```
 CCCCC  H    H    AA    L       I   SSSSS  TTTTTT  I
C       H    H   A  A   L       I  S         TT    I
C       HHHHHH   AAAA   L       I   SSSS     TT    I
C       H    H  A    A  L       I       S    TT    I
 CCCCC  H    H  A    A  LLLLLL  I  SSSSS     TT    I
```

Ausgabe 4

Erlaeuterungen:
DS - Datenschleuder
RC - Redaktion Chalisti
CR - Congress Redaktion
MK - Mik-Magazin
NE - Uebernommen aus einem Netzwerk
FA - Freier Artikel (Autorenangabe am Anfang oder Ende des Artikels)

Die Artikelkennung (DDS1,DMK2,etc) dient zum suchen der Artikel mit Editoren und Textverarbeitungssystemen. Mit der Marke 'NEXT' kann gleich zum naechsten Artikel gesprungen werden.

[Contrib][Chalisti][04] Inhaltsverzeichnis

Editorial

Das war er nun, mein erster Chaos Communication Congress. Wie war's ?
Nun, im grossen und ganzen war's super, auch wenn der Congress haupt-
saechlich von der Initiative einzelner lebte, die wiederum die Selbst-
darstellungswut anderer einzelner kompensieren konnte. Ich will mir als
nicht CCC-Mitglied nicht anmassen ueber CCC-Interna zu urteilen, aber mit
meiner eigenen Meinung auch nicht hinter dem Berg halten.

Ich fand es z.B. super, dass ein Vortragender, weil es Ihm so gut gefiel,
den Congress fuer Ihn um einen Tag verlaengerte, mit allen Konsequenzen
wie Zimmersuche, etc. .

Frei nach Terra "Die Chalisti ist zwar ein Magazin des CCC's, aber nicht
immer ein CCC freundliches Magazin" sprich das beruehmte "unabhaengig und
ueberparteilich", will ich hier auch meine Kritik am Congress und am CCC
loswerden. So z.B. die drohende Spaltung des CCC's in Steffens KKK und die
Betonkopf-Fraktion. Auch der Versuch von einigen die nicht stattgefundene
Verlegung des Congresses nach Ost-Berlin, so darzustellen, dass es letzt-
endlich kein Mehrheitsentscheid war. Obwohl z.B. die vielgeruehmten
"Sachzwaenge" die Verlegung erstmal verhindert haben.

Diese Chalisti 4 besteht faktisch aus Congresstexten, aber das hatten wir
ja in der letzten Chalisti schon angekuendigt. Die 3 vorherigen Chalisti's
sind im 4 Wochen Takt erschienen, deswegen werdet ihr ja sicher nix dagegen
haben, wenn wir uns diesmal 6 Wochen Zeit lassen. Die Chalisti 5 wird
vermutlich am 10.2. im naechsten Jahrzehnt erscheinen.

Was gibt es sonst noch ... Die Chalisti Redaktion wuenscht allen Lesern
(Ja genau ... Euch meinen wir) einen guten Rutsch ins neue Jahr. Wenn Ihr
nicht rutschen wollt, empfehlen WIR Euch: Schreibt einen Artikel fuer die
Chalisti. Man kann damit Naechte verbraten - es ist kaum zu glauben...

Fly & Terra

Chaos Hagen auf dem Weg ins Chaos

2nd Weihnachtstag 8.45 Uhr der erste Mensch - Thomas - laeuft bei mir zum Fruehstueck auf.

Die Augen noch leicht geschlossen - gestern bis tief in die Nacht ueber die "Nationale Frage" diskutiert. Wie war das noch: Selbstbestimmungsrecht fuer alle Voelker - Unterschied zwischen Nation und Kulturnation (z.B. deutscher Sprachraum: Schweiz, Oesterreich, DDR, BRD, vielleicht noch die Siebernbuerger, ...) - welche Perspektive haben wir als Linke - der Kapitalismus als imperiale Struktur verleibt sich gnadenlos die Gebiete im sozialistischen Lager ein. Nun - an sich wollte ich hier keinen Artikel ueber die teutsche oder welche auch immer Nation schreiben, sondern "unsern Weg ins Chaos".

Weisst du schon? Karsten ist krank! sagt Uli, als er zur Tuer reinkommt. Ach du schei...unser Netzspezialist faellt aus - kann nicht ersetzt werden - muss das Bett hueten - wird hoffentlich bald wieder gesund!
Leichte Niedergeschlagenheit - aber da muessen wir durch!

Nach einem eher ruhigen Fruehstueck machen wir uns dann - mit den Pooftueten unterm Arm - auf zum Bully des Hagener Hockey Clubs. Eben noch die noetige Hardware eingepackt (haste auch die Steckleiste fuer die Anschluesse dabei)? Ach, wir fahren noch bei Karsten vorbei, weil bei dem steht ja der Schlepp-top, auf dem ich jetzt den Text schreibe.

Also rueber zum Kranken - ihm kurz ins Auge geschaut und gute Besserung gewuenscht, Tanken und ab geht's und komm - ich schreib den Text jetzt direkt auf den Knien in die Kiste - aber oh weh "Bitte warten ... " und dann - hat dieser Armleuchter etwa "Schittbatterien" gekauft?
Beep, Beep, ...
Ausserdem stellt sich raus, dass die DIP-Schalter (und davon gibts 6 Stueck!) offensichtlich so eingestellt sind, dass statt LCD der Fremdbildschirm angesteuert wird. Nun ja, dann versuchen wir mal, die 720 Moeglichkeiten durch (ja klar, RFM - waere ja gut, aber wir haben kein Manual dabei).
Ach so, 2nd Weihnachtstach heisst auch, dass die Autobahnen zu sind, vor allem die A1. Aber wir als Kinder des Ruhrpotts kennen unsere Autobahnen: A45 -> A44 -> A43 -> A1 -> ... auf nach HH!

Zwischenstopp auf der Raststaette Muensterland. Voice back home - der Kranke soll schliesslich auch was zu tun haben: komm, such mal die DIP-Schalterstellungen raus. Wieder unterwegs, Netzteil aufschrauben, kommen wir an das Saftkabel ran? Nein, das kann nicht wahr sein - ein verklebtes Gehaeuse!

An der uebernaechsten Autobahnraststaette 'n Taesschen Kaffee, fuer 0.20 DPF Strom geliehen und mal angefangen, diesen Artikel einzutippen. Dann noch ein wenig auf der Autobahn und jetzt sitz ich hier endlich in der Pressestelle und hab eigentlich jetzt keine Zeit mehr zum Tippen.

Ciao, Ludger

GEDO@BOSKOPP.UUCP
GEDO@GLOBAL.ZER

[Contrib][Chalisti][04] Chaos Hagen auf dem Weg ins Chaos

Computer und Telefon in der DDR

Obwohl das Thema der Podiumsdiskussion "Das Telefonnetz in der DDR" lautete, wurde erst einmal eine Bestandsaufnahme der Technik, die zur Zeit in der DDR benutzt wird, gemacht. So sind zum Beispiel in der DDR die verbreitesten Rechner der C64, Spectrum, Atari XL und Geraete auf Z-80 Basis. Ein C64 kostet dabei in der DDR etwa 7000 Mark bei einem Monatseinkommen von ca. 900 Mark. Die Heimcomputer des VEB Robotron sind teilweise nicht sinnvoll nutzbar und Drucker werden nur in den Westen exportiert.
Im professionellen Bereich sind CP/M Geraete noch Standard. Die DDR-eigenen XTs sind nur zu 90% kompatibel zum Industriestandard. Weil der VEB Robotron zu lange auf 286er-Technologie gesetzt hat, wird Unix nur vereinzelt auf 386ern, die entgegen den CoCom Bestimmungen aus dem Westen importiert wurden, eingesetzt. Ein Verschicken von Disketten in die DDR ist/war wegen der Willkuer des DDR-Zolls nicht moeglich, weil nach dem Gesetz der magnetische Traeger ueberpruefbar sein muss und die Technik fuer die Ueberpruefung nicht vorhanden ist.

Das Telefonnetz

In der DDR hat nur ca. jeder zehnte Haushalt einen Telefonhauptanschluss. Der Muenzer um die Ecke ist immer noch ein alltaeglicher Notbehelf. Aber selbst dann hat man mit der alten Technik zu kaempfen: Die Vermittlungs-anlagen und Kabel (aus den 20er und 30er-Jahren) schreien nach Erneuerung. Darueber hinaus sind viele Telefonanlagen in Firmen und Instituten in ihrer Reichweite auf das Stadtgebiet begrenzt. Fuer 80 Mitarbeiter stehen manchmal nur drei Amtsleitungen zur Verfuegung.

Die Kosten fuer einen Telefonanschluss sind vergleichsweise gering:
26.- Mark kostet der Anschluss monatlich, ein in der Laenge unbegrenztes Ortsgespraech etwa -,50 Mark. Von Ost-Berlin nach West-Berlin gilt der Dreiminutentakt (pro Einheit -.85 Mark). Aber es ist nicht unueblich, dass zehn Jahre vom Tag der Antragstellung bis zum tatsaechlichen Anschluss des ersehnten Apparats verstreichen.

Datenfernuebertragung

Aber selbst wenn man nun einen Anschluss zur Verfuegung hat, kann man noch keine DFUe machen: Fuer Privatleute ist es praktisch unmoeglich, DFUe zu betreiben, weil es rechtlich untersagt ist und Antraege nicht bearbeitet oder abgelehnt werden. Versuche einzelner Mitglieder von Computerclubs in blockfreien Staaten eine Mailbox oder ein Netzwerk zu benutzen wurden unterbunden.

Informationsaustausch

Besonders jetzt ist es notwendig, einen schnellen und auch billigen Informationsaustausch innerhalb kurzer Zeit zu realisieren, um z.B. Infos einzuholen und Diskussionsgrundlagen fuer Gespraeche am runden Tisch zu liefern. Dies ist noetig, weil bis jetzt nur die etablierten Parteien Informationen wirkungsvoll verteilen und austauschen koennen.
Es stehen verschiedene Modelle zur Diskussion, um diese Isolation der Gruppierungen aufzuloesen:
1) Verbreitung von Infos auf lokaler Ebene durch Fotokopieren
   Ist sicherlich in jedem Fall notwendig, um Infos weiterzuverteilen.

Aber das Problem des Transfers zwischen den Staedten und Staaten ist damit nicht geloest.

2) Videotext als Wandzeitung
   Im Fernsehen der DDR laufen z.Z. Versuche zum Installieren eines Videotextsystems. Die Videotextdaten werden zusammen mit dem Fernsehbild verschickt. Auf der Empfaengerseite wird nur ein relativ einfacher Decoder benoetigt. Dieses Modell hat aber den Nachteil, dass die Ausstrahlung zentral erfolgt. Ansonsten ist aber eine schnelle und weitreichende Informationsverbreitung gewaehrleistet.
3) Mailboxen und Telefax
   Zur Zeit ist eine Uebertragung von Daten ueber das veraltete Telefonnetz nicht moeglich, wie einige Versuche zeigten. Daher scheidet vorerst der Einsatz von Mailboxen, Mailboxnetzwerken und Telefaxgeraeten aus. Zwar ist bereits die Modernisierung des Telefonnetzes mit Hilfe der Deutschen Bundespost Telekom geplant, aber dies ist nicht kurzfristig realisierbar und bringt auch wieder die hierzulande schon bekannten Probleme des Datenschutzes und der Abhaengigkeit von Autoritaeten mit sich. Die Chance eines richtigen Neuanfangs wird durch die vorschnelle Einfuehrung von ISDN in der DDR unterlaufen.
4) Vernetzung ueber Packet Radio
   Von Wau ging der Vorschlag aus, ein Netzwerk ueber Packet Radio (DFUe per Funk ueber ein paketorientiertes, fehlerkorrigierendes Protokoll (AX.25)) zu realisieren. Man koennte einzelne Stationen mit einem sehr geringen Hardwareaufwand aufbauen (z.B. C64 + Funkgeraet + Schaltung fuer etwa 40 DM). Die Sourcen und die Dokumentation zum Netzwerk waeren einfach erhaeltlich. In der Bundesrepublik wird eine weite Ausbreitung des Packet Radio Netzes nur durch die Deutsche Bundespost Telekom verhindert, weil sie u.a. einen Gebuehrenschwund im Telekommunikations-sektor fuerchtet. Da aber beim Amateurfunk nur bestimmte Infos (keine politischen Meinungen) und keine verschluesselten Texte uebertragen werden duerfen, sollte man die Uebertragung auf den Bereich des CB-Funks verlagern, der ausserdem in der DDR noch nicht genutzt wird. Dies ist besonders heikel, weil der CB-Bereich in der Regel nur fuer Sprach-uebertragung vorgesehen ist. Aber da es zur Zeit keine gueltigen Gesetze in der DDR gibt, die dies regeln, koennte man die Luecke nutzen, ein System aufbauen und hinterher die Gesetze an diesen Fakten ausrichten. Dies muss aber sehr schnell geschehen, weil es in einem halben Jahr schon viel zu spaet fuer dieses Buergernetz waere. Wau haelt es fuer realistisch, innerhalb von 1/4 Jahr etwa 30 bis 50 Stationen zu installieren. Dabei sollten die Freaks und Funkamateure aus der DDR den technischen Part uebernehmen und die Buergerinitiativen diese Technik fuer ihre Zwecke benutzen. Ein Problem hierbei ist die drohende Ab-haengigkeit von den "Technikgurus", die ein neues Informationsmonopol bilden koennten.
5) Ein weiterer Standpunkt wurde von Wolfgang Schroeder (M.U.T.) ver-treten, der mehr Ideen anstatt uebermaessiger Technisierung fordert.

Zum Schluss der Veranstaltung "Buergernetze" wurde beschlossen, pragmatisch die einzelnen Modelle in Arbeitsgruppen zu planen und eine "Wunschliste" fuer Technik, die in der DDR gebraucht wird, aufzustellen. Jeder sollte seine, vielleicht hier schon veraltete Technik spenden, um beim Aufbau einer neuen, unabhaengigen Informationsstruktur in der DDR zu helfen. Zuerst sollten Fotokopierer den Organisationen bereitgestellt werden und ein Kommunikationssystem aufgebaut werden, das auch ausbaubar sein sollte. Auf den Datentransfer kann jetzt und in Zukunft nicht verzichtet werden.

Henne/Gec.

Buergernetze und Kommunikationsziele ohne eisernen Vorhang

Perestroika: Vom Staatspriestertum zur Glaspost

Untertitel: "Von der Amtspost ueber die Buergerpost zur Chaospost"

Am 27.12.89 fand unter grossem Interesse (der Theaterraum des Eidelstetter Buergerhauses war total ueberfuellt) die Podiumdiskussions ueber Moeglichkeiten und Chancen eines "Buergernetzes" in der DDR statt.
Auf dem Podium waren:

- Wolfgang Schroeder vom M.U.T. (Mensch-Umwelt-Technik), einer kleinen Umweltgruppe
- Wau Holland, CCC
- 2 Vertreter eines Ost-Berliner Computerclubs.

Nachdem in einer vorhergegangenen Diskussionsrunde die technischen Resourcen des DDR-Telefonnetzes eroertert worden waren ("Computer und Telefon in der DDR"), wurde nun ueber den Bedarf und die verschieden Moeglichkeiten eines dezentralen und unabhaengigen Informationsnetzes gesprochen.

Wau stellte gleich am Anfang seine Idee vor: Das alternative Buergernetz auf Basis des Packet Radio. Ausgehend von dem Datennetz der Amateurfunker, des Packet Radios, das ein x.25-network (in Deutschland DATEX-P genannt) beinhaltet, sollte es mit relativ einfachen technischen wie auch finanziellen Mitteln moeglich sein, ein DDR-weites Computernetz aufzuziehen, das vollstaendig unabhaengig von staatlichen Behoerden waere.
Dieses ax.25 genannte System ist von der Amateurfunkern entwickelt worden und koennte wohl von diesen erworben werden. Die Programme sind im Sourcecode erhaeltlich und sind praktisch PD. Naeheres muesste mit den Amateurfunkern abgesprochen werden. Aber von dieser Seite waeren keine Probleme zu erwarten.
Eine funktionierende Minimalkonfiguration fuer einen Knoten dieses Netzes waere zB: ein C64, ein Modem und ein Funkgeraet, wobei Wau nicht die teuren Amateurfunkgeraete meinte, sondern die relativ guenstigen CB-Funkgeraete.
Mit ca 300 Knoten und 20-40 Datenkanaelen waere ein Kapazitaet verfuegbar, das dem BRD-Datex-p entsprechen wuerde.

Fuer den raschen Aufbau dieses Buergernetzes fehlt allerdings die Hardware. Es seien nun alle geneigten Leser aufgerufen, ihre alten, nicht mehr gebrauchten Akkustikkoppler, Modems, 8-Bitler etc an die DDR-Computerclubs zu spenden. Die Adressen koennen beim CCC erfragt werden.

- Framstag

Dummheit / Schlauheit in Netzen

Ein staendiges Problem in Mailboxen und Netzwerken sind die vielen sogenannten Dummuser und der von ihnen produzierte Datenschrott. Darum und um alle Randerscheinungen drehten sich die Diskussionen in den Veranstaltungen "Dummheit in Netzen" und "Semiprofessionelle Mailboxnutzung".

Inzwischen ist es wohl so, dass etwa 90% aller Nachrichten fuer den einzelnen Benutzer uninteressant sind, je nach Interessenlage verschiedene Bereiche. Dies liesse sich durch ein geeignetes Datenbanksystem verhindern oder begrenzen. Die heutige Bretterstruktur vieler Boxen ist nur etwas wie ein klaeglicher Versuch, die Datenflut zu sortieren. In Zukunft sollte man Mailboxsysteme planen, die sich ueber eine Datenbankabfragesprache bedienen lassen, um die zu erwartenden Datenmassen ueberhaupt noch sinnvoll verarbeiten zu koennen. Die Betreffzeilen reichen schon heute kaum mehr fuer eine Vorselektion von Nachrichten aus.
Eine andere Moeglichkeit waere die Einrichtung von moderierten Brettern, in die nur Infos und keine Kommentare, die meist fluessiger als fluessig und daher von vielen Leuten unerwuenscht sind, kommen. Nachrichten kann man dann nur persoenlich an einen gewaehlten Moderator schicken, der sie bei Gefallen in das schreibgeschuetze Brett weiterleitet.
Praktiziert wird dies bereits bei Konferenzen in diversen Mailboxen in den USA.

Es sollen aber auch noch andere frei beschreibbare, unzensierte Bretter zur Verfuegung stehen, um den Benutzern ihr Recht auf freie Meinungs- bzw. Muellverbreitung zu erhalten. Dies ist schliesslich ein entscheidender Vorteil im Vergleich zu herkoemmlichen Medien. Jeder hat das Recht, etwas zu schreiben, hat aber aber auch die Freiheit, es zu lassen.

Aber nicht nur die Daten muessen anders verwaltet werden. Um interessante Beitraege und kompetente User anzuziehen, muessen die Mailboxprogramme bedienbar werden. Der GeoNet-Standard ist hierbei schon ein Schritt in die richtige Richtung, weil er nach einer relativ kurzen Lernphase einen recht maechtigen Befehlssatz zur Verfuegung stellt, der auch noch dem erfahrenen User ausreicht. Nun muessen die Benutzer die Mailboxen nur noch begreifen und sinnvoll nutzen. Man muss bei den Benutzeroberflaechen einen Kompromiss zwischen Bedienbarkeit, Geschwindigkeit und Effektivitaet von einzelnen Befehlen finden: waehrend umfangreiche Menues (z.B. Btx, Fido) fuer den Anfaenger optimal sind, werden erfahrene Benutzer davon eher genervt. Das Konzept der Zukunft scheint eine Schreibtischmailbox fuer jeden Benutzer zu sein, die mit einer beliebigen Benutzeroberflaeche laeuft und verschiedene Netzwerkmailboxen (Server) anrufen (pollen) kann. Die Mailboxen wuerden erheblich entlastet und schliesslich zu reinen Servern umfunktioniert, die die Post fuer die Benutzer zum Abholen bereitstellen. Jeder Benutzer koennte dann komfortabel die ganze Welt mit seinem heimischen Computer jederzeit erreichen. Die Verbindungen werden automatisch nachts, wenn es billiger ist, aufgebaut.

Um Mailboxen attraktiver fuer Nicht-Computerfreaks zu machen muss sich auch die Einstellung einiger Sysops zu ihrer "Arbeit" aendern. Alles muss etwas professioneller werden und die Funktion in Richtung Dienstleistung gewandelt werden. Dann ist es auch moeglich, Geld fuer die Dienstleistungen (fuer Datentransfer, Hilfestellungen, Informationsdienste) zu verlangen, um das Medienprojekt zu finanzieren und ein stabiles System aufzubauen. Die Freak-

zeit mit den selbstgestrickten und kostenlosen Mailboxen scheint vorbei zu sein.
Es faellt immer wieder auf, dass der Sysop als Autoritaetsperson angesehen wird, was auch zu einer gewissen Selbstherrlichkeit des "Gottes ueber die Bits und Prios" fuehrt. Dies kann nicht Ziel eines Kommunikationssystems sein. Die Sysops sollten ihre Position und Funktion ueberdenken.
Dazu zaehlt auch eine Erhoehung der Datensicherheit: Der Sysop sollte nicht mitlesen koennen, was der User macht und die persoenlichen Nachrichten sollten verschluesselt gespeichert werden.

Das Ziel all dieser Bemuehungen ist dabei, mehr Nicht-Computerfreaks ein leicht bedienbares Medium zu geben, das darueber hinaus unabhaengig von Informationsmonopolen ist.
Denn bereits jetzt besteht die Gefahr, dass ein Informationskrieg entbrennt und grosse Verlage sich in Mailboxsysteme einkaufen, um nicht allein auf das vielleicht bald ueberfluessige oder weniger bedeutsame Zeitungsgeschaeft angewiesen zu sein.
Der grosse amerikanische Mailboxbetreiber CompuServe hat bereits einen Vertrag mit einem schweizer Unternehmen geschlossen, um auch in Europa ein Standbein zu haben. Deutsche Verlage versuchen mit mehr oder weniger Erfolg eigene Datenbanken und Informationssysteme aufzubauen.

Die E-Mail hat eine grosse Zukunft in der Bundesrepublik. Auch Hobby-netzwerker und private Mailboxbetreiber sollten ueber einen Schritt in Richtung Professionalitaet nachdenken, um eine attraktive Alternative zu den kommerziellen Anbietern zu schaffen.

Henne.

[Contrib][Chalisti][04] Dummheit / Schlauheit in Netzen

Das Poststrukturreformgesetz und seine Konsequenzen fuer Mailboxbetreiber

Fachschaft Jura der Uni Bielefeld - Datenschutzgruppe: Adolf (Addy), Baerbel, Werner

"Jederman (ich bin wirklich kein Chauvi, sondern der Gesetzgeber, d.S) ist berechtigt, sogen. Telekommunikationsdienstleistungen ueber Fest- oder Waehlleitungen zu erbringen."
Das steht im Poststrukurgesetz; es gilt ab dem 1. July 1989; damit werden Mailboxen zu Fernmeldeanlagen!

Das Telefonnetz steht aber weiter unter dem Fernmeldemonopol der DBP (-Telecom).

@25 des Poststrukturgesetzes: Bundespostministerium hat sich an den Grundsaetzen der Politik der BRD zu orientieren!

September 1988 wurde festgestellt, dass das Gesetz ueber die Einschraenkung des Fernmelde- und Postgeheimnisses (G10) vergessen worden war. Sie kamen auf den Dreh: Wenn das Poststrukturgesetz geaendert wird, dann gilt auch das Fernmeldegeheimnis, also muss auch das Gesetz ueber den Eingriff in dies Gesetz (G10 genannt) mit reingenommen werden. In ihrer Sicherheitsphilosophie nur logisch: es sollen keine Nischen entstehen, in die sich "Verbrecher oder Terroristen" einnisten. Deshalb werden Kontrollmoeglichkeiten geschaffen, die moeglichst weit gehen sollen. Sie schliessen die letzte Nische, wo sie bisher nicht hin koennen! Dies ist "nur" die konsequente Ergaenzung des Sicherheitspakets bestehend aus ZAG (Zusammenarbeitsgesetz), Verfassungsschutzgesetz, Gesundheitsreformgesetz (Datenuebertragung zwischen Krankenkassen, Aertzen, ...) uvam. Auf Anordnung koennen BfV, LfV, MAD und BND Auskunft ueber durchgefuehrten Fernmeldeverkehr (z.B. auch in Mailboxen) vom Fernmeldeanlagenbetreiber (also z.B. dem SysOp einer Mailbox) verlangen. Personal muss auf Anfrage von dem Mailboxbetreiber zur Verfuegung gestellt werden. Bei Gefahr im Verzuge auch ohne richtlichen Beschluss. Es gilt natuerlich auch immer 129 StGB (Unterstuetzung einer terroristischen Vereinigung): wenn bestimmte Tatsachen den Verdacht begruenden (und das heisst nach der Erfahrung der letzten Jahre - siehe den Weckerkauf von Ingrid Strobel, ..) im Prinzip immer (das ist die Regel - die Ausnahme von der Regel) kann ohne richterlichen Beschluss von den Kraeften der Bullizei direkt gehandelt werden! Der richterliche Beschluss wird dann "nachgereicht"! Auch ein Telefonat mit dem eigenen Rechtsanwalt, der vielleicht eine einstweilige Verfuegung bewirken koennte, hat keine aufschiebende Wirkung!
Es ist immer "Gefahr im Verzuge"!

Technisch:

"Die Ueberwachung des Fernmeldeverkehrs ist zu ermoeglichen!"

Aber: die Ueberwacher brauchen einen Beschluss vom Richter! Den koennen sie aber nachreichen!

In Augenscheinnahme --- du (als Mailboxbetreiber) musst es ihnen ermoeglichen, die Festplatte duerfen sie nicht etwa mitnehmen, sondern sie duerfen "nur" ueberwachen!

Diese Ueberwachung bezieht sich auf Fernmeldeanlagen (also auch Mailboxen), aber beachte:
1. Eine Fernmeldeanlage (sprich die Mailbox) endet nicht hinter dem Mond, sondern auf der Platte!
2. Die Userliste (oder die Backup-Disketten) im Schrank ist ein Blatt Papier - gehoert also nicht mehr zur Fernmeldeanlage!

Alle Daten ueber die User sind rauszugeben! Aber: was ich nicht weiss, kann ich nicht weitergeben - ich hab keinen Zugriff!

"Bin ich als Mailboxbetreiber verpflichtet, persoenliche Daten zu sammeln?" Nein!

Die Ueberwachung muss sich nach diesem Gesetz eindeutig auf "namentlich bekannte" Personen beziehen. Kann Name ein Pseudonym sein! Ja! Wenn es eine bestimmte Person ist, die nicht in der Mailbox ist, ist der Fall an sich gegessen! Unterlaufen durch Verschluesselung ist moeglich! Wenn User die eigenen Daten mit Passwort verschluesseln, kann der SysOp die persoenlichen Mitteilungen garnicht lesen. SysOps sind nicht verpflichtet, Zusatzeinrichtungen zu beschaffen, mit denen das "Entcrypten" der Daten ermoeglicht wird! Was auf dem Bildschirm erscheint, haengt vom Programm ab, mit dem die Mailbox betrieben wird. Aber die Ueberwacher duerfen auch die Telefonleitung komplett ueberwachen (geht nach G10 eh'). Man muss aber das Mitprotokollieren ermoeglichen.

Es darf niemandem zu Kenntnis gebracht werden (also insbesondere den Usern einer Mailbox nicht), was nach dem Ueberwachungsrecht gemacht wurde oder wird.

Man (der Ueberwacher) sucht den User X, findet aber bei der routinemaessigen Ueberwachung den User Y bei einer "nichtgesetzlichen Taetigkeit". Dann muss der Ueberwacher dieser strafbaren Handlung nachgehen - sonst ist das Strafvereitelung im Amt!

Sie haengen einem auf der Leitung und man kriegt keine Daten mehr rueber, dann kann man ihnen diese Kosten im Prinzip in Rechnung stellen! Ja!
(im Prinzip wenigstens!)
Also: Funktion der Mailbox darf nicht verhindert werden!

Brief- Post- und Fernmelderecht und Datenschutz Grundrecht auf informationelle Selbstbestimmung Widerspruch stehen sich gegenueber! -- Was ist mehr wert?

Art. 1 + 2 des Grundgesetzes sind hoeherwertig als die Einschraenkung des Post- und Fernmeldegeheimnisses.

Jede Mailbox muesste an sich datenschutzmaessig geschuetzt sein!

--------> Wird an der UNI BI diskutiert werden. Vielleicht wissen wir in 5 Jahren mehr!

Kann ich gegen ein Gesetz vorgehen? Ja! Normenkontrollverfahren eines jeden Betroffenen ist moeglich. Mailboxbetreiber sind Betroffene: also koennen sie ein solches Verfahren einstiehlen!

--------> Bulle und Bildschirm! Spracherkennung ist noch schwierig, aber ASCII-Analyse leicht moeglich! In den Staaten ist soetwas schon passiert! USENET.USE --- NSA und CIA ---

Diskussion + Informationsaustausch ueber Zerberus soll demnaechst erfolgen.

Detailtips, um Mailboxprogramme sicher machen zu koennen werden gewuenscht:
- persoenliche Mitteilungen duerfen beim SysOp nicht erscheinen; - die User koennen mit einem "Write protect Modus" selbst entscheiden, ob Messages beim SysOp angezeigt werden oder nicht.

Politisch:

Die Bielefelder FS-Jura (Gruppe Datenschutz) meint: Gerade bei Mailbox-betreibern geht es eher technisch-argumentativ zu:
technische Argumente werden benutzt, um sich vor Politik zu druecken!
Es fehlen politsche Inhalte auf Mailboxen und es fehlt oft auch politisches Bewusstsein bei Mailboxbenutzern und SysOps!

Wie koennen wir das ganze politsch kippen? Wir muessen uns einreihen in die grosse Gruppe der Gegner der Sicherheitsgesetzgebung - wenn wir das nicht schon lange haetten tun sollen.

sicherheitspolitsche Aufruestung ---> Wirtschaft und Wirtschaftlichkeit der TeleCom ist das Korrektiv fuer alle gesetzlichen Ueberlegungen!

Geht der Staat nicht ein wenig weit -- muss ich (als User oder Mailbox-betreiber) das hinnehmen?

Im Prinzip ist es dasselbe wie Fernmelde- und Briefgeheimnis. Briefe werden bei der Post schon geoeffnet! - da haben sie es nicht noetig, dem Empfaenger von Briefen auf die Bude zu ruecken.

Ab wieviel Teilnehmer muss ein Chatsystem als Demonstration genehmigt werden? Es kommt der Tag, wo ein Pseudonym als Vermummung gelten wird!

Unser Bundeskanzler Helmut Kohl (BuKaKo) freute sich ueber die Menschen in der DDR, die hingingen und sagten: "Das Volk sind wir". Sie gingen zu dem MfS (Ministerium fuer Staatssicherheit) und sahen nach, wie durch die Sicherheit des Staates geschuetzt wurde; warum sollen wir nicht mal nach Pullach (BND) oder Koeln (Bundesamt fuer Verfassungsschutz) gehen!
Ob sich dann BuKaKo - ach klar - er muss sich freuen!

Kontakt:
Fachschaft Jura Uni Bielefeld:
Universitaetsstrasse 25 4800 Bielefeld 1
Mo 18.00-20.00; (0521) 106 4292 Voice
E-Mail: FS-JURA@BIONIC.ZER
BIONIC-Tel.Nr.: 0521-17 11 88

Ludger
ChaosHa(gen)
gedo@boskopp.uucp & gedo@global.zer

Was soll der Staat duerfen ?

Von den Notstandgesetzen bis zur Stasi-Abschaffung

Da der angefragte SPD-Politiker Peter Paterna (PP; Postexperte der SPD, Mitglied des aus 5 Maennern bestehenden G10-Ausschusses des Deutschen Bundestages; nicht erschienen ist, wird die Podiumsdiskussion ohne ihn begonnen. Mit Peter Greger und Dr. Peter Pas nehmen zwei Kenner der Computerscene der DDR und Mitglieder des Neuen Forums (NF) an der Diskussion teil.

Adolf Groeger (Nickname Addy) Fachschaft Jura; Gruppe Datenschutz; Uni Bielefeld) fuehrt moderierend ins Thema ein: Dies ist der erste Congress, auf dem Gesellschaftspolitik betrieben wird!

Provokante These:
"Elektronisches Medien werden benutzt,um Politik zu verdraengen!"

"Terrorismus" nach der Definition der Bundesregierung ist "Bewaffneter Kampf fuer politische Ziele!" Einstieg ist das G10 (Gesetz zur Einschraenkung des Grundrechte nach Art. 10 Grundgesetz: Brief- und Fernmeldegeheimnis). Im Rahmen eines Normenkontrollverfahrens koennten Aenderungen am G10 durch das Postreformgesetz gekippt werden! Antragsberechtigt sind (weil Betroffene im Sinne des Grundgesetzes) User und Mailboxbetreiber. Der BuKaKo (KandesBunzler) muesste sich freuen, wenn wir nach Koeln (Verfassungsschutz) oder Pullach (BND) kommen, wie er sich gefreut hat, als DAS VOLK das Ministerium fuer Staatssicherheit (MfS) der DDR besichtigt hat!

Laut Datenschleuder (Zentralorgan des Chaos Computer Clubs), so ein Einwurf eines Mailboxbetreibers, behauptet der Bundespostminister (BPM): "Es geht bei G10 nur um privat betriebene Vermittlungseinrichtungen (nicht aber um Mailboxen)!"; das G10 sagt aber: "Alle Betreiber von Fernmeldeeinrichtungen!" BPM: "Es ist alles nicht durchschaubar." Gemessen am Gesetzestext ist das gelogen.

Die Vertreter des NF: "Private Anbieter von Telekommunikationsdiensten gab es nicht in der DDR." Nicht mal mehr eine privat initiierte Zeitung (wie die DS) waere moeglich gewesen! Ausrede fuer diese Restriktionen "Dann kann auch kein rechtsradikales Gedankengut verbreitet werden!" Funktamateure aber wurden zugelassen und schaerfstens beaeugt!

Ein Vergleich der Situationen in DDR und BRD zeigt:

BRD: Der Staat hechelt der technischen Entwicklung hinterher! Im Prinzip determiniert die Oekonomie die gesetzlichen Regelungsbeduerfnisse! Regierung schliesst Nischen (ist eine Nische etwas Unverzichtbares oder etwas, was schleunigst geschlossen gehoert?).
Historische Dimension: der Postdienst von Thurn und Taxis (16. Jh) wurde eingefuehrt, um revolutionaere Daten abzufangen!

DDR: Der Staat bestimmt, was sein darf und was nicht und legt damit die technische Entwicklung fest! Besuch des MfS hat andere Gruende und steht in einer voellig anderen historischen - naemlich revolutionaeren - Situation. Die Bedrohung war viel unmittelbarer als in der BRD; Wegen G10 waere auch in der DDR niemand zum MfS gegangen.

Der anwesende Prof. Dr. Klaus Brunnstein (im folgenden KB genannt): Am Beispiel Wackersdorf laesst sich das Primat der Oekonomie zeigen; dass die Industrie selbst merkt wann es sich nicht mehr lohnt!
NF: Ist kapitalistische Demokratie wirklich der Weg, um die Interessen des Volkes durchzusetzen? Aber eine andere Struktur (Sozialismus, d.S.) ist auf lange Sicht diskreditiert ("vermauert und verbaut")! Volksentscheid wird vom NF als Moeglichkeit der Einflussnahme auf Poltik angestrebt.

Am Runden Tisch wird z.Zt u.a. ueber ein Mediengesetz diskutiert.
Den Rundfunk oeffentlich-rechtlich zu organisieren ist ein Weg, gesellschaftliche Kontrolle auszuueben. Die die das Geld haben, werden bestimmen! Die breite Masse ist allerdings konsumorientiert!

Addy: Sichern heisst einschraenken! (Das ist zwar trivial, aber muss immer mal wieder gesagt werden, der Aetzer)

KB: Telefonnetz vergesellschaften! Computerisierung okkupieren!

NF: Kommunikationssystem wird geschaffen - aber fuer die Wirtschaft!

NF: Blauaeugige Basisdemokratie zerschlagen!

Pu(blikum): Leitungen werden unkontrolliert ueberwacht!
Pu: Idee des Counterparts, d.h. der "fortgeschrittenere" Partner macht nichts ohne Beteiligung des nicht so weit "Fortgeschrittenen"

KB: Zurueck zur Kommunikationsthematik, d.h. wir diskutieren hier ueber Verfuegung und Distribution von Informationen!
Technologiefolgenabschaetzung funktioniert nicht, Beispiele sind Volkszaehlung und ISDN

Ein uneingeschraenktes Fernmeldegeheimnis nach Art. 10 GG (d.h. ohne G10) ginge nicht, dann haetten wir die Alliierten noch in den Leitungen.

Noch den Bestimmungen der CoCom-Liste waere ein Datennetz nach vollem ISDN-Standard gar nicht in die DDR exportierbar. - Das kann eine Technologie-Folgeabschaetzung natuerlich nicht ersetzen.

PP musste stellenweise fuer die enormen Fehlleistungen seiner Genossen - vor allem auch als Regierungspartei - harte Angriffe hinnehmen, sein Eintreten fuer die Volkszaehlung mit dem Hinweis auf dringend benoetigte Daten z.B. zum Wohnraumbedarf stiess zunaechst auf schallendes Gelaechter und dann sofort auf scharfen Widerspruch: "Vor allem muessen Sie sich jetzt vorhalten lassen, mit diesem Datenschrott auch noch zu planen (KB)!

Die Themafrage "Was soll der Staat duerfen?" wurde exemplarisch am Beispiel des Umgangs des BMPT mit den im ISDN anfallenden Verbindungsdaten ("wer/wann/mit_wem/wielange") diskutiert. PP sah hier vor allem einen Zielkonflikt. Und zwar zwischen dem "Dienstleistungsangebot" in Form detaillierter und damit nachpruefbarer Abrechnungen, oder solchen Features wie selektive Anrufunterdrueckung, Identifikation des Anrufenden schon vor dem Abheben, Anrufweiterschaltung und aehnlichen Gimmicks einerseits und der dafuer ggf. hinzunehmenden Einschraenkung in Form von Ueberwachung, Speicherung. Aber die Frage, ob wir all diese Wohltaten in Form von vollautomatischen digitalen Dienstleistungen ueberhaupt wollen, ist ja gar nicht diskutiert worden. Die ISDN-Plaene hat nie ein demokratisch gewaehltes Parlament abgesegnet, das war eine reine Regierungsentscheidung.
Und das Interesse des BMPT an wasserdichten abrechenbaren Daten waere durchaus auch anders zu befriedigen, vor allem ohne Datenspeicherung mit der Moeglichkeit, diffizile und aussagekraeftige Verhaltensprofile zu erstellen. Hier sei nur an so sensible Zusammenhaenge wie telefonische Beratung (Aids, Drogen, Psycho...) erinnert. Der Vorschlag, hier koenne nur noch mit

Einzelfallregelungen jeweils ein Spezialriegel vorgeschoben werden, kann nicht ueberzeugen. Ein Rechtssystem, dass im Wesentlichen mit Einzel-regelungen arbeitet, kann nicht mehr verstanden werden und ist damit ein Un-Rechtssystem.

So muessen sich die verantwortlichen Stellen denn auch entgegenhalten lassen, mit der service-orientierte Argumentation nur Nebelkerzen zu werfen, um vom fundamentalen Misstrauen der Obrigkeit gegenueber den Menschen abzulenken.

Die falschen Entscheidungen (ISDN) fuer die naechsten 20-30 Jahre sind ohnehin schon jetzt nur sehr schwer zu korrigieren, ein solch komplexes System schreibt man nicht mal eben so auf die Schnelle um.

So fuehrt die Frage nach den Befugnissen des Staates schnell zur Frage nach dem Bewusstsein und der Verantwortung der Informatiker und Software-ingenieure. Hier sind die Aussichten gar nicht so finster, gerade Informatiker wissen oft eher als konventionelle Techniker, auf wessen Seite sie stehen. Das kann aber eine grundlegende politische Debatte nicht ersetzen. Ein klares, auch grundgesetzlich verankertes Prinzip der "Achtung der Privatdaten" koennte die vielen verwirrenden Einzelregelungen zum Datenschutz ersetzen und vor allem als deutliches Bekenntnis zum Recht des Individuums auf unerfasstes Denken und Leben Zeichen setzen.

Uli/Ludger ChaosHa(gen)

Uhu@GLOBAL.ZER, Ulrich@BOSKOPP.UUCP
GEDO@GLOBAL.ZER, GEDO@BOSKOPP.UUCP

[Contrib][Chalisti][04] Was soll der Staat duerfen ?

Europaeische Wissenschaftsnetze in den 90ern

Die wichtigsten Wissenschaftsnetze in Europa sollen ihren BenutzerInnenn in den Universitaeten und Forschung in den 90er Jahren schnellere internationale Verbindungen zwischen den lokalen Netzen bereitstellen. Das europaeische Ziel ist gleich, doch der Weg dazu geht ueber eine Schlacht um europaeische oder amerikanische Standards, Postmonopole oder Systeme von Computerherstellern. Offenen Systemen werden dabei mehr Chancen zugewiesen als herstellergebundenen Loesungen.

Zu den wichtigsten europaeischen Forschungsnetzen gehoeren das auf dem IBM-System basierende EARN (European Academic Research Network), das kooperative EUnet (European Unix Network), das Netz der Hochenergie-physikerInnen HEPnet (High Energy Physics), auf DEC-Technik, sowie die in RARE (Reseaux Associes pour la Recherche Europeenne) verbundenen X.400-Netze auf dem OSI-Standard (Open Systems Interconnection). Die SkandinavierInnen im NORDUnet (Nordic Network) unterstuetzen als Loesung fuer die Zukunft parallel schon verschiedene Protokolle.

Lokale Netze koennen in internationalen Netzen ueber verschiedene Protokolle verbunden werden: da ist zum einem das amerikanische Protokoll TCP/IP (Transmission Control Protocol/Internet Protocol), das in Deutschland in lokalen Netzen schon zu einem weithin benutzten und zunehmend beliebteren Industriestandard geworden ist.

Demgegenueber steht das X.400-Protokoll der geplanten europaeischen Wissenschaftsnetze, die aus der europaeischen Foederation von RARE, hervorgegangen sind. Die auf dem internationalen Standard OSI, Open Systems Interconnection basierende X.400-Dienste sollen ermoeglichen, zukuenftig nicht nur Text, sondern auch Graphiken und Ton zu verschicken. Gegenueber den amerikanischen TCP/IP-Protokollen koennte X.400 daher bedeutende Vorteile bringen.

Mit diesen Multimedia-Anwendungen koennten die europaeischen Regierungen den europaeischen Computerherstellern und Unternehmen den Vorsprung eines offenen Standards bieten. Der bedeutendste Nachteil der X.400-Dienste ist die Tatsache, dass benutzerfreundliche Anwendungen noch nicht verfuegbar sind.
Andererseits werden die Netze durch die Festlegung auf die X.25-Dienste der nationalen Postgesellschaften technisch eingeschraenkt und fuer zukuenftige Netz-Projekte eventuell zu langsam.

Einen Kompromiss zwischen europaeischem OSI und amerikanischem TCP/IP versuchen Netze wie EUnet, HEPnet und teilweise EARN zu gehen. Um ihren BenutzerInnen im Uebergang zu einem internationalen OSI-Netz die bestehenden Dienste ueber IP oder EARN zu ermoeglichen, sind diese Netze in der europaeischen Initiative RIPE (Reseau IP europeen) zusammengeschlossen.
Mit den Aktivitaeten, die US-Standards wie TCP/IP ausnutzen, stehen diese Netze jedoch ausserhalb europaeischer Foerderung. In juengster Zeit engagierten sich auch die X.400-Netze in RARE fuer die von WissenschaftlerInnen benoetigten IP-Anwendungen.

Auch das auf X.400 basierende DFN befindet sich in der schizophrenen Lage, trotz des Benutzerinteresses an IP-Diensten mit den Geldern vom BMFT nur auf OSI-Standards festgelegt zu sein.

Unter dem Druck der Universitaeten auf das DFN wurde eine Vereinbarung zwischen dem DFN und der Telecom getroffen. Diese stellt fuer die Universitaeten ein pauschaltarifiertes X.25 Netz zur Verfuegung. Dabei handelt es sich praktisch um das allzeit bekannte Datex-P Netz. Die einzigen Unterschiede bestehen in der veraenderten NUA-Adresse (45/44 050 xxxx xxxx), den Geschwindigkeiten (9,6KBps oder 64KBps), sowie der Abrechnung, die eben jetzt volumenunabhaengig geschieht. Dadurch koennen die Universitaeten laengerfristig planen und sind nicht so grossen Kostenschwankungen wie bei volumenabhaengigen Netzen unterworfen. Seit dem bekannt wurde, dass dieses WIN existieren wird, haben einzelne Rechenzentren auch schon Verhandlungen mit der GMD gefuehrt, um das EARN in Zukunft ueber das WIN laufen zu lassen und damit auch die Zukunft von EARN zu sichern. Den Betrieb des zentralen EARN-Rechners in Bonn wurde inzwischen auch zugesichert. Das WIN wird stellenweise auch als Uebertragungsmedium fuer UUCP, sowie Bundeslandnetzen (Bsp.: Niedersaechsischer Rechnerverbund NRV) genutzt werden.

Anschliessend konnten noch Fragen gestellt und diskutiert werden. Nachdem verschiedene Fragen zum EuNet, speziell zur Struktur von Unido gestellt wurden, wurde durch die Frage: "Wie siehst du das Verhaeltnis Unido-Subnet" eine interessante und stellenweise auch heftige Diskussion begonnen. Verschiedene anwesende Subnet-Benutzer und andere Anwesende diskutierten ueber den Sinn bzw. Unsinn von Subnet, Unido, Kostenstrukturen, Mailboxen am EuNet, etc.
Im Laufe der Diskussion wurden auch die Probleme der Moeglichkeiten von Studenten angesprochen, wie diese an den Universitaeten Netze benutzen koennen oder aber auch ueber Universitaeten sich vernetzen koennen. Nur an ganz wenigen Universitaeten koennen Studenten Netze wie EARN benutzen. Es wurde gemeinsam ueberlegt, wie man erreichen koennte, dass die Verantwortlichen in den Rechenzentren sich mehr mit den Gedanken anfreunden, Studenten auf dieses neue Medium zur Verfuegung zu stellen.

Anke Goos/Terra

[Contrib][Chalisti][04] Europaeische Wissenschaftsnetze in den 90ern

Computernetze im Umweltschutz: Die Nordsee faengt in Bayern an!

Wie koennen Computer und Datennetze fuer den Umweltschutz genutzt werden? Fuer die Internationale Nordsee-Schutzkonferenz (INK) im Maerz 1990 haben Umweltschutzverbaende auf dem Chaos Communication Congress einen Aktionsplan entworfen, wie die "alternativen Medien" der Computernetze zum Schutz der Nordsee eingesetzt werden koennen.

Auf der Nordsee-Schutzkonferenz in Den Haag treffen sich die Anrainer-staaten wie schon 1987, um gemeinsame Konzepte abzustimmen.

Den Umweltgruppen reichen die immer wiederkehrenden Absichtserklaerungen nicht aus. Sie fordern konkrete Massnahmen. Fundierte Informationen sollen auch die Nordsee-Verschmutzer im Binnenland zu umwelt-bewusstem Handeln ermutigen. Geplant ist, von einem der Begleitschiffe der Konferenz via Computernetz international Hintergrundberichte zu verbreiten. Damit soll das konventionelle Nachrichtenangebot bekannter Agenturen fachlich ergaenzt werden.

Zahlreiche Hintergrund- und Korrespondentenberichte, Features und aktuelle Meldungen werden von Bord des Aktionsschiffes mit dem Namen des friesischen Freiheitskaempfers Pidder Lyng auf die internationalen Datennetze ausgeschickt.

Von der Pidder Lyng werden die Nachrichten bis hin zu lokalen Mailboxen in der Bundesrepublik verteilt. Freie Journalisten, Umweltgruppen, Mailbox-Interessierte vor Ort koennen diese Infos aus dem lokalen Mailbox-System abrufen und auswerten.

Die konkrete Planung soll verschiedene Netze in die Informationsverteilung einzubeziehen:

GreenNet - Ein von Umwelt- und Friedensgruppen genutztes Netz, das zusammen mit Peacenet aus San Francisco weltweit Nachrichten, auch an Journalisten verbreitet.

EARN,EUnet - als europaeische Netze, sowie weltweite Netzwerke wie Bitnet, Internet und Bionet.

MBK1 - Eine Mailbox im Geonet, die als professioneller Anbieter auch ueber Tele(fa)x einen schnellen Nachrichtenaustausch gewaehr-leistet.

Zerberus - Auf dem Schiff wird eine Zerberus-Mailbox angeschlossen, die mehrmals taeglich die aktuellen Nachrichten mit den deutschen Zerberus-Boxen austauschen wird.

Btx - Nach Moeglichkeit sollen alle Berichte und Nachrichten kostenlos ueber Btx angeboten werden.

Darueber hinaus koennen gegen Kostenbeteiligung die Berichte direkt via Fax oder Telex gesendet werden.

Diese Aktion ist ein erster Versuch, die Staerke von menschlichen und technischen Netzen zu testen. Der Erfolg der Aktion haengt wesentlich davon ab, ob es gelingt, die Information aus den Netzen auf konventionelle

Medien wie Presse und Funk, aber auch oeffentliche schwarze Bretter in
Schulen und Universitaeten zu uebertragen.

Weitere Informationen erteilt:
Mensch-Umwelt-Technik e.V. (M.U.T.)
c/o Wolfgang Schroeder
Im Winkel 3
2000 Hamburg 20
Tel.: 040/464811 (14-18 Uhr)
E-Mail: MBK1:M.U.T.
MUT-EV@Umwelt.Zer

Sicherheit in offenen Netzen

Erster Teil frei nach Dr. Pfitzmann von der Uni Karlsruhe:
Mit der Einfuehrung der digitalen Netzwerke (ISDN) durch die Bundespost wird die Frage der Datensicherheit neu aufgeworfen. Mit ISDN werden mehrere analoge Systeme zu einem Digitalen zusammengefasst (Telefon, Fax, Datenuebertragung, Fernseher etc.) und damit zentralisiert. Fernseh- und Radiosendungen sollen nicht mehr verteilt werden, sondern unter der Endstufe von ISDN (Integriertes Breitband-Fernmeldenetz) auf Bedarf vermittelt werden. Eine Ueberwachung wird damit durch die technischen Gegebenheiten stark vereinfacht und auch erst moeglich. Dazu kommmt, dass eine Ausspaehung und/ oder Verfaelschung digitaler Daten kaum bemerkbar ist; daraus folgt, dass neben einem rechtlichen auch ein technischer Datenschutz unabdingbar ist.

Bei der Ausspaehung von Daten muessen zwei Arten der unkontrollierbaren Informationsgewinnung beruecksichtigt werden: Zum einen der illegale Zugriff von fremden Dritten auf die Leitungen, oder der 'legale' Zugriff offizieller Organe ueber die Verteilerzentralen.

Gegen das illegale Abhoeren von Leitungen kann man sich einfach schuetzen. Zum einen kann durch die in Zukunft haeufigere Verwendung von Glasfaserleitungen die Moeglichkeit des unbemerkten Anzapfens drastisch verringert werden, zum anderen ist durch die Verschluesselung aller ueber die Leitung transferierten Daten ein guter Datenschutz erreicht.

Das wirksamste Verfahren waere die sog. asymetrische Verschluesselung, bei dem eine Nachricht mit dem oeffentlichen Schluessel des Empfaengers codiert wird. Der Empfaenger entschluesselt die Nachricht mit dem nur ihm bekannten dazugehoerigen zweiten Teil des Schluessels (RSA-Verfahren). Bei Verwendung anderer Verschluesselungsverfahren ist dies technisch kein Problem, bis 800 kbit/sec auf Software-Basis, mit Spezial-Chips sogar 30 Mbit/sec (Prof Beth, Uni Karlsruhe, hat nach meinen Informationen Chips mit ueber 100 Mbit/sec entwickelt - genaue Infos bitte nachfragen direkt bei Beth bzw ASTA@DULRUU51.bitnet).

Zum Zweiten: Um die uebertragene Information vor den Vermittlern geheimzuhalten, ist eine unabhaegige End-to-End-Verschluesselung zusaetzlich zur Verschluesselung der Daten durch die oeffentlichen Dienste, die diese durchfuehren um die Leitungen zu schuetzen, noetig. Um vor den offiziellen Stellen Absender, Empfaenger sowie Kommunikationsbeziehungen geheim zu halten, stehen einige Moeglichkeiten zur Verfuegung. Eine zeitliche Entkopplung von Informationsauswahl und Nutzung, ein breites Empfangen von codierten Informationen und allgemeine Verteilung waeren Ansaetze, den Empfaenger zu schuetzen.

Zum Schutz des Absender koennten sog. MIXe errichtet werden, die mehrere Leitungen zusammenfuehren, und Informationen zeitlich versetzt ueber willkuerliche Ports wieder ausgeben. Kritisch wird dies nur bei Echtzeitvorgaengen, wie zum Beispiel dem Telefonieren. Diese technischen Moeglichkeiten koennen Spionage und Ausspaehung nicht vollkommen ausschliessen, allerdings wird das notwendige

Vertrauen in die Netzwerkbetreiber, in diesem Fall Post, auf ein Minimum reduziert, resp. man macht sich so von der Korrektheit der Post in einem grossen Mass unabhaengig.

Vielleicht noch ein kleiner Einwurf zur Sache Verschluesselung. Haeufig taucht das Argument auf, dass die Freigabe der Information wie man wirkungsvoll Daten verschluesselt und Datentransferwege verschleiert, von subversiven und kriminellen Organisationen ausgenuetzt werden koennte, ihre Aktivitaeten zu verbergen; und darum oeffentliche Freigabe all dieser Informationen gradezu straeflich sei! Dem kann man entgegenhalten, dass solche Organisatinen von alleine genuegend Phantasie aufbringen, sich dieses Wissen auf anderen Wegen anzueignen und auszunuetzen. Dies ist also absolut kein Argument schutzlose Buerger der Moeglichkeit des freien und unkontrollierten Datenaustauschens zu berauben.
Damit waere die eigenliche Informationsverteilung vortrefflich anonymisiert. Das Problem das jetzt noch offen ist, ist die zuverlaessige Indetifizierung des Absenders, bei gleichzeitiger Wahrung seiner Anonymitaet in anderen Bereichen.

Zweiter Teil frei nach E. Raubold (GMD) (Dies ist keine mit der Post auf irgend eine Art verknuepfte Organisation):
Zuerst wird das Problem der Identifizierung unabhanegig vom Problem der der Anonymitaet gegenueber anderer Stellen diskutiert.
Zwei Beispiele um zu zeigen dass diese Identifikation unbedingt notwendig ist, und ein in Zukunft sicher steigendes Problempotential aufweist.
Die Aufgabe von Bestellungen (mit z.B. Telefax) unter Vortaeuschung eine falschen Identitaet kann Firmen wenn doch nicht ruinieren, doch arg in Probleme treiben.
Versicherungsagenten arbeiten haeufig fuer mehrere Gesellschaften gleichzeitig, so koennen unabsichtliche oder absichtliche Vertauschungn auftreten, womit sich Private Vorteile ergattern koennten.

Der technische Aufwand, um eine absolute Sicherhiet der Verbindungen und der Software mit konventionellen Mitteln zu erreichen, ist unvertretbar hoch, verschiedenene Banken die Geldtransfers vornehmen verlangen jede fuer sich Sicheheitsstandards, die dann sogar untereinander in Konflikt komen koennen. Kompliziert wird es auch, wenn man dann solche 'vertraulichen' Daten in eigene Applikationen uebernehmen will. Ausserdem kann Sicherheit bei der Hardware in solchen Faellen auch nicht garantiert werden, da der Zugang zu dieser Hardware in den seltesten Faellen kontrolliert werden kann/will.
Um trojanische Pferde und andere Sicherheitsprobleme einfacher detektieren oder auch eliminieren zu koennen, wird eine Normung von Kommunikation (a la X.400) und Betriebssystem zwischen Rechnern verwandter und verschiedener Gesellschaften gefordert, um Luecken in Systemen leichter beseitigen zu koennen. Andere, 'radikalere' Stimmen forderten gar eine voellige Neugestaltung all dieser am Austausch kritischer Informationen beteiligten Systeme.

Waehrend der erste Teil des Gespraeches ein gestoertes Verhaeltnis zwischen Kunde und 'Hersteller' also der Post aufzeigte, stellte der zweite Teil Probleme der Benutzer untereinander dar. Dies in dem Sinne das im Moment keine Identifikation von Teilnehmern an einem Netz gewaehrleistet werden kann (X25, Telefax etc), Passwoerter nicht sicher sind, da 'Verraeter' die in Umlauf bringen koennen, und mitgeschriebene Logs verfaelschbar sind.

Das CCITT-Dokument X.509 hat hierzu einige gute Prinzipien zur Sache Personenidentifikation aufgezeigt. Es versucht folgende sechs Schwaechen im momentanen System (ohne Aenderung irgendwelcher Basisbedingungen (Leitungsicherheit, Verschluesselung etc))

aufzuzeigen und zu beheben.
a) Identitaet eines Anderen ablauschen.
b) Maskerade (so tun als ob man ein anderer waere)
c) Replay (antworten auf Briefe schicken, die man selber eigentlich
   gar nicht haben sollte, und so eine 'Legitimitaet' zu erschwindeln)
d) Daten zum eigenen Gebrauch abfangen
e) Waehrend der Sendung der Daten diese Verfaelschen
f) 'Repudiation' Das Verneinen des Erhalts einer Meldunge oder auch
   so tun als ob man eine Meldung erhalten haette, die die Gegenstelle
   aber nie abgeschickt hat.

Ein praktischer Ansatz um diese Probleme im Spezialfall Teletext wurde von der Firma mbp in Zusammenarbeit mit dem GMD entwickelt, und erlaubt es, eine elektronische Unterschrift an ofizielle oder vertragsbildende Texte zu binden, und gleichzeitig die Unverfaelschtheit dieser Texte zu gewaehrleisten.
Dies wird erreicht, indem jeder Benutzer dieses Systems einmal mit einer persoenlichen (Chip-)Karte ausgeruestet wird, auf der ein RSA-Schluessel gespeichert ist. Jedesmal, wenn dieser Benutzer nun eine Meldung absenden will, muss er in einen vor unbefugten Zugriffen gesicherten PC seine Karte einfuehren, und der Rechner ermittelt mit Hilfe dieser Karte und dem zu sendenden Text eine 'Signature' die diesem Text angefuegt wird. Die Empfangsseite kann so feststellen wer (welche Karte) die Verantwortlichkeit fuer diesen Text uebernimmt, und hat die Garantie, dass der Text waehrend der Uebertragung nicht von Dritten verfaelscht wurde.

Das System wird schon vereinzelt eingesetzt, und es laufen Anstrengungen aufzuzeigen, dass solche Signaturen durchaus rechtsgueltig sind, also solche Dokumnete vertraglichen Character haben. So wird zum Beispiel dieses System zwischen Gerichten und Klagestellern bei Mahnverfahren erprobt.
Natuerlich nuetzt diese Kontrollmethode nichts, wenn der Zugriff von Unbefugten zur Maschine die die Karten erstellt, sowie den Uebertragungseinheiten nicht verhindert werden kann.

Konflikte existieren zur Zeit noch, wenn man Anonymitaet + Autenthizitaet verknuepfen will. (Kreditkarte mit der ich so anonym wie mit Bargeld meinen Kaugummi kaufen will, ohne dass offizielle Stellen mich als KaugummiKaeufer eruieren koennen, aber das Geld trotzdem von meionem Konto abgezogen werden muss)

Anmerkungen:

Im Rahmen des DEC-Seminars "Datensicherheit in Forschungsnetzen" vom 25.11.89 in Sindelfingen lud Prof Beth vom E.I.S.S. (European Institut of Security Systems), Uni Karlsruhe, alle interessierten Studenten, egal welcher Fachrichtung und Uni, ein, sein Institut zu besuchen. Bitte vorher telefonisch anmelden. Die Tel-No. ist bei der Auskunft der Uni Karlsruhe zu erfragen.

Auf der 16.5 KIF (Konferenz der Informatikfachschaften) in Wien, Dezember 1988, wurde ein Workshop zum gleichen Thema abgehalten. Dort ging man noch detailierter (Entwicklung der (zur) Informationsgesellschaft, TEMEX etc) auf dieses Thema ein. Ein Papier dazu kann beim KIF-Verteiler angefragt werden: kif@unido.bitnet oder kif@unido.uucp

Literaturhinweise:
- Datenschutz+Datensicherung Telefon-MIXe A.Pfitzmann u.a.
  Uni Karlsruhe
- Datenschutz garantierende offene Kommunikationsnetze
  Informatik-Spektrum 1988 11:118-142
- Security in Data networks Eckard Raubold GMD Darmstadt

Alex/Gec/Fly/Framstag

[Contrib][Chalisti][04] Sicherheit in offenen Netzen

Straffreiheit bei Selbstanzeige - Sackgasse oder Chance?

Auf dem Podium sitzen:
- Staatsanwalt (StA) Giessler von der Staatsanwaltschaft Hamburg als Fachmann und Beteiligter
- Tanja als Fachfrau und juristischer Beistand des Moderators
- Juergen Wieckmann als Fachmann fuer Hackerethik (zeitweilig)
- und Padeluun als Moderator

Die Diskussion um die Frage, ob Selbstanzeige eine geeignete Perspektive fuer Hacker im Konflikt mit dem Strafgesetz seinkann, findet vor dem Hintergrund einer eindeutigen Rechtslage statt:

Paragraph 303a des Strafgesetzbuches (StGB) stellt bestimmte Formen des Hackens unter Strafe. Ob und wie hoch bestraft wird, bestimmen die folgenden Beteiligten in dieser Reihenfolge:

- der Daten-Inhaber (z.B. eine Firma), der Strafantrag stellen muss, bevor der StA in Aktion treten kann
- dann der StA, der Anklage erheben muss/kann, bevor der Richter aktiv wird
- der Richter, der entweder verurteilt oder nicht.

Der Hacker selbst hat darauf keinen Einfluss, schon gar nicht dadurch, dass er sich selbst den Strafverfolgungsbehoerden offenbart, mit der Hoffnung, dass er wegen Geringfuegigkeit nicht oder in nur schwachem Masse verurteilt wird.

Das haeufig - und hier auch wieder - angefuehrte Gegenbeispiel aus dem Bereich des Steuerrechts eigne sich, so Giessler, nicht zum Vergleich, weil es "rechtssystematisch" ganz anders einzuordnen sei. Da naemlich verzichte der Staat auf sein Recht zum bestrafen, weil es "um sein eigenes Geld", die Steuern naemlich, gehe, und nicht um Rechte Dritter, die er zu schuetzen verpflichtet ist.

Das Strafgesetz garantiert generell jedem gewisse Rechte. So z.B. Eigentum, Briefgeheimnis,etc. . Zu diesen schuetzenswerten Rechtsguetern gehoert u.a. auch das Recht auf einen Geheimbereich. Deshalb kann dies nicht mit dem Steuerrecht verglichen werden, wo bei Straffreiheit durch 'Selbstanzeige' nur der Staat selber betroffen ist, welcher natuerlich auf die Wahrung seiner Rechte verzichten kann, nicht aber einfach dritten Personen dieses Recht absprechen kann, ohne diesen die Chance zur Anklageerhebung zu geben.

Auf die Frage nach der tatsaechlichen Auswirkung der entsprechenden neuen Paragraphen (202a, 302a) gibt Giessler die Zahl der ihm bekannten Verfahren mit weniger als 10 an, davon allerdings keines wegen professionellen Hackens (Firma gegen Firma). Dem Einwand, dass ja im Prinzip nur mehr oder weniger "offene" Systeme gehackt werden, begegnet er mit der Erklaerung, dass auch schon der symbolische Schutz mit einem trivialen Passwort als "besondere Sicherung" der Daten gelte. Es komme darauf an, dass die Daten als besonders geschuetzt gekennzeichnet seien. Ausserdem haenge natuerlich auch das

Strafmass davon ab, wie ernsthaft die Daten geschuetzt worden waren.

Giessler appelliert an die Hacker, nicht auf alle Verletzlichkeiten staendig aufmerksam machen zu wollen. Auch der Mensch selbst sei ein System, dessen Verletzlichkeit sehr leicht demonstriert werden kann, aber nicht darf. Sei es nicht auch anmassend, als "Patron der Datennetze" zu entscheiden, was an die Oeffentlichkeit gezerrt gehoere?

Gegen die Forderung nach einem klaren Anspruch auf Straffreiheit bei Selbstanzeige verweist Giessler auf die Moeglichkeit der StA, bei ueberwiegendem oeffentlichen Interesse bzw. bei geringer Schuld das Verfahren einzustellen. Die Grenzen dafuer liegen allerdings da, wo der Rechtsfrieden empfindlich gestoert und der Kreis der Betroffenen groesser werde. Viel Presserummel schaffe auch viel oeffentliches Interesse. Er wirbt um Vertrauen in die Strafverfolgungsbehoerden, der Staatsanwalt sei kein Buettel irgendeines anonymen Gebildes ohne soziale Verantwortung. Damit provoziert er den entschiedenen Einwurf aus dem Publikum: "Das Vetrauen liegt deutlich im Minusbereich, auch ein netter Staatsanwalt aendert daran nichts!" Der Kritik am Umgang der Staatsanwaltschaft mit Betroffenen begegnet Giessler mit dem Eingestaendnis, dass die Qualitaet der Staatsanwaltschaft von den Menschen abhaenge, auch hier gebe es Flops und Spitzen. Spontaner Gegeneinwand: "Eine Institution muss sich auch daran messen lassen, welche Subjekte sie noch als in ihren Reihen tragbar empfindet!"

An dieser Stelle richtet Steffen das Augenmerk auf die soziale Katastrophe, die auch ohne Verurteilung schon der massive Einsatz der Strafverfolgungs-behoerden fuer den Betroffenen mit sich bringt. Da sollen Leute isoliert, weichgekocht, evtl. umgedreht werden, die eigentlich keine Kriminellen sind. Gerade bei cleveren Hacks sind die Mechanismen viel haerter als bei irgend-welcher Kleinkriminalitaet, weil noch ganz andere Instanzen mit drin haengen (Durchsuchungen, BND, Verfassungsschutz, auslaendische Dienste...). Auch bedauerte Giessler, dass Durchsuchungen angewendet werden muessten, doch seien sie zur Beweissicherung nicht zu vermeiden.

Er raeumt ein, dass eine solche "Heimsuchung" durch die Polizei vor allem fuer junge Leute sehr schlimm ist. Er weist aber auch darauf hin, dass ein Teil der Belastung von den Medien ausgehe, die grundsaetzlich ja nicht von der StA benachrichtigt wuerden. Er riet dem (jugendlichen) Hacker diesen Hack nicht an die grosse Glocke zu haengen, dies habe meist nur schlechte Aus-wirkungen fuer den Hacker selber (auch wenn dies fuer Jugendliche manchmal sehr schwer sei, Stichwort "Ich, der Supermann").

Mehr kann und wollte er mit Verweis auf laufende Verfahren (hallo Steffen) nicht sagen.

Wohin aber soll dann der bedraengte Hacker sich in seiner Not wenden? Spontane Antwort Giessler: "Nicht an die Staatsanwaltschaft - die ist dafuer nicht zustaendig!" Das Auditorium nimmt dieses Statement sehr lebhaft auf. Spaeter allerdings weist Giessler auch auf die Institution der Jugend-gerichtsbarkeit hin, in der von Jugendstaatsanwaelten und Jugendrichtern bisweilen regelrechte "Sozialarbeit" geleistet werde. Der Staat schuetze immerhin nicht grundsaetzlich nur Opfer, sondern ggf. auch den "schwachen Taeter" vor der Ueberreaktion eines "staerkeren Opfers". Dazu bemerkt Giessler, dass man bei dem Begriff Opfer immer vor Auge haben muesse, das dieser als juristischer Fachbegriff nicht negativ belastet sei wie sonst in der Oeffentlichkeit. Auch werde der Begriff Datenschutz oft in einem falschen Kontext benutzt. Es gehe letztendlich nicht um Daten die geschuetzt werden sollten, sondern um den Dateninhaber, der vor dem Missbrauch seiner Daten zu schuetzen sei.

Ausgehend vom Stichwort Strafantrag kommt der Vorschlag auf, mit den Betroffenen, deren Sicherheitsluecken ja zu deren Vorteil aufgedeckt werden, ein Einvernehmen zu suchen. Ohne Strafantrag keine Strafverfolgung! Diesem

Vorschlag stimmten alle Anwesenden mehr oder weniger zu. Er wurde sogar soweit gesponnen, dass man sich an Firmendachverbaende richten sollte, um eine Liste derjenigen Firmen zu erstellen, die das Angebot der 'freundlichen Hacker, die die Sicherheitsloecher finden wollen' annehmen und, unter Einhaltung bestimmter 'Regeln', hacken, Straffreiheit zusichern wuerden. Einflussnahme auf den Gesetzgeber mit dem Ziel, die geltende Rechtslage zu aendern, waere eine weitere Moeglichkeit, doch sei dieser Weg sehr langwierig und eine mehr oder minder theoretische Moeglichkeit...

In den drei Stunden der auf 90 Minuten angesetzten Veranstaltung gibt es deutliche Worte ueber entschiedene Standpunkte, am Schluss auch Applaus fuer alle Teilnehmer auf dem Podium.

Alex/Fly

[Contrib][Chalisti][04] Straffreiheit bei Selbstanzeige - Sackgasse oder Chance?

Capt. Crunch : Workshop Harper's Konferenz - Kurze Zusammenfassung

Am Donnerstag abend, sammelte sich eine kleine Gruppe, um den Inhalt der Harper's Konferenz zu diskutieren.

Die Harper-Konferenz wurde vom Harper Magazin in New York initiiert. Sie luden bekannte Amerikanische Hacker und Ehrengaeste ein, um ander Diskussion der Hackerethic teilzunehmen. Es war geplant diese Konferenz 10 Tage dauern zu lassen, und Harpers Magazin hatte dafuer zu sorgen, dass die Teilnehmer freien und bezahlten Zugang zum WELL-(Datenbank)-System erhielten. Nach einer kleinen anfaenglichen Konfusion eroeffnete ich das Treffen, und informierte die Teilnehmer von Harpers Plaenen die Texte dieser Konferenz in einem im April zu erscheinenden Artikel zu verwenden. Harpers Mag. hatte klargestellt, dass sie das Copyright besitzen wuerden, und ich gab dies so an die anderen Diskussionsteilnehmer weiter.

Ausserdem umriss ich kurz die Themen der Harpers Konferenz und beschrieb die Teilnehmer, und wer sie waren. Dann beschrieb ich kurz die unten aufge-fuehrten Themen:

Harpers Conference Topics

1) Einfuehrung - Eine kurze Liste der Teilnehmer und knappe Biographien. Nicht nur Hacker nahmen teil, sonder auch Regierungsvertreter und hochrangige Beamte. Sogar Clifford Stoll nahm daran teil.

2) Das Metaforum. Ein Ort, wo man ueber das Forum diskutieren kann. Dies ist der Ort, wo die Regeln des Forums diskutiert werden, Kritik und Vorschlaege angebracht werden.

3) Die Diskussion beginnt. Der wichtige Teil der Diskussion begann nun...

4) Die Ethik der Regierung. Hacken und Hacker aus der Sicht der Regierung. Alle Anwesenden stimmten darin ueberein, dass die Regierung eine schwammige Position einnimmt, und gewisse Unterorganisationen innerhalb der Regierung aeusserst unorganisiert sein koennen.

5) Von der Theorie des Hackens zur Praxis. Es fand eine Diskussion des Computersystems PROFS des weissen Hauses statt, und den beteiligten Hackern gelang es zu diesem System Zugang zu erhalten.
Dies als eine Demonstration der Hackerpraxis. Im wesentlichen waren die amerikanischen Hacker sehr arrogant, und schmissen die Mitbeteiligten raus.
Dann wurde das Recht Information zu erhalten diskutiert.

6) Hacker bei denen von Hackern gehackt wird. Eine Diskussion ueber die Realitaet eben dieses Vorgangs fand statt, und es wurden einzelne Beispiele aufgefuehrt. Die Diskussion wurde danach recht hitzig und flamig (persoenlich angreifend,kritisierend) . Die Hacker gingen ins TRW und zeigten, wie einfach es ist, private Informationen von Leuten zu erhalten. Dann wurde ein Mitschnitt dieses Vorgangs ins Konferenz-

system hochgeladen. Das endete in noch mehr Flames.

7) Was gibt's sonst noch zu hacken ? Diskussion uber zukuenftige zu hackende Systeme.

8) Das Manifest. Die Verfassung und die ersten Ergaenzungen wurden diskutiert.

9) Ein ungeschriebenes Manifest. Dies war der letzte Diskussionspunkt und war dazu gedacht, Themen die bis anhin noch nicht besprochen wurden noch in die Diskussion einzubinden.

10)Metaforum II. Wie haben wir's gemacht. Ein Diskussion ueber die Konferenz, und wie sie so ablief, ein Haufen Flames zu Harpers Entschluss, die Diskussionszeit zu kuerzen, und die Beschraenktheit der Konferenz.

11) Cyborg. Eine Diskussion zum AIDS information virus und seinen Effekten auf die Computerwelt.

Zusammenfassend habe ich die anderen ermutigt, die Konferenz us dem System downzuloaden und nach Belieben zu lesen, dann schlug ich vor, dass andere im Chaos Computer Club diese kommentieren sollten und eine Person zu bestimmen, die diese Kommentare und Schlussfolgerungen zusammenfassend schicken wuerde an:

unido!uunet!apple!well!crunch

2.Virenforum auf dem Chaos Communications Congress 1989

Eine Bestandsaufnahme auf der Grundlage des 1.Virenforums beim CCC 1985

Teinehmer an der Podiumsdiskussion:
Klaus Brunnstein
Ralf Burger
Wau Holland
ein sachkundiges Publikum
und als Moderator Juergen Wieckmann

DIE DISKUSSION
BURGER: Mittlerweile haben die Virenprogrammierer erstaunliche Ideen entwickelt, es wird immer Komplexer und besser programmiert. Die Quellen sind normalerweise nicht ausfindig zu machen. Zum AIDS-Virus: Viel Know-How, versteckte Dateien, Fallen fuer Utilities, Programm-Abbruch nicht moeglich. Grosse Wirkung mit wenig Aufwand.

BRUNNSTEIN: "Anomalien" (sprich Viren etc.) sind hilfreich beim Erkennen von Sicherheitsmaengeln. Bei mir wird nichts ueber Virenprogrammierung veroeffentlicht. Virenerkennung bei einem Programmcode von 170 Kbyte dauert etwa 3 bis 4 Wochen. International gibt es etwa 12 Zentren zur Virenbekaempfung. (Offensichtlich Amtlich, Unis oder Firmen,der Autor)
Ich erwarte eine drastische Steigerung sowohl an Qualitaet als auch an Quantitaet. Prognose: Bald 2000 (in Worten Zweitausend) verschiedene Viren. Etwa eine Infektion pro Anwender und Jahr wird erwartet.
WAU: Mittlerweile gibt es bei vielen Firmen die Ausrede << wir haben einen Virus >> statt unser Computer ist kaputt.

Akute Virengefahr gibt es im Moment hauptsaechlich fuer offene Systeme wie MS-DOS, bei denen Programme und Daten nicht durch eine vernuenftige hierarchische Struktur getrennt sind. Bei MS-DOS gibt es zu viele direkte Eingriffsmoeglichkeiten.

BURGER: Bereits seit 1985 gibt es bei mir die erste deutsche Virensammel-stelle, Service fuer Menschen, die Viren einschicken, ist kostenlos, es dauert bei neuen Viren 2 bis 3 Tage, dann hat der Anwender eine neue Version eines Virenscanners, die auch seinen Virus erkennt. Auf die Bemerkung Burgers, sein Programm erkenne jedes Virus, entgegnete Brunnstein er, Burger, sei ein Scharlatan und wuerde unwahre Dinge erzaehlen.
Die Geister scheiden sich vor allem bei dem Thema, ob man Virenprogramme - in welcher verstuemmelten Form auch immer - veroeffentlichen soll oder wie ausfuehrlich die Dokumentation sein soll. Der Vorwurf gipfelt in der Behauptung, mit Veroeffentlichung solcher Dokumentationen wuerde Burger Beihilfe zu Computersabotage nach Paragraph 303a StGB leisten.

WAU: Wer keine kuenstlichen biologischen Viren mag, koennte den Wissenschaftlern digitale Viren in die Computer setzen, damit die merken, was sie eigentlich anrichten.

BRUNNSTEIN: Computerviren sind keine Mittel zum politischen Kampf

(Volkszaehlungsboykott, Militaer etc.)

WAU: Es gibt auch nuetzliche Viren, zum Beispiel kann man damit ein Betriebssystem patchen, wenn man das System nur mit Disketten faehrt und das Update automatisch auf alle benutzten Disketten bringen will.

Sollte man wirklich Unterscheidungen zwischen guten und boesen Viren machen? Das Schlimme an den Dingern ist schliesslich, dass sie sich unkontrolliert vermehren und ausbreiten.

Ein Virenprogrammierer im Publikum erzaehlte, seine Firma haette ihn gezwungen, fuer eine Messeversion einer neuen Software einen Virus zu entwickeln, um unerlaubte Kopien zu verhindern. Er konnte es nicht mit seinem Gewissen vereinbaren, erzaehlte, er haette die Dateien versehentlich geloescht und leider kein Backup angelegt.
Kurz darauf habe er auch aus anderen Gruenden gekuendigt.

Brunnstein warnt vor den Gefahren, die Viren bei staendig steigender Anzahl von Steuerfunktionen im Haushalt anrichten koennen. Heute schon waere der PC nicht mehr Stand-Alone-Geraet, es gaebe Telefon, Modem, CD-Rom, demnaechst Stereoanlagen, Kuehlschraenke, Heizungssysteme etc., die daran haengen.
(Ist das wirklich die Utopie, die uns vorschwebt und ist sie auch technisch realistisch?)

Die Diskussion konzentrierte sich dann auf den ethischen Aspekt.
Schliesslich kann man auch mit anderen Mitteln Schaden anrichten, koerperliche Gewalt gegen andere ausueben, und trotzdem tun es die meisten nicht. Wir muessen dahin kommen, die Gesellschaft so umzuformen, dass niemand mehr noetig hat, so zu reagieren. Bislang sind im militaerischen Bereich sicher schon Viren entwickelt worden, die als Kriegswaffen Verwendung finden sollen. Logistik beim Militaer ist nicht mehr ohne Computerhilfe denkbar. Dabei ist unerheblich, ob das in Ost oder West passiert, eher wohl auf beiden Seiten.

Zusammenfassung von BURGER: Die Art von Viren ist egal. Zur Klassifizierung ist nur etwa 1 Std. noetig. Man muss sicherstellen, dass die Programe sich nicht veraendern koennen. Dafuer gibt es mittlerweile Hardware- und Softwareloesungen.

WAU: Systeme werden immer komplexer und unueberschaubarer. Doch die Komplexitaet als Alibi fuer Hilflosigkeit ist nur eine Ausrede aus Bequemlichkeit. Es gipt auch in komplexen Systemen immer Teile, die relativ einfach sind, und an diesen Stellen kann man ansetzen.

SCHLUSSWORTE:
BRUNNSTEIN: Herkoemmliche Computer auf der Basis vonNeumann'scher Maschinen Haben prinzipbedingte Schwaechen, die durch die Theorie ihres Aufbaus determiniert sind. Groessere Sicherheit ist mit diesem Konzept nicht vereinbar. Andere Maschinen haben moeglicherweise andere Schwaechen.
BURGER: Wir geben an uns geschickte Viren nicht weiter, auch nicht an kompetente Personen. Die Virenzahl wird weiter zunehmen, Ausblicke fuer die Software: 1 Program fuer eine Anwendung und individuell angefertigt, dann gibt es fuer Viren keine Chancen mehr. Das Softwareengineering wird sich weiter entwickeln, aber es wird ein Wettlauf sein zwischen Virenentwicklern und Virenjaegern. (Ende offen?)
WAU: Es gibt eine Art hippokratischen Eid fuer Programmierer und fuer Menschen ueberhaupt. Viren sind eine Erfindung. Ob sie auch eine Soziale erfindung sind? Immerhin haben sie die Menschen zum Nachdenken ueber ihren Umgang mit Technik gebracht.
JueWi: Noch etwas zum Nachdenken - Veroeffentlichen von Viren im Sourcecode oder Dokumentationen dazu beruehrt auch eine Machtfrage. Hat dann nur eine Elite Zugang zu Informationen?(=Macht)
Die Menschen stehen vor einem Dilemma: Freie Informationen fuer alle, aber darf man wirklich alles veroeffentlichen ohne Ruecksicht auf eventuelle

Folgen?

In aller Eile zusammengestellt mit Dank auch an das Publikum, dessen Kommentare und Meinungen ich hier mit verwendet habe von

Michael(ChaosHA) mk@boskopp.uucp

Cracker, Jaeger und Sucher

Software und Information - Copyright oder oeffentliches Gut

"Copyright ist aberglaeubische Kulturfeindlichkeit". Mit diesem Statement begann die Diskussion zum Thema Copyright mit Prof. Frank (Uni Paderborn), Guenter Freiherr von Gravenreuth (Anwalt, bekannt aus Funk und Cracker-intros), sowie Rainer Zufall (ein Cracker).

Mit obigem Satz provozierte Prof. Frank. Schon nach den ersten Erklaerungen waren die wenigen Leuten im Theater wach. Um diesen Satz naeher zu erklaeren holte er aus. Software ist keine Ware. Der Name Software - also weiche Ware - ist an sich schon falsch. Deswegen benutzte er von da an auch nur noch den Begriff "Soft". Seiner Meinung nach ist Soft Information, die frei verbreitet werden sollte. Soft ist ein geistiges Produkt, wie ein Bild, ein Musikstueck, etc auch. Dieses ist damit auch ein Bestandteil der Kultur. Wenn man nun einen "Kopierer" kriminalisiert, weil dieses eine Arbeitsbeschaffungs-massnahme fuer Anwaelte ist (Blick zu Gravenreuth), es aber keine Begruendung fuer die Kriminalisierung der Kopierer gibt. Aehnlich wie im Mittelalter, wo Hexen verbrannt wurden, weil es einen Aberglauben aber keine Begruendung fuer die Verbrennung gab. Aehnlich wie die Verfolgung von Hexen, findet auf die "Informationsverbreiter" eine Raubkopiererjagd statt. Soft als Kultur heisst aber auch, dass jedes Kopieren von Daten eine Sicherung von Kulturgut ist. Man stelle sich vor, was waere, wenn um Mittelalter die Moenche die Bibel nicht abgeschrieben haetten. Es ist eine reine moralische oder ethische Vorstellung, dass es "kriminell" sein muss, Programme, Informationen - egal, ob auf Diskette, Papier oder anderen Formen - zu kopieren. Es waere irgendwie falsch zu meinen, das ein Programm nur in einen Kopf entsteht. Es ist die Summe von Wissen von anderen Menschen, Nutzung fremder Software und aeusseren Anregungen. Deswegen sieht Prof. Frank ein Programm als allg. Gut an und verwenden dort den Begriff des "Informationskommunismus". Dieser Begriff hat er auf einer Tagung in San Marino zuerst verwendet, was aller-dings einige Stimmen aus dem Reformlaendern des Ostblockes gestoert hat. Daher verwendet er nun den Begriff des Informationskulturismus. Die Software als Ware, als Sache mit Substanz ist ein Gespenst. Man kann sich die Dienst-leistung bezahlen lassen, nicht aber das Programm an sich.

Gravenreuth sieht sich deswegen dann als "Ghostbuster". Erstmal stellt er klar, dass Software-Diebstahl kein Diebstahl ist, da dafuer praktisch der Diskettendiebstahl noetig ist. Viel mehr sagt er schon nicht mehr, sondern fragt ganz einfach: "Wovon soll der Programmierer leben ?". Der Anwalt ist ja im Zweifelsfall derjenige, der dem Programmierer zu seinem "Recht" verhilft.

Rainer Zufall meinte erstmal, dass Cracker von vielen Softwarefirmen ausge-nutzt werden. Sie bekommen nur kleine Betraege, der Hauptgewinn geht an die Verlage. Im Endeffekt ist es in der Regel fuer die Programmier besser, Ihre Software als Shareware zu vertreiben. Beim Crackertreffen, welches auch waehrend des Congresses stattfand, war dort so ein Fall. Ein Programmierer hat fuer die Firma Omnikron einen Assembler geschrieben. Allerdings gab es diverse Probleme mit der Zahlung, deswegen hat der Programmierer den Vertrag gekuendigt. Jetzt vertreibt er den Assembler (nun heisst er Turbo-Ass) als Shareware. Wer eine Doku und eine Registration fuer Update haben moechte, sollte 50 DM ueberweisen. Der Turbo-Ass kann weitergegeben werden. Inzwischen hat er schon fast mehr Geld bekommen, als ueber den Vertrieb. Natuerlich kann ein Programmierer nur gute bzw. sehr gute Software ueber

Shareware vertreiben. Fuer schlechte Sofware wuerde kein Geld bezahlt werden. Das ist sicher auch ein Vorteil, den schlechte Software gibt es ja genug.

Natuerlich darf man nicht vergessen, dass Software nur eine Form von Daten sind. In allgemeinerer Natur sind das ja auch nur Informationen, wie z.B. Sportnachrichten. Gerade wg. diesen hat ja das Bundesverfassungsgericht (das ist nicht zum Essen) eine Entscheidung gefaellt, dass jeder Buerger das Recht auf eine informelle Grundversorgung besitzt. Damit muessen die privaten Fernsehanstalten zulassen, dass die oeffentlich-schrecklichen Sender eine gewissen Minutenzahl an Filmauschnitten aus Sportbegegnungen unentgeltlich erlauben.

Auf jeden Fall scheint das Urheberrecht ueberarbeitungswuerdig zu sein. Im Grunde ist dieses Recht ueber 100 Jahre alt und wurde nur immer wieder an neue Gegebenheiten (Neue Medien, etc) angepasst. Aber ein "anpassen" genuegt nicht mehr. Prof. Frank gab den Programmierern noch den Rat ihre Soft eben als "Public Domain", "Shareware", etc zu vertreiben um damit immer mehr Tatsachen dahingehend zu schaffen, dass das Urheberrecht praktisch in seiner heutigen Form sinnlos wird.

Terra

[Contrib][Chalisti][04] Cracker, Jaeger und Sucher

!K U R Z B E R I C H T E !

1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1

Hagbard

Wer war Karl Koch ? Als Hacker, als Medienzielscheibe, als Mensch.
Fuer einen Antrag auf einen Therapieplatz hat Karl einen Lebenslauf geschrieben, der vorgetragen wurde. Er schildert sein Leben als Abfolge von Katastrophen.

Presseberichte: Jagd oder Berichterstattung ?

Waehrend sich die Presse frueher darauf beschraenkte, ueber die Technik-faszination der Hacker zu berichten, wurden waehrend der Berichterstattung die Hacker diesmal als Kriminelle, Spione oder gar Terroristen bezeichnet. Hagbard wurde als neue Super-Story benutzt. Ihm wurde Geld versprochen - oder auch nicht -, man nannte seinen richtigen Namen in Zeitschriften und vergass den Menschen. Nur wenig objektive Berichterstattung der haeufig genannten 4.Gewalt eines Landes.

Karl beim VS. Auf Anraten von Freunden zum Verfassungsschutz gegangen, dort sich vielleicht alles von der Seele geredet - in der Hoffnung auf ein besseres Leben. Eine Situation die neu fuer einen Menschen ist. Was kann er sagen, was nicht. Wo ist die Grenze - wo schweigt man. Man steht allein.

Aber war Karl nur Opfer ?
In der Diskussion wurde die Problematik der Drogen angesprochen. Es artete fast in einer Grundsatzdiskussion aus. Weiche Drogen zulassen ? War Karl immer Karl ?

War Karl ein Hacker oder ein Krimineller ?
Er hat gegen die Hacker-Ethik verstossen, er kann deswegen nicht als Hacker bezeichnet werden. Aber deswegen Aussperren ? War es damals richtig, dass Wau bei einem Interview im Beisein Karl's davon sprach: "Mit diesen Leuten - Kommunikationsabbruch". Welche Schuld trifft die Freunde ?

Der VS hat Karl gedraengt den Kontakt zu seinen Freunden abzubrechen. Dieser sei fuer ihn schaedlich. Vielleicht stimmte das. Vielleicht aber auch nicht. Echte Freunde sind ein Halt, wenn ein Mensch sich in einer ausweglosen Situation sieht.

Die Geheimdienste spielen seit Jahrhunderte das Spielchen der Beeinflussung, der Munkelei und des Versteckens. Wer sich mit diesen Stellen einlaesst, kann nur verlieren.

Zurueck zur Hacker-Ethik. Ein wichtiger Punkt in der Diskussion.
Prof. Brunnstein bemerkte, dass dies die erste wirkliche Bewaehrungsprobe der Hacker-Ethik war und das sich die Hacker-Ethik im Ernstfall als kein Schutz fuer die Gemeinschaft gelten kann. Dabei wird natuerlich vergessen, dass das Funktionieren der Hacker-Ethik zur Folge hat, dass die Oeffentlich-keit - also auch der CCC, das BKA oder sonstwer - von dieses "Hacks" nix mitbekommt. Die gehen ja nicht an die Oeffentlichkeit die Hacks werden zwischen "vernueftigen" Operatoren und den Hackern selbst geklaert.

Terra

2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2

Feminines Computerhandling
- Die etwas andere Wahrnehmung - ein Realitaetsabgleich -

Etwa 45 Leute, darunter auch ca. 30 Maenner, fanden sich zu diesem Workshop zusammen. Leider hatten die eingeladenen Frauen von der GI (Gesellschaft fuer Informatik) kurzfristig ihre Zusage zurueckgezogen.

Ohne Einfuehrungsreferat ging es deshalb sofort ans Eingemachte:
Wie kommen Frauen zum Computer, was machen sie damit, wie machen sie's, und vor allem: ist das anders als bei Maennern?

In allen angesprochenen Bereichen wurden z.T. erhebliche Unterschiede festgestellt:

Da waren z.B. Gruende fuer die Anschaffung eines Computers, der vorwiegende Einsatz, das Erlernen der Anwendungen, Zeit- und Energieaufwand fuer die Computernutzung, der Sinn fuer Spiele und vor allem fuer welche(!), Zielsetzung und Vorgehensweise beim Programmieren, Umgang mit Fachwissen und -sprache uvam.

Der Erfahrungsaustausch zeigte, dass Frauen einen Computer vorwiegend aus praktisch-rationalen Gruenden, also als Arbeitsmittel anschaffen und dann wirklich auch so verwenden. Maenner greifen hierbei eher zu irrationalen Argumenten (Verwaltung der Videocassettensammlung, "ich will programmieren" u.ae.), tatsaechlich aber verbringen sie sehr viel mehr Zeit mit den spielerischen Moeglichkeiten der Maschine.

Ein Exkurs dreht dann zunaechst darum, wie sich schon in der Schule unterschiedliche Herangehensweisen abzeichnen. Trotzdem scheint hier die Kluft noch laengst nicht so deutlich zu sein wie spaeter, nur etwa doppelt soviel Jungen wie Maedchen wuenschen sich einen Computer. An den Unis sieht das in den Informatik-Studiengaengen schon ganz anders aus.

Es zeichnet sich ab, dass vor allem die Art der Maenner, die Beschaeftigung mit den Computern oft mit einem gewissen Feature-Fetischismus ("hoeher, schneller, weiter") zu betreiben, Frauen wenig sympatisch ist und Zugaenge da unnoetig erschwert, wo Computer-Bereiche schon von Maennern besetzt sind. Dies bezieht sich sowohl auf die Art, wie und warum Maenner miteinander und mit Kolleginnen ueber Rechner reden als auch auf die offiziellen Dokumentationen und Handbuecher. Auch der CCC und der Congress sind davon wohl nicht auszunehmen.

"Solange nicht auch voellig unfaehige Frauen in hoechsten Positionen sind, ist die Gleichberechtigung nicht erreicht."
(Ilona Staller/La Cicciolina)

Weitere Informationen erteilt:
Rena Tangens
Art d'Ameublement
Marktstr.18
D-4800 Bielefeld 1
0521-6 11 93
E-mail: RENA@BIONIC.ZER
MBK1:PADELUUN

Rena\Uschi\Ludger\Ulli

3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3-3

Antifa-Workshop (Mi., 17.00)

Initiator: Rowue (E-Mail: rowue@smoke.uucp und rowue@chaos-hh.zer)

Hintergrund dieser Arbeitsgruppe bildet die bundesweit festgestellte Aversion verschiedener Antifa-Gruppierungen gegen den Umgang mit Computer(netze)n. Die versammelten 12-15(?) TeilnehmerInnen machten die unterschiedlichen Arbeitsformen der Antifa-Gruppen transparent: Politische Arbeit auf der Straae versus politische Arbeit im Netz.

Beispielgebend wurde von der - inzwischen aufgeloesten - Wiesbadener Antifa berichtet, die starke Beruehrungsaengste formulierte. Auch die Antifa Braunschweig lehnt diesen Bereich der politischen Arbeit "grundsaetzlich ab" (Edel). Kontakte, so ein Mailbox-Teilnehmer,bestuenden bisher nur zu Hamburg (Rowue) und zu einer Berliner Antifa-Gruppe. Bemerkenswert erschien auch die bisherige Zurueckhaltung der verschiedenen "Asten" in der BRD. Da in vielen Boxen bereits Antifa-Infos gesammelt werden, sollten die daran beteiligten Mailboxuser Kontakt mit Antifa-Gruppen in ihrer Umgebung aufnehmen, um so Datenaustausch anzuregen.

Da die Antifa-Gruppen ohne das Angebot von Inhalten das "nackte" Angebot eines Antifa-Netzes wohl nicht nutzen werden, wurde die konkrete Ausarbeitung eines Konzepts (Welche Daten sollen ausgetauscht werden?) gefordert, an der sich auch moeglichst alle Antifa-Gruppen beteiligen sollten. Ziel des Netzes soll u. a. sein, einen Gegenpol gegen faschistoide Teilnehmer und evtl. Gruppen in der E-Mail-Szene zu bilden (->Naziware...), Aktionen und Aktivitaeten von 'Faschos' im Vorfeld ihrer Planungen vorherzusehen und nach Moeglichkeit z.B. Gegenveranstaltungen zu organisieren. Allgemein koennten durch ein solches Netz Kontakte faschistoider Personen und Grupp(ierung)en untereinander aufgedeckt werden.

Dazu besteht ueber Mailboxen die Moeglichkeit, Daten verschluesselt auszutauschen. Au□erdem lassen sich Kommunikationsstrukturen erheblich schwerer rekonstruieren als bei Informationsaustausch ueber Telefon (voice). Dabei sollte noch ein Weg gefunden werden, um die Gefahr von Falschinformationen zu vermindern.

Es wurde von einigen TeilnehmerInnen angeregt, die verschiedenen Mailboxen anzuschreiben, um die Einrichtung eines speziellen Brettes bzw. Verteilers "Antifa" und Kontaktaufnahme mit lokalen Antifa-Gruppen anzuregen.

KONTAKTE: Rowue (s. o.).
Ein Pseudo-User (Verteiler fuer Mails) ANTIFA an der SMOKE.UUCP existiert bereits und soll demnaechst auch in Berlin und Dortmund eingerichtet werden, Auch LINKSYS (am Z-Netz) sammelt bereits Antifa-Daten.

89-12-27, 22.01 Ingo, Juergen

4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4-4

Cyberspace-Praesentation auf dem Hackerkongress

Cyberspace - darunter versteht man einen kuenstlich geschaffenen Raum, der aus den Vorstellungswelten der Cybernauten entsteht. Der Ansatz des Cyberspace geht auf den Science-Fiction-Roman "Neuromancer" von William Gibson zurueck: Dort wird eine Weiterentwicklung der herkoemmlichen Mailbox-Systeme beschreiben, indem die Hacker der Zukunft ("Cyberpunks") sich ueber ein "Simstim"-Geraet eine direkte Verbindung ihrer optischen und sinnlichen Wahrnehmung mit der "Matrix" verschaffen, einem darauf aufgebauten Datennetzwerk. Die Bewegung in der Matrix geschieht ebenfalls ueber reine Gedankensteuerung, indem das Simstim-Geraet die Gehirnimpulse direkt ueber Elektroden ausliest.

Mike Weber und Bernd v. den Brincken aus Koeln arbeiten an einer konkreten Realisierung dieser Vision. Dabei werden EEG-Signale (Gehirnstroeme) ueber einen Verstaerker und AD-Wandler in einen PC eingelesen und in Signale fuer einen Grafik-Rechner (Amiga) umgewandelt. Diese Grafik fuehrt nun im Sehzentrum der Versuchsperson zu einer Rueckkopplung, sodass sie lernen kann, die EEG-Stroeme bewusst zu steuern. In einer naechsten Phase des Projekts koennen mehrere Personen per Datenfernuebertragung ueber ein Mailbox-System verbunden werden.

Auf dem CCC-Kongress werden neben einem Vortrag auch Workshops zu zwei Bereichen des Projekts angeboten:

1 - Aufnahme, Verstaerkung und Verarbeitung der EEG-Signale, wobei Detailfragen wie Elektrodenanschluss, Verstaerkertechnik und Auswertungs-Software behandelt werden.

2 - Um eine moeglichst weite Verbreitung bei maximaler Kompatibilitaet der Anwender sicherzustellen, muss ein Standard einerseits fuer die Uebertragung der Grafik-Daten und andererseits fuer die logische Struktur des grafischen Raumes geschaffen werden.

Kontakt:
ArtCor c/o Bernd v. den Brincken, Rheingasse 13, 5000 Koeln 1,
Tel. 0221-241705

5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5-5

UNIX - WORKSHOP I + II

Im ersten Workshop (:-)) wurden die Grundlagen von UNIX beschrieben, wie sie u.a. in der Chalisti 2 nachzulesen sind.

Im zweiten Teil wurde tiefer in UNIX eingestiegen. Was davon an dieser Stelle von Interesse sein koennte waere eine kurze Aufzaehlung der IPC (Interprozess Kommunikation) Moeglichkeiten unter UNIX.

1.) Shared Memory: schnell, aufwendig, nur bedingt portabel
    (Hier greifen zwei Prozesse auf einen gemeinsamen Speicherbereich zu)
2.) Pipes: schnell, einfach, portabel, aber nur zwischen Vater und Sohn Prozess. (Temporaeres Austauschmedium mit dem Verhalten einer Datei). Praktisch handelt es sich um einen Informationskanal
3.) Named Pipes (FIFO): mittel schnell, Behandlung wie Dateien, einfach verstaendlich, halb portabel, aber jeder Prozess darf mit jedem Prozess kommunizieren, schreibzugriffe sind Atomar (Dateien werden geLockt), Nachrichtengrenzen bleiben nicht erhalten, d.h. man muss selber fuer die Trennung der einzelnen Nachrichten sorgen (ein Datenstrom).
4.) messages (auch message queues): nur im System V, langsam, puffer (von ca. 4k, impl. abhaengig), schreibzugriffe auch hier atomar, hierbei werden die Nachrichtengrenzen erhalten.
5.) sockets (engl. fuer Steckdose): nur in BSD UNIX (aber auch verschiedene Impl. fuer andere *NIXe, so z.B. XENIX), schnell, universell, TCP/IP beruht auf diesen, INTERNET benutzt diese

Ansonsten sei verwiesen auf folgende Buecher zu UNIX, etc.
Tanenbaum, Operating systems Prentice Hall
Gulbins, Unis System V Rel. 3

Fly/Gec

6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6-6

Captain Crunch mit dem Picturephone

Ich gehoere zu den Menschen, die bisher noch keine Vorfuehrung von John Draper alias Captain Crunch gesehen haben. Ich war also recht gespannt und der Titel "How Do Hackers Behave in Natural Diseases" klang sehr viel-versprechend. Mit der ueblichen chaosmaessigen Verspaetung begann dann auch der Workshop. Captain Crunch gab zunaechst eine kurze Einfuehrung und liess sich dann mit den Konferenzteilnehmern in den USA verbinden. Das war eine recht interessante Prozedur, denn erst muss jeder Teilnehmer den AT&T-Operator anrufen, der dann die einzelnen Anrufer zusammenschaltet. Die Konferenz selbst war ebenfalls anregend, denn ausser den Bildern gab es Berichte ueber das letzte Erdbeben in San Franzisco. Zwischendurch fand bei den Bilduebertragungen ein kurzer Countdown statt, um der Gegenstelle anzuzeigen, jetzt kommt das Bild. Dabei ging es nicht um eine technische Notwendigkeit, schuld war nur das Human Interface. Wenn der Geraeuschpegel waehrend der Bilduebertragung zu hoch ist, werden die Daten nicht empfangen. Meistens ging der Transfer ohne Schwierigkeiten zustatten, und als Lohn fuer die Ruhe gabs dann Bilder von T-Shirts (The Great Quake - I Survived), San Franzisco direkt nach dem Beben und Portraits der Konferenzteilnehmer. Leider wurde nichts aus dem interaktiven Frage- und Antwortspiel, die Veranstaltung musste wegen Zeitueberschreitung abgebrochen werden. Sehr stoerend fand ich das Verhalten der Leute, die staendig rein- und rausrannten, obwohl vorher und auf der Tuer darauf hingewiesen wurde. Trotz Chaos ist sowas fuer den Arsch. Alles in allem fand ichs trotzdem gut, es war neu und die Amis hatten eine Menge zu erzaehlen, ohne dabei rumzu-stottern. Wer Telefonkonferenzen in den USA ausprobieren moechte, kann eine 976-Nummer anrufen. WARNUNG! Das CHAOSpressecenter warnt vor unueberlegten Anrufen in die USA bei Nutzung des eigenen Telefonanschlusses.
(Ich hack jedem die Finger ab, der meinen nimmt).

Michael(ChaosHA)
EMail:MK@Boskopp.UUCP oder Michael_Kube@GLOBAL.ZER

[Contrib][Chalisti][04] !KURZBERICHTE!

IMPRESSUM

"Die gesamte Menschheit bleibt aufgefordert, in freier Selbstbestimmung
die Einheit und Freiheit des globalen Dorfes zu vollenden."

Herausgeber: Chaos Computer Club e.V./Redaktion Chalisti

V.i.S.d.P. : F.Simon

Redaktion: Volker Eggeling, Frank Simon

Mitwirkende an dieser Ausgabe:
Anke, ChaosHagen, Chaos-Luebeck, Framstag, Gec
und andere Chaos-Engel

Redaktionen: Chalisti, c/o Frank Simon, Kennedystr. 12,
2900 Oldenburg, Tel. 0441/592607
Datenschleuder, Lachswehrallee 31, 2400 Luebeck,
Tel. 0451/865571
MIK-Magazin, c/o J. Wieckmann, Barmbeker Str.22,
2000 HH 60, Tel. 040/275186

Verbreitung: Zerberus : /Z-NETZ/CHALISTI
UUCP(dnet) : dnet.general
UUCP(sub) : sub.org.ccc
EARN/CREN : CHAMAS@DOLUNI1, Brett chamas.chalisti
GeoNet : mbk1: brett ccc-presse
FidoNet : ccc.ger
MagicNet : Artikel&News

Adressen: EARN/CREN : 151133@DOLUNI1
UUCP : eggeling@uniol (eunet)
terra@olis (subnet)
Zerberus : chalisti-redaktion@mafia
GeoNet : mbk1: chaos-team
FidoNet : Volkmar Wieners on 2:241/2.1205
MagicNet : trendbox:gec
AmNET II : HENNE;SML

Teilnehmer aus diversen anderen Netzen wie z.B. ArpaNet,
DFN, etc. nutzen bitte die Bitnet Adresse ueber das
entsprechende Gateway.