinstallationen, gegen 16 Uhr, können die Teilnehmer ihre Technik aufbauen. Auswärtige Gäste können zum Abend bereits anreisen.

Am Dienstag dem 26. Dezember 10 Uhr wird der Aufbau und die Einrichtung des Archivs, Congressredaktion, Cafe, usw fortgesetzt. Dieses soll bis 16 Uhr abgeschlossen sein, so dass am Abend die letzten inhaltlichen Vorbereitungen erfolgen können.

Der Congress beginnt am Mittwoch dem 27. Dezember um 12 Uhr (Einlass ab 10 Uhr) und endet am Freitag dem 29. Dezember um 17 Uhr. Anschliessend werden ab 19 Uhr die Räume geräumt.

Der genaue Congressfahrplan wird Anfang Dezember erstellt.

MELDUNGEN:
Referenten und andere, die aktiv am Congress mitwirken möchten, wenden sich bitte an Steffen Wernery 040-483752 (nach Mittag's)
GEO1:S.WERNERY, STEFFEN@NETW.ZER
oder ihre Kontaktperson.

- Wir bitten um Verbreitung dieses Hinweises -