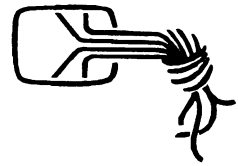
Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende

Ein Organ des Chaos Computer Club



ISSN 0930-1054
DM 3,50
#38 März 1992
Streifbandzeitung C11301F

This page is intentionaly left blank.

IMPRESSUM

Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende

Adresse: *Die Datenschleuder, Schwenckestraße 85, D-W 2000 Hamburg 20*

Telefon: *(040) 490 37 57*

Telefax: *(040) 491 76 89,*

Mailbox: *DS-RED@CHAOS-HH.ZER (040-491 10 85, 1200/2400 8n1)*

Internet/UUCP: *ds-red@cchh.hanse.de*

BTX: **CHAOS#*

Redaktion: *andy, cash, rowue, steffen, wau, terra, ron, hacko, nomade*

V.i.s.d.P.: *Heye Fulda*

Herausgeber: *Chaos Computer Club e.V., Adresse wie Red.*

Adreßänderungen: *bitte ABOMV@CHAOS-HH.ZER mit alter und neuer Anschrift mitteilen*

Druck: *Druckerei in St.Pauli, Große Freiheit 70, D-W 2000 Hamburg, auf chlorfreiem Papier*

Namentlich gekennzeichnete Artikel geben nicht unbedingt die Meinung der (Gesamt-) Redaktion wieder.

Einzelpreis 1,00 DM. Abonnement für 8 Ausgaben 60 DM, Sozialabonnement 30 DM. Mitglieder des Chaos Computer Club e.V. erhalten die Datenschleuder im Rahmen ihrer Mitgliedschaft.

Editorial

Nachdem wir jetzt bereits 23mal Editorialentwürfe verworfen haben und immer noch zu keinem Gescheiten Ergebnis gekommen sind geben wir es hiermit auf, vervollständigen mit dieser Erklärung unsere Satzfahnen und gehen zu Bett, damit wir es morgen früh rechtzeitig schaffen selbige zur Drukkerei zu bringen...

Und also schließen wir mit einem freien Zitat aus einem bekannten Buch, frei nach Gedächnis: Das Fliegen ist eine Kunst oder vielmehr ein Trick. Der Trick besteht darin, sich auf den Boden zu schmeißen, aber daneben und die Kunst darin, sich nichts draus zu machen, wenn es beim ersten Mal nicht klappt. Such Dir also einen schönen Tag aus und probiers... Wer jetzt noch nicht gemerkt hat, daß wir nichts zu sagen haben, tja, der (und alle anderen) waren hoffendlich auf dem Congress, welcher wohl den größten Teil dieser Ausgabe stellt. Wir könnten jetzt noch was dazu sagen, daß diese Datenschleuder die erste ist, bei der wir Mickeymouse-Technologie eingestezt haben, aber die die Antwort ("Da seid ihr aber nicht die ersten") können wir uns denken und deshalb lassen wir es.

Gute Nacht.

Wer hat übrigens mein' 27B-6 gesehen ?

Virenpanik zur CeBit

Pressemitteilung

4. März 1992

Wie die Sicherheitsbranche die Werbetrommel rührt. Eine Stellungnahme des Chaos Computer Club - Hamburg.

Rechtzeitig zur weltgrößten Computermesse, der CeBIT in Hannover (11. bis 18. März) stiften Warnmeldungen vor dem „Michaelangelo"-Virus Unruhe und Panik unter den Betreibern von Personalcomputern.

Bereits seit Januar leistet der bekannte Hamburger Viren- Spezialist, Professor Klaus Brunnstein vom Viren Test Center, Pressearbeit mit beängstigenden Warnungen vor dem Sabotageprogramm, welches am 6. März zuschlagen soll. Das Bonner Bundesamt für Sicherheit in der Informationstechnik (BSI) zog am 14. Februar mit einer amtlichen Warnmeldung und einer Beschreibung der bösartigen Computergeschwulst nach.

Seitdem reibt sich die Sicherheitsbranche die Hände - allein bei Professor Klaus Brunnstein stapelten sich in der letzten Woche 40 Postsäcke mit Anfragen verunsicherter PC-Benutzer.

Prof. Brunnstein, der dem CCC lange Jahre unwissenschaftlichen Umgang mit diesem Thema vorwarf, muß sich in dieser Situation fragen lassen, ob er als Wissenschaftler die entstandene Panikstimmung bei Privatpersonen und in der Wirtschaft verantworten kann.

Hinter der Virenpanik verbirgt sich eine Marketingphilosophie, wie man sie schon anläßlich des „Freitag dem 13. Virus" oder des „DATACRIME" in den Medien beobachten konnte.

Irreführung des Verbrauchers unterstellt Steffen Wernery, einer der Sprecher des CCC, fragwürdigen Vertretern der Sicherheitsbranche. Diese versuchen wiederholt bei jedem neuen Virus durch Panikmeldungen die Verkaufszahlen für Entseuchungsprogramme und Fachinformationsdienste in die Höhe zu treiben. Nach Wernerys Ansicht könnte nur ein verantwortliches Betreiben von Computersystemen eine langfristige Lösung darstellen.

Die Gefährlichkeit von Viren ist vor allem durch das Informationsdefizit der Benutzer gegeben. Mangelnde Folgenabschätzung, mit oder ohne Technikgebrauch ist letztlich kein computerspezielles Problem; Alkohol im Straßenverkehr gehört genauso dazu wie FCKW in Sprühdosen. Schon 1930 formulierte Albert Einstein anläßlich der Eröffnung der Berliner Funkausstellung: „Sollen sich auch alle schämen, die gedankenlos sich der Wunder der Wissenschaft und Technik bedienen und nicht mehr davon geistig erfaßt haben als die Kuh von der Botanik der Pflanzen, die sie mit Wohlbehagen frißt."

Daher hält der Chaos Computer Club vor allem eine Bewußtseinsbildung unter Sicherheitsgesichtspunkten für notwendig. Wesentlicher Kritikpunkt ist, daß Sicherheit in Unternehmen solange deligiert wird, bis letztlich jemand zuständig ist, der keinen Einfluß mehr hat. Sicherheit ist eine

Führungsaufgabe. Der einzige Vorteil der Computerviren ist, daß wenn diese die Laptops und Taschencomputer des Establishments erreichen, endlich auch die Entscheidungsträger sensibilisiert werden.

Für Verbraucher empfiehlt sich die regelmäßige Überprüfung des Computers mit VirenScannern, wie sie vom WDR-Computerclub über Btx kostenfrei angeboten werden und

der Einsatz von Prüfsummenprogrammen vor jeder Datensicherung. Häufiger Disketentausch mit wechselnden Partnern wird sonst schnell zum Risiko.

Das Problem mit den Computerviren ist so alt wie der Computer. Der „Michaelangelo"-Virus wird von gängigen VirusScannern erkannt. Die Gefahr, die von „Michaelangelo" ausgeht, ist nicht größer, als jene vom Virus „Freitag, der 13te", der eine Woche später - während der CeBIT - aktuell wird.

Die derzeitige Berichterstattung scheint nur dem Ziel zu dienen, der Sicherheitsbranche zur CeBIT volle Auftragsbücher zu bescheren. Zumindest die Viren-Experten auf den internationalen Datennetzen haben dem Virus Michaelangelo bisher keine besondere Beachtung geschenkt. Er gilt dort nicht als außergewöhnliches Problem.

stve & terra & amm

Haftung

bei Programmfehlern und Viren

Referent: Freiherr Günther v. Gravenreuth (Anwalt)

Hier kann leider nur eine unvollkommene Wiedergabe der Auskünfte erfolgen. (Auch mein Turbo-Kuli konnte leider nicht mithalten. Außerdem bin Ich kein Jurist.) Aber dieser Text kann im Zweifelsfalle sowieso keinen Anwalt ersetzten. (Aber ich ich hab' mir trotzdem Mühe gegeben, keinen Müll zu erzählen.) [*Schönen gruß von Anna und Arthur, der, der daß Maul hält*]

Das wichtigste Gesetz in diesem Zusammenhang ist das Produkthaftungsgesetz, das regelt, unter welchen Bedingungen wer wie weit für Schäden haften muß, die durch ein Produkt (in unserem Falle ein Programm) wie auch immer verursacht werden.

Ein Hersteller muß selbstverständlich haften für vorsätzlich verursachte Schäden und bei „positiver Vertragsverletzung", d.h., wenn eine zugesicherte Eigenschaft vom Produkt nicht erfüllt wird. In letzterem Fall hat der Käufer ein Rücktrittsrecht (vom Vertrag), falls der Fehler nicht schnell genug behoben wird, und es besteht für den Hersteller eine Schadenersatzpflicht. (Das gilt für Individualsoftware, d.h. Auftragsarbeit.)

Änderungen des Pflichtenheftes bzw. Abweichungen davon müßen mit dem Auftraggeber abgesprochen werden. Dabei besteht sogar eine Mitwirkungspflicht des Programmierers (bzw. Herstellers); d.h., er muß den Auftraggeber (je nach dessen Wissensstand, also wenn der das Problem selbst nicht erkennen kann) auf Probleme mit dem Pflich-

tenheft hinweisen, wenn also eine andere als die spezifizierte Lösung besser wär. Wurde das Pflichtenheft erfüllt, muß der Auftraggeber selbstverständlich das Produkt auch (vertragsgemäß) kaufen.

Grundsätzlich verjährt nach deutschem Recht ein Fehler nach 6 Monaten, auch wenn er nicht durch Verschleiß verursacht wurde, also auch bei Software. (Verschleiß ist da ja relativ selten.) Der Käufer muß die Fehler selbst vor Ablauf dieser Frist reklamieren, andernfalls hat er in aller Regel keine Ansprüche gegenüber dem Hersteller (Prüfungspflicht des Käufers). (Das gilt i.d.R. für „Stangensoftware".)

Die Haftung nach dem Produkthaftungsgesetz unterliegt weiteren Beschränkungen: So ist die Haftung bei direkten Personenschäden (für andere besteht sowieso keine Haftung) auf bis zu 160 Mio. DM beschränkt. Die Haftung für Sachschäden, die nur besteht, wenn das Funktionieren der fehlerhaften Funktion ausdrücklich zugesichert wurde, gilt nur für Privatsachen. (Was „privat" heißt, entscheidet dabei nicht der Benutzer oder die hauptsächliche Verwendung des Gerätes, sondern andere objektive Kriterien.) [*Siehst Du was Du glaubst, oder glaubst Du was Du siehst, der Seher*]

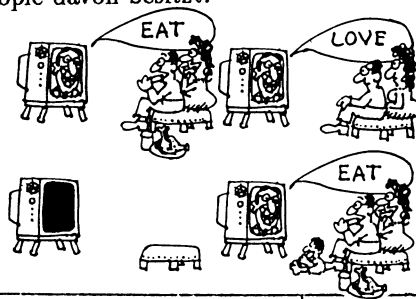
Falls die Erkennung des Fehlers bei der Herstellung noch nicht möglich war, besteht natürlich auch keine Haftung für den Hersteller. Bei Importgeräten haftet im Allgemeinen der Importeur oder der Händler, da eine Klage in Taiwan (z.B.) kaum jemandem zuzumuten ist.

Der Autor des Programmes kann bei Fehlern nicht belangt werden, wenn er bei einer Firma für diesen Zweck angestellt war. Da Programmieren eine „gefahrengeneigte Arbeit" ist, muß sein Arbeitgeber die Fehlerfreiheit sicherstellen, nicht der Programmierer selber. Ein freier Programmierer dagegen haftet natürlich selbst.

Hat ein Anwender eine fehlerhafte Version eines Programmes gekauft, so muß er diese beim Vertreiber gegen die „fehlerfreie" Version umtauschen (oder Geld zurücknehmen und neu kaufen). Er darf nicht stattdessen eine Schwarzkopie der neueren Version benutzen (auch wenn sie nicht teuerer ist).

Auch von einem rechtmäßig erworbenen Programm dürfen Kopien nur mit Zustimmung des Urheberrechtsinhabers angefertigt werden, soweit der bestimmungsgemäße Gebrauch des Programmes dadurch nicht beeinträchtigt wird. (Das gilt z.B. auch für Kopien auf die Festplatte, soweit diese ausdrücklich verhindert werden (Kopierschutz).)

Zur Realisierung der Rücknahme eines Programms durch den Hersteller: Er kann vom Kunden die Rückgabe der Hardware und die physikalische Löschung des Programms verlangen (ggf. mit eidesstattlicher Erklärung und notarieller Beglaubigung). Eine physikalische Rückgabe des Programms ist nicht erforderlich, sofern der Hersteller noch eine Kopie davon besitzt.



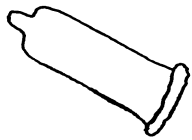
Nun zum Thema Viren bzw. Programmanomalien, also Progammcode, der die Fähigkeit zur Reproduktion hat und eine Funktionalität (das kann auch die Reproduktion sein), die in rechtswidriger Weise etwas ausführt, das der berechtigte Benutzer nicht wünscht. Gutartige Viren sind danach zwar theortisch möglich, aber kaum praktisch. (Welche Funktionalität wünschen schon alle Benutzer eines Programms, die dieses nicht selbst erfüllt?) [*Softwarefehler beheben, ein „User"*] (Nebenbei: Man darf Viren nicht nach unbeteiligten Dritten bennen, solange auch eine andere Bennung möglich ist. Der Entwickler des Virus ist dabei natürlich nicht unbeteiligt.)

Eine Virenverseuchung stellt natürlich einen Mangel dar. Es ist aber von der Beweisführung her sehr problematisch und teuer, nachzuweisen, daß das Virus beim Hersteller auf die Diskette gelangt ist.

Die Praxis, zeitlich befristete Lizenzen zu vergeben und das Programm nach Ablauf der Zeit sich selbst zerstören zu lassen, ist nur dann zulässig, wenn der Benutzer darüber informiert wird und wirklich nur das Programm und nicht irgendwelche anderen Dateien zerstört werden.

Die Veränderung eines Programms ist im allgemeinen nicht zulässig, außer zur Beseitigung von Fehlern oder vielleicht zur Druckeranpassung. (Aber auch ein Virus, das Fehler beseitigt, muß nicht gutartig sein. Vielleicht will der Benutzer es ja gar nicht.)

Ingo



Phreaking

In letzter Zeit machen sich immer mehr technikinteressierte Telefonbenutzer zu Nutze, daß die Vermittlungsstellen verschiedener Staaten und Telefongesellschaften ihre internen Daten zur Vermittlung von Telefongesprächen durch Töne im normalen Sprachband übertragen. So ist es ihnen möglich, kostenlos zu telefonieren, indem sie der Vermittlungsstelle im Ausland mit Frequenzen nach der international anerkannten und benutzen C5-Norm vorgaukeln, daß das kostenlose Telefongespräch zu einer Firma im Ausland (z.B. über 0130er-Nummern) schon beendet ist, während die nationale Vermittlungsstelle wegen der Kürze des Beendungssignals davon ausgeht, daß das Gespräch noch läuft. Mittels eines weiteren Signals kann man dann eine neue Nummer anwählen: Gleich nach dem gefakten Gesprächsendesignal folgt das Kommando mit der gewünschten Rufnummer, so daß die Kosten von der ausländischen zuerst angewählten Firma getragen werden. Man kann sich dann über Transitleitungen von einem Land zum nächsten schalten, wobei einige Länder aber offensichtlich sinnlose Rückschaltungen (z.B. Deutschland-USA-Deutschland) schon technisch verhindern (z.B. in den USA und Japan), weil die Anzahl der Auslandsleitungen nur begrenzt ist und z.B. in Frankreich bereits erhebliche Kapazitätsprobleme auftraten.

Als vorausschauender Phreak sollte man daraus seine Konsequenzen ziehen und diese überlasteten Strecken nur mäßig benutzen, um die Telefon- gesellschaften nicht zu verärgern und so technische Sperren

zu provozieren. Welchen Leitungsweg die 0130er-Vermittlungsstelle bei der Anwahl einer ausländischen Nummer nimmt, ist von Vermittlungsstelle zu Vermittlungsstelle unterschiedlich aber für den Phreak recht interessant zu wissen. Ein einfacher Weg um das zu erfahren ist, die Nummer 0130/0000 anzurufen, dann sagt einem die freundliche Stimme, wohin man verbunden wird, wenn man 0130 wählt. In Frankfurt gibt es z.B. für die Phreaks ein paar Probleme, weil dort die Digitalisierung bereits weiter fortgeschritten ist als bei den anderen Vermittlungsrechnern.

Als Geräte benutzen die Phreaks selbstgebaute Beeper, ähnlich den gebräuchlichen Geräten zur Abfrage von Anrufbeantwortern, aber viel leistungsfähiger. Neuerdings gibt es auch fertige Computerprogramme für populäre Computer (z.B. Amiga, Macintosh), die aber teilweise recht stümperhaft programmiert sind oder es gibt Probleme durch Störfrequenzen wenn mehrere Interrupts gleichzeitig laufen. Besser ist ein gerade entwickelter Bausatz für einen D/A Wandler, der direkt an einem gängigen parallelen Druckeranschluss (z.B. bei einem PC) angeschlossen wird und die benötigten überlagerten Zweifrequenztöne in Form einer Sinuskurve erzeugt.

„ECKBERT, WEISST DU OB WIR TELEFON HABEN?"
„NÖ, KEINE AHNUNG. WER ISS'N DRAN?"

Der Bauplan sowie zwei einfache Softwareprogramme zur Programmierung des Geräts unter MS-DOS sind über den Chaos Computer Club zu beziehen. Die Bauteilekosten liegen unter 20 DM und die ganze Schaltung inklusive Verstärker findet in einem Schnittstellenstecker Platz. Software für andere Rechner ist in Planung, die Sourcen helfen bei der Entwicklung eigener Programme. Man kann die Töne auch Zuhause auf Band aufzeichnen und dann mit dem Recorder in die Telefonzelle gehen. Dabei sollte man aber auf sehr gute Tonqualität achten (z.B. DAT-Recorder) und die Bandlaufgeschwindigkeit muß exakt gleich sein, weil es sonst Timingtrouble gibt.

Das Problem dabei ist, daß immer mehr Menschen kostenlos telefonieren wollen, aber von der eigentlichen Vermittlungstechnik keine Ahnung haben. Wenn man nicht wochenlang trainiert und sich mit der Materie befaßt, kann es zu fatalen Fehlbedienungen kommen, so daß die Post und die geschädigten Firmen auf diese Praktiken aufmerksam werden. Bisher hat es jedoch lediglich eine postinterne Untersuchung der Vorfälle gegeben, nachdem einige "Experten" unbedingt in diversen Zeitschriften über ihre Hacks prahlen mußten und die betrogenen Firmen die Bundespost Telekom unter Druck setzten. Besonders zu verurteilen sind die Softwaretrader, die für enorme Geldsummen Bluebox-Computerprogramme an technikunerfahrene Benutzer verkauften und gleichzeitig Panik in der Phreakszene über angebliche Verhaftungen und Rückverfolgungen von Gesprächen verbreiteten, um nichtzahlende Experimentie-

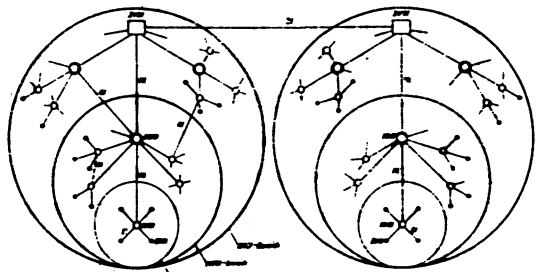
rer abzuschrecken. Wahr ist lediglich, daß die Zielrufnummern in der digitalen Vermittlung (DIF), die die 130er-Nummern in normale internationale Telefonnummern wandeln und die Verbindung aufbauen gespeichert werden, wie es z.B. auch im Autotelefon C-Netz gehandhabt wird. Der angerufenen Firma im Ausland ist maximal der Einwählpunkt in Deutschland bekannt (z.B. Hamburg, Frankfurt,...).

Trotzdem ist natürlich immer Vorsicht beim Forschen angesagt, denn wer weiss besser als die Phreaks, daß die Entwicklung im Bereich der Technik nicht halt macht? In der Regel ist aber eine Nachverfolgung für die Firmen wirtschaftlich nicht interessant solange ihr normaler Geschäftsbetrieb nicht ernsthaft blockiert wird und die Bundespost verdient an den Phreaks nicht schlecht, so daß sie aus eigenem Antrieb wohl nichts unternehmen wird. Auf jeden Fall sollte die Phreak-Szene erheblich besser zusammenarbeiten und sich nicht gegeneinander verschanzen, weil davon nur die verachtungswürdigen kommerziellen Verwerter profitieren, die keinerlei Pionierarbeit leisten.

Innerhalb Deutschlands funktioniert das Blueboxing-Verfahren nicht, weil die Leitungsdaten dort systemintern und nicht im normalen Sprachband übertragen werden. In Zukunft wird es für die Phreaks noch größere Probleme geben, weil im Zuge der Umstellung von analogen auf digitale Vermittlungsstellen auch das C7-Verfahren zur Weitergabe von Leitungsdaten eingeführt wird, bei dem Daten- und Sprachleitung getrennt sind. Dadurch wird Phreaking zwar schwieriger, aber auch interessanter und man sollte nicht vergessen, daß es wohl immer Länder geben wird, die sich keine Vermittlungsanalage leisten können, so daß die alten Beeper nicht auf dem Müll landen müssen. Ausserdem wurde Blueboxing schon vor Jahren totgesagt und heute funktioniert es noch immer in Deutschland, der Schweiz, Österreich, Italien, usw. Probleme gibt es noch in Russland, weil man dort fast nie eine Auslandsleitung bekommt.

Kurz wurde auf dem Workshop noch einmal auf die Redboxes eingegangen, die nur in den USA und Kanada funktionieren und in der Telefonzelle wertvolle Dienste leisten, indem die Toene, die beim Einwerfen von Münzen entstehen über einen Beeper simuliert werden.

Netzgestaltung im Fernmeldedienst



Viele Phreaks haben auch schon mit den postinternen 1177-Nummern herumprobiert. Einige hatten auch schon Erfolg, man sollte aber bedenken, daß an diesen Nummern sowohl automatische als auch mit Menschen besetzte Prüfplätze angeschlossen sind, so daß es für die Post überhaupt kein Problem ist, die Leitungen zurückzuverfolgen.

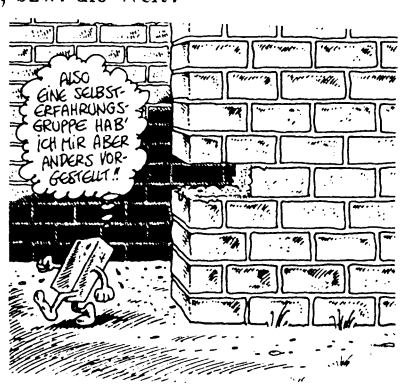
Vor der Umsetzung der in diesem Artikel erwähnten technischen Möglichkeiten hat sich mensch selbstverständlich vorher nach den damit verbundenen rechtlichen Bestimmungen zu erkundigen.

henne

Feminines Computerhandling

Erstmalig vor zwei Jahren sammelten sich die Frauen auf dem CCC, um ihr eigenes Projekt aufzuziehen. Thema: Frauen und Technik. Nachdem im letzten Jahr schlechte Erfahrungen mit den männlichen Zuhörern dieses Kollegs gemacht wurden, wurde dieses Mal den Männern der Zutritt rigoros verwehrt, um endlich einmal ungestört diskutieren zu können. Einzeln sollten sich alle Teilnehmerinnen vorstellen und kurz eine Einführung über ihre Erfahrungen im Umgang mit Computern geben. Eine bunte Mischung war vertreten: Schülerinnen, Studentinnen, Seminar- und Projektleiterinnen, Anwenderinnen von Textprogrammen und im Bereich der politischen Arbeit. Sie alle hatten zum Teil schon mehrjährige Erfahrungen gesammelt und begründeten ihr Interesse am Computern mit der Faszination an Kommunikationstechniken und der neuen Rolle der Frau beim Eindringen in die bisher männliche Domäne der Technik.

Zwei Fragen wurden zu Anfang gestellt:
Programmieren Frauen anders als Männer?
Was bringt Informationstechnologie für die Frau, bzw. die Welt?



Zunächst wurde jedoch sehr viel allgemeiner die Frage aufgeworfen, warum es eigentlich so wenige weibliche Anwender gibt. Die Antwort war vor allen Dingen gesellschaftspolitisch zu sehen: Aufgrund der Erziehung seien Frauen und Technologie zwei Welten, die aufeinanderprallen. Selbst wenn Interesse vorhanden ist, gibt es für Frauen lediglich minderwertige und weniger umfangreiche Angebote wie z.B. die Textverarbeitung. Dieses Problem der Abdrängung schließt den Kreislauf, bei den Frauen erlahmt das Interesse.Eine Änderung der Gesellschaftsstruktur, diesem von den Männern geprägten Apparat, wäre notwendig, um Abhilfe zu schaffen. Immerhin ist das System schon durchläßiger geworden, eine gewisse Dynamik ist bemerkbar.

Wie kann man dem abhelfen? Da bei beiden Geschlechtern eigentlich das gleiche Interesse vorhanden ist, muß frau mehr Durchsetzungsvermögen zeigen, sich nicht mehr so sehr in den Hintergrund drängen lassen, da Männer ein anderes Selbstverständnis besitzen. Bei der Lösung von Problemen ist das Verhalten dann dementsprechend: Eigenständiges Arbeiten und Ausprobieren ohne fremde (männliche) Hilfestellung ist erwünscht, selbst wenn dieser Weg langwieriger sein sollte. Die Auseinandersetzung mit der Technologie erfolgt demnach nicht nur in der Anwendung, vielmehr ist eigenverantwortliche Weiterentwicklung gefragt.

Auf diese Art und Weise kann vielen anderen Frauen der Weg zum Computer und dessen Faszination geebnet werden. Genauer nach letzterem befragt, wurden männertypische

Aspekte genannt: der Umgang mit mathematischen Problemen, die Omnipotenz des Gerätes und das Gefühl, es zu beherrschen, es sich "untertan" gemacht zu haben. Kann der Computer dabei zur Sucht werden?
Bei der Mailbox als Medium kann diese zwar als Ergänzung des Kommunikationsbereiches gesehen werden, andererseits kann die Dialogsituation auch verschieden aufgefaßt werden: Das fehlende face-to-face ist kein Ersatz für persönliche Kontakte und könnt eventuell auch eine Verarmung darstellen. Auch die Beurteilung der immer größer werdenen Informationsflut in immer kürzerer Zeit ist problematisch, der einzelne könnte unter dem Zwang zum Perfektionismus überfordert sein.

Wie sieht nun die Entwicklung in den nächsten Jahren aus? Zur Zeit gibt es lediglich Aufstiegsmöglichkeiten für absolut „perfekte" Frauen, da wir uns in einer Übergangsphase befinden, wo sich das Bewußtsein innerhalb der Gesellschaft nur langsam ändert. Aufgrund der Tatsache, daß jedoch vermehrt Diskussionen in der Öffentlichkeit, sprich den Medien geführt werden, wird diese Veränderung sichtbar, wobei das Problem der Alibifunktion von Frauen in Führungspositionen („Quotenfrau") einen negativen Beigeschmack hat. In diesen Zusammenhang gehört auch die gerade aktuelle Diskussion über die Abschaffung der Koeduktion, um Frauen und Männern die gleiche Ausgangsbasis zu schaffen, die sicherlich in Zukunft zur Gleichstellung beider Seiten auf dem Gebiet der Technologie führt.

Henrike

Netzwerkdienste

Praxis am Beispiel InterNet

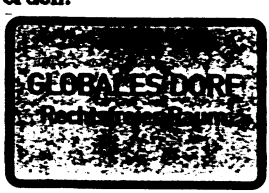
Vortragende:
Zotty (e-mail: umv001@dbnmeb1.bitnet)
Princess (e-mail: iws88116@ibm.rz.uni-passau.de)
Framstag (e-mail: framstag@rz.uni-ulm.de)

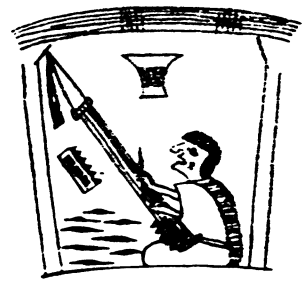
Das InterNet wurde ausgewählt, weil sich an diesem Netz die Möglichkeiten auch der anderen Netze gut zeigen lassen. Aus der Vielzahl der Fähigkeiten wurden folgende ausgewählt und vorgestellt: Mail, Conferencing (NetNews), Remote Login, File Transfer, Realtime Conferencing.

Mail bietet als elektronische Post die Möglichkeit, Nachrichten über die Netze an einen oder mehrere Empfänger zu senden. Innerhalb Deutschlands erreicht die Nachricht ihren Bestimmungsort oft in wenigen Stunden, während die normale Briefpost mindestens einen Werktag braucht. Bei kurzen Nachrichten ist diese Versandform auch deutlich billiger. Sogar Fortgeschrittene haben jedoch Probleme, im oft verschlungenen Netze-Dschungel unbekannte Netzwerkadressen zu finden. Besondere Schwierigkeiten können sich ergeben, wenn die Adresse in einem anderen als dem eigenen Netz liegt, da die Adressen in verschiedenen Netzen verschieden angegeben werden. Der Übergang zwischen Netzwerken wird deshalb in einem Text namens GATOR (GATeway Orientierungs- Ratgeber) erklärt, der über die meisten Netze erhältlich ist. Wert gelegt wird auch auf gewisse Umgangsformen: Man sollte sich kurz fassen, möglichst treffende Betreffzeilen zu schreiben (sonst findet sich niemand durch seinen Mail-Datenwust durch) usw.

Conferencing oder NetNews ist ein weiterer wichtiger Dienst, der auf allen Netzen angeboten wird. Er ähnelt einer riesigen Sammlung von (Fach-)Zeitschriften, die allerdings nur aus Leserbriefen bestehen. Jeder Benutzer kann Texte über diesen Dienst an alle anderen schreiben. Da die Netze die gesamte Welt umfassen, ist die normale Verkehrssprache Englisch. Im InterNet heißt dieser Dienst UseNet oder News. Das Schreiben eines Artikels ins Usenet nennt man „posten". Um die Datenmengen auf den Platten der Rechner im Netz nicht ins Unendliche steigen zu lassen, werden die Artikel nach einer bestimmten Zeit („Expire"; sie ist je nach Newsgroup - s.u. - unterschiedlich lang) gelöscht. Jeder Artikel enthält vor dem eigentlichen Text einen Header mit verschiedenen Informationen (Betreff, Absender, Newsgroup etc.) und danach die Signature des Autors (mit e-mail-Adresse und Spruch oder anderer persönlicher Note...). Wichtig ist auch die Distribution, also der Bereich, in dem der Artikel verbreitet werden soll. Die Möglichkeiten reichen von local (nur auf dem lokalen System) bis world (im gesamten Netz, also weltweit). Für einige Newsgroups - allerdings sehr wenige - gibt es auch eine Moderation, d.h., vor der Verbreitung der Texte wird von einem Moderator (oder einer Gruppe) entschieden, ob er für dieses Brett wirklich von Interesse ist.

Zur besseren Übersicht ist das gesamte Usenet in ca. 2000 Newsgroups eingeteilt. Sie entsprechen etwa verschiedenen Zeitschriften (um in der Analogie zu bleiben) oder deren Rubriken. Die Gliederung ist also hierarchisch. Als Obergruppen (weltweit) gibt es (mindestens) alt(ernatives), comp(uters) (zum Beispiel comp.binaries.ibm.pc), misc/-(ellaneous), news (Bsp. news.announce.newusers:
eine der wenigen moderierten Newsgroups; hier stehen Infos für neue Benutzer), rec(reation) (wie rec.pets.birds o.ä.), sci(ence) (z.B. sci.lang.japan oder sci.physics.fusion), soc(ial) (soc.religion.islam) und talk (etwa talk.abortion). Außerdem gibt es deutsche Gruppen wie dnet oder sub (mit sub.kultur u.a.), regionale Gruppen (north, ruhr etc.) und lokale Gruppen (unter loc).
Ein wenig Statistik: Im November 1991 fanden (auf einem Unirechner) 30.718.672 Lesezugriffe auf das Usenet statt. Es wurde insgesamt 1 Gigabyte Daten im Usenet hin- und hergeschoben.
Natürlich gibt es auch für die äußere Form von News-Artikeln einige Richtlinien, an die man sich auch halten sollte, wenn man nicht mit „flames" (unfreundlichen Beschwerde-Mails) überschüttet werden will. Die Texte sollten nicht mehr als 75 Zeichen pro Zeile haben, keine Sonderzeichen enthalten und so weiter. Natürlich sollte auch das Copyright beachtet werden.





Remote Login funktioniert nur, wenn eine Verbindung zu dem entfernten (remote) Rechner besteht, auf dem man sich einloggen möchte. Man kann dann mit diesem Rechner fast so arbeiten, als würde er unter dem eigenen Schreibtisch stehen. Im Internet bestehen zwischen den Rechnern grundsätzlich Standleitungen, in anderen Netzen gibt es so etwas nicht, remote Login ist also nicht in allen Netzen möglich. File transfer (ftp) ist ein Dienst, mit dem ein Benutzer sich Dateien von einem fremden Rechner auf seinen eigenen kopieren kann. Auch das ist nicht immer problemlos, da teilweise zwischen Binär- und ASCII-Dateien unterschieden werden muß.
Wohl der interessanteste Dienst ist das Realtime Conferencing. Ähnlich wie im Amateur- oder CB-Funk können sich da mehrere Leute über Gott und die Welt unterhalten. Das ist sehr beliebt zum Kennenlernen, Infos Austauschen (Stichwort online-Hilfe) und überhaupt.
Anläßlich der Vorstellung von Usenet entbrannte übrigens auch in dieser Veranstaltung die Diskussion über Sinn und Unsinn von Newsgroups wie alt.sex, des Emma-Artikels dazu und der Reaktionen darauf.

Ingo & Nikolaus

CHIPKARTEN

Anwendung und Funktion

Projektleiter: Marcus Janke, Peter Laackmann

In den letzten Jahren wurden sehr viele verschiedene Formen der Identifikations-, Kredit- und Guthabenkarten entwickelt. Die hauptsächlich benutzten Technologien sind Magnetstreifenkarten, Karten mit optischer Codierung sowie Chipkarten, die entweder eine festverdrahtete Logik (Guthabenkarten, Telefonkarten der Post) oder einen Microprocessor enthalten (Kreditkarte, Buchungskarten). Diese Technik gilt zur Zeit als sehr sicher, da z.B. ein Passwort auf dem Chip existiert, das durch eine Sicherheitsschaltung gegen Auslesen von aussen geschützt werden kann.

Das Projekt „Telefonkartenworkshop" und der Vortrag „Chipkarten" am 28.12.91 sollten die Technik der Karten sowie der dazugehörigen Informationsverarbeitung darstellen, also die Funktionsweise der Kartentelefone, der dazugehörenden Anschlusseinheiten in der Vermittlungsstelle sowie der zentralen Datenverarbeitung. Die Projektleiter stellten ein Lesegerät als Hardware für den C-64 vor, welches alle auf einer Telefonkarte gespeicherten Daten wie Gebührenstand, Seriennummer, Datum sowie Hersteller der Karte in Sekundenbruchteilen ausliest. Die Hardware selbst ist sehr einfach, liegt im Kostenbereich von unter 20,-DM und findet im Userportstecker Platz.

Sp141

Sp142

Sp143

Weiterhin wurde der Aufbau des Chips durch Auswertung von Licht- und Elektronenmikroskopfotos untersucht, wobei die Art der Speicherung auf dem Chip als EEPROM erkannt wurde, welches durch eine zusätzliche Schaltung gegen Missbrauch geschützt ist. Weiterhin ist der Chip selbst mit einer Kunststoffschicht bedeckt, die ihn vor UV-Einwirkung und mechanischer Beschädigung schützt. Wird diese Schutzschicht entfernt, so werden die Daten auf dem Chip gelöscht, so daß auch das direkte Auslesen der Daten mittels eines Elektronenmikroskops nicht mehr möglich ist. Wie aus Datenblättern bekannt wurde, ist das „Aufladen" einer Telefonkarte durch Eingabe eines 32-Bit Passwortes möglich. Ein interner Fehlerzähler begrenzt die Anzahl der Versuche für dieses Passwort auf 4, danach wird die Karte dauerhaft unbrauchbar. Ein auf dem Chip vorhandener Rahmenzähler begrenzt auch diese Zahl auf maximal 64 Aufladungen. Früher war geplant, die Karten an Automaten der Post aufzuladen, wobei das Passwort aus den übrigen Daten mit Hilfe einer Kryptofunktion berechnet werden sollte. Inzwischen sind die Preise für Chipkarten jedoch gesunken, so daß sich das Aufladen nicht mehr amortisiert. Auch ist der Aufwand und das erhöhte Risiko für das System zu hoch.

Ein weiterer wichtiger Aspekt bei der Anwendung dieser Technik als Telefonkartensystem ist der Datenschutz. Im Vortrag wurde darauf hingewiesen, daß über jedes Gespräch in einer Kartentelefonzelle ein Gebührendatensatz von 100 Bytes angelegt wird, in dem Daten stehen wie Standort des Kartentelefons, KARTENNUMMER, ZIELRUFNUMMER, Dauer und Zeit des Gesprächs sowie weitere postinterne Daten. Dieser Datensatz soll nach Angaben der Bundespost nach 80 Tagen gelöscht werden, wird jedoch auch für Statistiken verwendet. Diese Tatsache ist den meisten Benutzern sicherlich nicht bekannt.

Peter Laackmann

MausNet

Im Jahr 1984, die Welt ist im Orwell-Fieber und Bob Woodward hat eben seine Biographie über den Blues-Brother John Belushi und dessen Drogentod veröffentlicht, war die bundesdeutsche Mailboxszene noch nicht besonders ausgeprägt. Wenige Systeme wie RMI von Rupert Mohr, Decates und MCS [*huhu thommy, der grüßer*] führten ein vergleichsweise einsames Dasein. Ein Jahr vorher blamierte sich der Stern mit den „Hitler-Tagebüchern" und William Gibson schrieb seinen „Neuromancer".

Tauchte beim „Neuromancer" der User unmittelbar über sein nervliches Sensorium in ein komplexes, weltumspannendes Datennetz Namens „Matrix" ein, so mußte er in der Realität höchst mittelbar und extrem langsam mit den wenigten verfügbaren Systemen Kontakt aufnehmen. Und auch von weltumspannenden Netzen konnte damals noch nicht die Rede sein. Zwar gab es an einigen Universitäten „Usenet" (Larry Wall brachte im April '84 die erste Version seines „rn" heraus), aber Tom Jennings, der Begründer des FidoNet, fing gerade mal mit zwei Systemen an.

Zu diesem Zeitpunkt – Ende 1984 – fingen einige Enthusiasten aus einer Apple-Keimzelle in Münster an, ihre eigene Mailbox zu programmieren. Sie waren der kryptischen und unergonomischen Bedienung anderer Systeme überdrüssig, wo wilde Zahlenkombinationen das Mailboxprogramm steuerten und man geradezu einen Führerschein oder Lehrgang brauchte um sich als User zurechtzufinden. Ihnen schwebte etwas intuitiv

bedienbares vor, für Anfänger ebenso leicht, wie für Fortgeschrittene schnell zu bedienen. Übersichtliche Menues mit Hotkeys statt Zahlenkürzeln und Kommandozeilen (Das Programm Zerberus, welches zwar auch mit Kommandozeile, dafür aber mit wesentlich leichter zu merkenden Wort-Befehlen arbeitete, konnten die Autoren nicht kennen da es erst ein Jahr später erschien. Es dürfte ihre Absichten aber wohl auch nicht beeinflußt haben...)

Verwirklicht wurde das Ganze auf einem Apple II Clone unter Turbo-Pascal und wurde unter dem Namen M.A.U.S. - die Abkürzung stand damals noch für „Münster Apple User Service" - Anfang April '85 auf die bundesdeutsche Szene losgelassen. Die Art der Benutzerführung ist seither eine Art Markenzeichen für die Maus-Software, in gewisser Weise auch eine Politik. Bezeichnend dafür ist die Tatsache das die entsprechenden Code-Zeilen seit dieser ersten Version unverändert bzw. nur erweitert wurden. Wenig später wurde das Programm innerhalb weniger Tage von der Apple-Basis (ein Wortspiel übrigens, für den, der's versteht :-) auf MS-DOS und Turbo-Pascal 3.0 konvertiert - notgedrungen, denn die alte Hardware hat ihren Dienst eingestellt. Zu diesem Zeitpunkt eröffnete Wolfgang Mexner die erste Zerberus Mailbox und FidoNet hatte eine Handvoll Installation in Deutschland.

Heute, Ende 1991, besteht das MausNet aus 50 Installationen bundesweit (zwei Sites in Österreich sind in Vorbereitung). Diese geringe Zahl von Installationen für eines der ersten deutschen Mailboxprogramme läßt sich in der nicht-ganz-so-einfachen Einsteigsprozedur für neue Sysops erklären. Während beim Z-Netz der Kauf des Programms, bei FidoNet sogar nur die erfolgreiche Installation des Paketes genügt um Sysop zu werden, wird im MausNet eine kurze Vorstellung des potentiellen Neu-Sysops verlangt. Er soll in eigenen Worten ein wenig von seiner Person erzählen und wie er zum MausNet kam, resp. wieso er eine MausNet Mailbox betreiben will. Die Sysops geben danach in der Regel ihr Placet. Diese psychologische Hemmschwelle hat bisher die Fluktuation im MausNet recht gut eingedämmt. Ist man als neuer Kollege akzeptiert, dann erhält man die Maus-Software gegen 100.- Shareware-Gebühr (für kommerzielle Stand-alone Nutzung fallen 500.- KAUFpreis an).

Die Netzstruktur im MausNet ist streng baumförmig auf einen Hauptserver ausgerichtet. Pro Netzaufruf (zwischen 4:00h und 6:00h morgens) finden zwischen zwei miteinander verbundenen Boxen jeweils ZWEI Anrufe statt, die auf jeweils andere Telefonrechnungen anfallen. In der ersten Stufe senden die Systeme in den untersten Netzebenen (also die Blätter im Baum) ihre Daten (auf ihre Rechnung) nach 'oben'. Nach einiger Zeit erhalten sie den Rückruf von ihrem Server, der die neuen Daten der anderen Systeme (auf seine Rechnung) überträgt. Die insgesamt übertragenen Daten werden gegen die entstandenen Kosten aufgerechnet und jedes System zahlt an seinen Server nur für die Daten die es mehr empfängt als es gesendet hat. Eine automatisierte, aber ziem-

lich gerechte Art der Abrechnung. Weiterhin hat diese Netzstruktur auch den Vorteil, das eine Laufzeit von einem Tag durch gesamte Netz beinahe garantiert werden kann (was es nur verhindern kann ist der Ausfall eines Systems).

Über die Gateways im MausNet kann man diese Geschwindigkeit nicht ganz beibehalten. Der FidoNet-Gateway in Aachen läuft zweimal täglich um im FidoNet 242 liegt die Laufzeit aus dem MausNet heraus in der Regel bei 1.5 Tagen. Der Z-Netz Gateway in München läuft auch zweimal täglich - eine MausNet Mail schafft es innerhalb 1.5 Tagen in große Teile des Netzes. Nur gibt Z-Netz leider keine Rückmeldung über unzustellbare Mails. Der InterEUNet Gateway in Bremen wird sogar viermal täglich betrieben - mit entsprechend guten Laufzeiten. Der ProNet-Gateway in Köln läuft einmal täglich, wobei mir über die Laufzeiten im ProNet nichts bekannt ist. Der GEnie Gateway ist leider seit wenigen Tagen eingestellt.

User-Politik im MausNet ist die Offenheit. Es gibt im Netz nur drei Typen von Benutzern. Der GAST, der sich nicht namentlich einträgt. Er sollte möglichst schon einige Newsgroups lesen können und, je nach Sysops, auch Programme downloaden. Der Typus USER hat seinen Namen im System hinterlassen und sollte dann nahezu vollen Lesezugriff, evtl. auch öffentlichen Schreibzugriff haben. Das Versenden von persönlichen Mails ist nur nach Entrichtung eines Jahresbeitrages (20.- bis 50.-, je nach Stadt PRO JAHR(!)) möglich. Der SYSOP zum Schluß ist für die technische Funktion des Systems zuständig.

Vernetzungen und Gruppenwünsche gehen in der Regel von Userseite aus, werden auf jedenfall aber dort abgestimmt. Für eine neue Newsgroup muß man zehn Unterstützer für die Einrichtung finden - eine Abstimmung ist in der Regel nicht nötig. Bei einer Vernetzung über einen Gateway müßen sich die User dafür aussprechen, und in der Regel wird darüber auch abgestimmt. Gleiches gilt, wenn ein anderes Netz von uns Newsgroups beziehen will.

Wen dieser kurze Einblick neugierig gemacht hat, den lade ich herzlich ein, sich mal bei uns umzuschauen. Nähere Infos über die Maus-Software selbst gibt es bei js@ac.maus.de

Michael Keukert

Voicemailboxen und PID

Nachdem nun die Allergie gegen Anrufbeantworter und ihre langweiligen Ansagen immer weiter um sich greift, haben sich mailboxverwöhnte Menschen etwas neues ausgedacht: Voicemailboxen, die Informationen in Form von Sprache bereitstellen und über normale Tonwahlfrequenzen (z.B. Beeper vom Anrufbeantworter (Kosten: ca. 10 DM) oder von jedem Kartentelefon aus) bedienbar sind. Die Möglichkeiten reichen von persönlichen Nachrichten an bestimmte Benutzer über öffentliche Foren und Infotexte bis hin zu Konferenzen mit mehreren Teilnehmern. Diese Dienste nennen sich in postdeutsch „persönliche Informationsdienste" oder auch PID. International eingebürgert ist der Begriff „Audiotext" und „voice response systems".

Die Post führt zur Zeit gerade einen Feldversuch mit acht Anbietern durch. Beschränkungen: Keine Sexanbieter, keine Konferenzen und kein Glücksspiel. Die Systeme sind alle unter den neuen 0190-Nummern angeschloßen, bei denen der Anrufer über seine Telefongebühren die Leistungen bezahlt (eine Einheit dauert dann nur 12 Sekunden). Dabei erhält der Anbieter selbst aber nur 46% [*2*23, der seher*], den Rest behält die Bundespost. Der Anbieter muß ein Mindestgebührenaufkommen von 3000 Einheiten im Monat garantieren.

Von der Darmstädter Firma Telesys wird ein postzugelassenes, sehr leistungsfähiges aber auch recht teures Voicemailboxsystem angeboten, das sehr viele Leitungen auf einmal bedienen kann und z.B. als Kundeninformationssystem für Luftfracht bei Lufthansa eingesetzt wird.

Wem ein kleineres System reicht, der kann sich eine Steckkarte für den PC zulegen, die je nach Leistungsfähigkeit zwischen 100 und 1000 Mark kostet. Vorgeführt wurde die BigMouth Karte von der amerikanischen Firma Talking Technology, die eine Sekunde Sprache als vier Kilobyte auf der Festplatte speichert. Die Texte sind völlig frei definierbar und verschiedene Menuefuehrungen (z.B. für verschiedene Sprachen) sind möglich. Als Beispiel zeigte Steffen Wernery sein menuegeführtes Stöhnsystem mit Hitparade zum Mitmachen (Telefonnummer siehe unten). Ein Problem bei dieser Steckkarte ist nur, daß der Hersteller pleite ist und es nur noch sehr wenig Lagerbestand gibt.

Ein Teilnehmer bemerkte, dass es in der Novemberausgabe der Funkfachzeitschrift „cqdl" einen Bauplan inklusive Software für ein solches Gerät gibt.

Zum Schluss noch ein paar Nummern zum Ausprobieren: 040/4807780 Telefun Hamburg (Steffen Wernery) mit Stöhnmenue
0031/20/6001480 Hacktic-Redaktion Amsterdam (holländisch/englisch)
040/4903757 Chaos Computer Club - Hamburg
02421/2040 Teletreff Düren (Deutsche Bundespost) Konferenztestsystem mit 10 Leitungen

henne

Mailboxsystem ZERBERUS

Da der eigentliche Hintergrund dieses Workshops, oder was auch immer, nicht genau festgelegt war, berichtete uns padeluun zuerst einmal über die neue Version von Zerberus, die zur CeBit fertig sein soll.

Sie soll in der Bedienung wesentlich einfacher sein. Dies kann Mensch ja auch schon an der Bionicce hier auf dem Congress testen.

Die wesentlichen Neuheiten sind:

- neugestalteter Menuebaum, der auch für User mit langsamen Modem gut zu bedienen ist
- Bessere Verwaltung der Bretter, leider auch weniger (Bretter)
- Zerberus soll nach einem Logout keinen RAM-Speicher mehr klauen
- Modularer Aufbau des Systems
- Bessere Kostenverwaltung
- Zerberus soll jetzt richtig professionell werden aber nicht in den "totalen Kommerz" verfallen

Der Menuebaum ist so gestaltet, daß nicht mehr alle Unterbretter mit angezeigt werden, sondern erst eine Auswahl aus Hauptbrettern, von welchen Mensch eins auswählen kann. Darauf bauen sich die Unterbretter der „1. Etage" auf, usw. So ist der Menuebaum auch für User mit niedriger Geschwindigkeit erträglich benutzbar.

Auch die Verwaltung der Bretter soll erheblich einfacher werden. Genaueres konnte Mensch leider nicht erfahren. Denkbar wäre da eine bessere Organisation von Masken, etc. Wünschenswert wäre auch ein Autoeintrag.

Ebenso wie der Menuebaum und die Brettverwaltung soll auch das Speichermanagement erheblich besser werden. Zerberus klaut keinen Speicher mehr nach jedem Logoff, so daß der SysOp nicht mehr eine Unmenge an Sicherheitstools (z.B. timeboot, oder Memory-Watcher) einbauen muß, damit sich das System nicht aufhängt. Besonders Interessant ist so etwas natürlich für Systeme, die von dem/n Systembetreiber/n [*der Systembetreiberin, der streicher*] nicht immer zu erreichen ist, weil die Mailbox z.B. in einem Büro untergebracht ist.

Die Bedienerfreundlichkeit des alten Zerberus wurde noch von interessierten Zerberuslern und teilweise nur nörgelnden Fido-Menschen durchgekaut. Das ganze wurde am oberschwierig zu bedienenden Befehl SUCHEN getan. Es ist recht kompliziert und zeitaufwendug dazu, nach irgendetwas zu suchen. ein Diskussionsteilnehmer hatte versucht einen Betreff mit „*Congress*" zu suchen, um zu erfahren, wo der Congress stattfindet. Es hat nicht geklappt. Auch die Geschwindigkeit läßt zu wünschen übrig. Dies soll auch anders werden. Da einige Programmierer jetzt Informatiker sind, haben sie gelernt, richtige Suchstrukturen zu basteln, die das Verknüpfen erlauben und die Geschwindigkeit erhöhen. padeluun gab zu bedenken, daß die Suchgeschwindigkeit natürlich auch sehr stark von der Mailboxhardware abhängt.

Durch diese Entwicklungsschritte soll Zerberus professionell werden. Da wirft sich natürlich die Frage nach dem Preis auf. Bei dem derzeitigen Preis von 898.- DM +

MwSt wird es allerdings bleiben. Es wird allerdings keine Sozialtarife mehr geben. Aber es gibt eine sogenannte Light version, die in ihrer Leistung eingeschränkt, jedoch voll einsatzfähig ist und für eine kleinere Mailbox volkommen ausreicht. Sie enthält dann keine Features, wie z.B. die direkte Gebührenabrechnung per Bankeinzug, etc. padeluun wird jedoch wiederholt vorgeworfen, daß er nur „den totalen Gewinn" machen will und sich kaum um die Interessen der User kümmere. Er stelle sich als Guru des Netzwerks hin. Aber die Programmierer müßen ja auch irgendwie leben. Ein so großes und gewartetes Programm ist ber PD- und Sharewarekonzepte nicht finanzierbar, da der Arbeitsaufwand einfach viel zu hoch ist und „die Programmierer dann verhungern würden". padeluun hat es satt, zu leben wie ein (.zensiert.) und will nicht mehr in einer „Durchgangswohnung" leben, wo jeder auch in den entferntesten Winkel vordringen kann. Wer kann es ihm verdenken?

beppo

Radios und Armbanduhren

Die Hacktik-Redaktion aus Holland zeigte auf dem Congress in der Veranstaltung „Radios und Armbanduhren", daß es ohne großen Aufwand möglich ist, Cityruf-Meldungen, die eigentlich nur für den Empfänger bestimmt und keineswegs öffentlich sind, abzuhören.

Die Texte werden von der Cityruf-Sendestelle zum portablen Cityrufempfänger per Funk als ASCII-Text übertragen. Hacktic entwickelte eine kleine Platine, an die auf der einen Seite ein Scanner (Funk-Empfänger) und an die andere Seite ein beliebiger Rechner mit serieller Schnittstelle angeschloßen werden. Nun kann man ein einfaches Terminalprogramm starten und es erscheinen Meldungen wie „sofort 346236 anrufen", „Termin Mueller 15:00 Uhr" oder „du bist gefeuert" auf dem Schirm, während die Empfänger der Nachrichten nichts davon ahnen. Theoretisch möglich ist auch das Senden von Cityrufsignalen und -texten, die sonst nur über Btx oder die telefonischen Aufnahmestellen eingespeist werden können. Man muß lediglich eine sendefreie Lücke abpaßen und die Daten senden.

Die Anschlußzahlen zeigen, daß Cityruf immer mehr eingesetzt wird, nicht nur im beruflichen, sondern auch im privaten Bereich. Die Telekom weist die Kunden nicht auf diese Sicherheitslücke im Cityruf-System hin, so daß verbrecherisch veranlagte Menschen mittels Bufferung von Cityruf-Daten über mehrere Monate eine digitales Persönlichkeitsbild der belauschten Cityruf-Benutzer erstellen können.

Henne

Definitionsfragen

Neue Themen aufgreifen ?

[*Auch wenn der Autor meinte, dieser Text seihe nur im Kontext mit anderen Texten zu verstehen, haben wir diesen Text alleine verwendet, wir meinen, er sei auch ohne Kontext zu lesen, die Red.*]

Selten hat eine 2-Stunden-Veranstaltung in den letzten Jahren auf einen Chaos Communication Congress soviel Wirbel im Vorfeld erzeugt. Die ersten Fälle über den gezielten Einsatz von Viren oder Hacks gegen die Technik zur Durchsetzung politischer und wirtschaftlicher Ziele bringt eine neue Qualität in die Diskussion über Technik-Folgen und die Abhängigkeit einer Gesellschaft.

Nun ist es eine nicht selten verwendete Methode, erstmal Nachrichten (die erst durch eine Interpretation zur Information wird, wie die Informationswissenschaft lehrt) in Zweifel zu ziehen. Der Spiegel ist ein beeindruckendes und einflußreiches Medium in diesem unseren Lande. Er hat viel aufgedeckt und gilt als Medium, welches gut recherchiert. Aber anscheinend wird hier geglaubt eine Nachricht aus Medien mit der Nachricht eines anderen Mediums widerlegen zu können. Dabei wird ignoriert, daß die Meldungen auf deren Grundlage viele Arbeiten, eben Quelleninformationen sind. Die Meldungen die wir anführen beziehen sich auf Meldungen und Stellungnahmen im Zuge von Diskussion der NASA und Jap Ministerien oder GMD-Meldungen. Aussagen über Viren gegen die Space Shuttle und das Umfeld sind berichtet worden, die NASA hat dazu Stellung genommen, und die ursprüngliche Meldung korrigiert oder versucht aus ihrer Sicht „richtigzustellen". Es muß begriffen werden, daß ein weltweites Kommunikationsmedium stark von der Selbstregulierung lebt. Im Gegensatz zu „Zeitungsenten", wo die korrigierende Meldung einer Zeitung in der letzten Ecke steht, hat die Stellungnahme und die Diskussion in den Kommunikationsnetzen den selben Stellenwert. Hier korrigieren nicht „nachrecherchierende" Journalisten, sondern die betroffenen Leute, die ihre Meinungen und Informationen gegenüberstellen. Daher sollte eine Aussage: „Techno-Terrorismus gibt es nicht" mit vorsichtig genossen werden.

Die Hacker-Ethik spricht davon, dass Hacker nach ihren Handlungen beurteilt werden sollen. Da wir im CCC bekanntlich das „hacken" als kritischen-spielerischen Umgang mit Technik begreifen, müßen wir uns überlegen, was diese Aussage für uns heißt. Wir müßen uns sogar fragen, ob diese Aussage so stehen bleiben kann. Muß nicht die Intention eines Handels auch - vielleicht sogar der wichtigere - Rolle bei der Beurteilung eines Menschen spielens ?

Es wurde angesprochen, daß der CCC sich selbst bestimmte Aufgaben gestellt hat, wie z.B. Informationsfreiheit. Es besteht kein Zweifel, dass wir unsere Daseinsberechtigung nicht zuletzt aus diesem Begriff ziehen. Aber inhaltliche Arbeit ist zentral vom Umfeld der Arbeitsmöglichkeiten im CCC und von seinem inneren Zustand abhängig. Diese Erfahrung mußte der CCC vor einigen Jahren machen. Der sogenannte Hamburger Klüngel und die Kritik am Stil einzelner Personen haben damals ihre Wirkung gehabt. Die Arbeit des CCCs wurde behindert. Die anfängliche Medienarbeit hat ein Bild der Öffentlichkeit über den CCC erzeugt, mit den wir heute Leben müßen. Es ist vielleicht sinnvoll, sich über Fehler und Verantwortung in der Vergangenheit zu unterhalten. Aber für unsere heutige Arbeit hat zu gelten, daß wir erstmal mit diesem Status/Zustand leben müßen und demnach agieren sollten.

Bis heute steht die Aussage: „Wenn in der Welt ein Bit umkippt, klingeln beim CCC die Telefone". Häufig genug merken wir das. Es ist für die interessierten Kreise heute kaum noch zu bezweifeln, daß es zum gezielten Einsatz von Viren, Würmern, elektr. Bomben, Systemeinbrüchen, etc gegen Technik zur Durchsetzung von Gruppenzielen kommen wird. Themen wie Viren, Würmer, Hacker, etc führen auch heute zum Griff in die Schublade „CCC". Wenn wir damit rechnen müßen, daß der Techno-Terrorismus kommt, dann müßen wir darüber reden und das Thema nicht totschweigen oder durch Begriffsänderungen verwässern. Und wenn der Begriff „Techno-Terrorismus" aus der VS-Ecke kommt, dann ist das zwar ein Problem aber kann auch ignoriert werden. Die - ebenfalls anscheinend ohne Probleme - verwendeten Begriffe wie Widerstandswissen oder Technologiefolgenabschätzung kommen aus anderen Ecken und sind dadurch nicht minder vorbelastet. Trotzden sollten wir uns trauen die Begriffe zu verwenden, weil sie in Gegendwart und Zukunft verwendet werden. Eine offene Diskussion, die klare Stellungnahme, ist eine Vorraussetzung dafür, daß wir bei diesem Thema nicht schon wieder nur reagieren müßen und dadurch nie jemand geholfen haben, sondern das wir im Vorfeld agieren - und wenn es nur dadurch geschieht, daß wir darüber reden und die verschiedenen möglichen Argumente und Sichtweisen zu hören.

Ein „Verbot" dieses Thema gab es nicht. Aber Aussagen wie: „Bei dem Thema sitze ich nicht auf dem Podium" oder Kurzbeiträge in der Vorbereitung der letzten beiden Congresse haben durch die Person, die sie bringt einen gewissen Einfluß, die einer sachliche Diskussion zuwiderläuft. Da muß sich auch jede(r) seine(r) persönlichen Verantwortung bewußt sein.

Wie auch gesagt wurde: „Wir müßen durch das Thema Techno-Terrorismus durch". Wir sollten nur selbst entscheiden, wann wir durch müßen und das nicht von außen aufdrücken lassen. Auch wenn viele die Diskussion auf dem Congress nur mittelmäßig fanden und am Thema teilweise vorbeilief: Es ist ein Erfolg, daß wir angefangen haben.

terra

DUTCH POLICE ARRESTS HACKERS

The facts

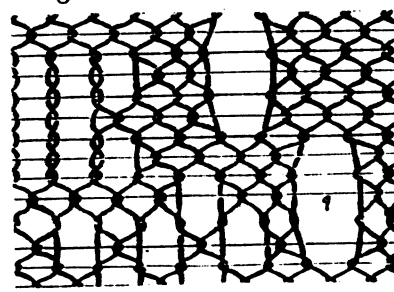
At 10.30 in the morning of monday the 27th of January 1992 Dutch police searched the homes of two hackers. In the city of Roermond, the parental home of the 21-year old student H.W. was searched and in Nuenen the same happened to the parental home of R.N., a Computer Science engineer, age 25. Both were arrested and taken into custody. At both sites, members of the Amsterdam Police Pilot Team for computer crime were present, alongside local police officers and representatives of the national organisation CRI (Criminal Investigations Agency). Both suspects were transported to Amsterdam. The brother of one of the suspects was told the suspects could receive no visits or mail. All of this has happened more than one week ago and the two are still in jail as we write this.

The charges

A break-in supposedly occured at the bronto.geo.vu.nl site at the VU University in Amsterdam. This UNIX system running on a SUN station (IP 130.37.64.3) has been taken off the net at least for the duration of the investigation. What happened to the actual hardware is unknown at this time.

The formal charges are: forgery, racketeering and vandalism. The police justifies the forgery part by claiming that files on the system have been changed. The vandalism charge is valid because the system had to be taken off the net for a period of time to investigate the extent of the damage. By pretending to be regular users or even system management the hackers committed racketeering, the police says.

Both suspects, according to the Dutch police, have made a full statement. According to a police spokesman the motive was „fanatical hobbyism". Spokesperson Slort for the CRI speakes of the „kick of seeing how far you can get".



„Damages"

According to J. Renkema, head of the geophysics faculty at the VU, the university is considering filing a civil lawsuit against the suspects. „The system was contaminated because of their doing and had to be cleaned out. This cost months of labour and 50.000 guilders (about US$ 30,000). Registered users pay for access to the system and these hackers did not. Result: tens of thousands of guilders in damages." Renkema also speaks of a „moral disadvantage": The university lost trust from other sites on the network. Renkema claims the university runs the risk of being expelled from some networks.

Renkema also claims the hackers were discovered almost immediately after the break-in and were monitored at all times. This means all the damages had occured under the watchful eyes of the supervisors. All this time, no action was taken to kick the hackers off the system. According to Renkema all systems at the VU were protected according to guidelines as laid down by CERT and SurfNet BV (SurfNet is the company that runs most of the inter-university data-traffic in The Netherlands).

What really happened?

The charge of „adapting system-software" could mean that the hackers installed back-doors to secure access to the system or to the root level, even if passwords were changed. New versions of telnet, ftp, rlogin and other programs could have been compiled to log access to the networks.

What really happened is anybody's guess. One point is that even the CRI acknowledges that there were no „bad" intentions on the part of the hackers. They were there to look around and play with the networks.

About hacking in general

In the past we have warned that new laws against computer crime can only be used against hackers which are harmless. Against the real computer criminals a law is useless because they will probably remain untraceable. The CRI regularly goes on the record to say that hackers are not the top priority in computer crime investigation. It seems that hackers are an easy target when 'something has to be done'.

And „something had to be done": The pressure from especially the U.S. to do something about the „hacking problem" was so huge that it would have been almost humiliating for the Dutch not to respond. It seems as if the arrests are mainly meant to ease the American fear of the overseas hacker-paradise.

A closer look at the charges and damages

The VU has launched the idea that system security on their system was only needed because of these two hackers. All costs made in relation to system security are billed to the two people that just happened to get in. For people that like to see hacking in terms of analogies: It is like walking into a building full of students, fooling around and then getting the bill for the new alarm-system that they had to install just for you.

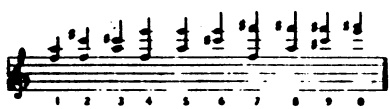
Systems security is a normal part of the daily task of every system- adminstrator. Not just because the system has to be protected from break-ins from the outside, but also because the users themselves need to be protected from each other. The 'bronto' management has neglected some of their duties, and now they still have to secure their system. This is not damages done, it's work long overdue.

If restoring back-ups costs tens of thousands of guilders, something is terribly wrong at the VU. Every system manager that uses a legal copy of the operating system has a distribution version within easy reach.

„Month of tedious labour following the hackers around in the system". It would have been much easier and cheaper to deny the hackers access to the system directly after they had been discovered. „Moral damages" by break-ins in other systems would have been small. The VU chose to call the police and trace the hackers. The costs of such an operation cannot be billed to the hackers.

Using forgery and racketeering makes one wonder if the OvJ (the District Attorney here) can come up with a better motive than „they did it for kicks". If there is no monetary or material gain involved, it is questionable at best if these allegations will stand up in court.

As far as the vandalism goes: there have been numrous cases of system management overreacting in a case like this. A well trained system-manager can protect a system without making it inaccesible to normal users. Again: the hackers have to pay for the apparent incompetence of system management.



This does not mean that having hackers on your system can not be a pain. The Internet is a public network and if you cannot protect a system, you should not be on it. This is not just our statement, it is the written policy of many networking organisations. One more metaphore: It's like installing a new phone-switch that allows direct dial to all employees. If you get such a system, you will need to tell your employees not to be overly loose-lipped to strangers. It is not the callers fault if some people can be „hacked". If you tie a cord to the lock and hang it out the mail-slot, people will pull it. If these people do damages, you should prosecute them, but not for the costs of walking after them and doing your security right.

Consequences of a conviction

If these suspects are convicted, the VU makes a good chance of winning the civil case. Furthermore, this case is of interest to all other hackers in Holland. Their hobby is suddenly a crime and many hackers will cease to hack. Others will go „underground", which is not beneficial to the positive interaction between hackers and system management or the relative openness in the Dutch computer security world.

„Our system is perfectly secure !"

(and if you prove it's not,

we'll have you put in jail)

übernommen von der HACKTIC

Informatik & Ethik

Teilnehmer:
Prof. Schefe, Uni Hamburg
Kai Rennberg, TU Berlin (FB Informatik), Gesellschaft für Informatik
Frank Möller, Student Uni Hamburg, Politologie

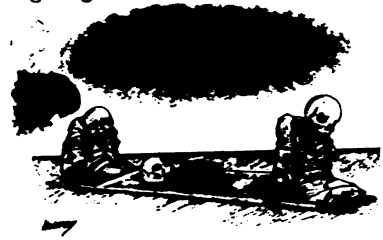
Vortrag von Kai Rennberg

Mögliche Konfliktfelder der Informatik und Ethik:
- Rationalisierung („Jobkiller Computer")
- Arbeitsplatzgestaltung („Verdummung der User")
- Mensch und Computer („Computerisierung der User")
- Informatik und Militär („Kriegsförderung durch Informatik")
- Inviduum und Staat („Datenschutz")

Welche Organisationen betätigen sich schon auf diesem Gebiet? Die „IFIP" (International Federation for Informatik Processing) auf internationalem Gebiet, die „CEPIS" (Council European Professional Infomatik Society) auf europäischem Gebiet sowie die GI (Gesellschaft für Informatik) in Deutschland. Von diesem Organisationen wurden schon verschiedenlich Versuche unternommen, so etwas wie „die zehn Gebote" für Informatiker zu formulieren. Bsp. 89/90 „ethischer Code", IFIP; „Informatik & Verantwortung", GI.

Herausgestellt hat sich aber, daß diese Papiere aufgrund der Anzahl der daran Beteiligten immer nur Minimallösungen sein können. Einig war man sich darüber, daß die Informatik als Wissenschaft nur Werkzeug der Informationsverarbeitung, nicht Selbstzweck sein darf.

Weiterhin existiert ein „Ampelpapier" auf dem man -im grünen Bereich- festgehalten hat, was man tun sollte, und im roten, was auf keinen Fall. Im größten Bereich, im gelben, stehen die Sachen, die man noch nicht endgültig beurteilen kann.



Vortrag von Prof. Schefe

Sollte es einen ethischen Code für den Informatiker geben?

Nein, denn: Ein Regelcode würde bisheriges Verhalten der Informatiker bestätigen, nur innerhalb ihrer (Fach-)Disziplin kompetent zu sein und weiterhin kein Blick für Folgen in der Gesellschaft zu haben. Zur weiteren Ausführung die Klärung des Moralbegriffes: „Beschränkung eigener Aktivität zur Wahrung der Interessen anderer." Moral ist heute wichtiger denn je, da die Möglichkeiten des eigenen Handelns auf Grund technischer Möglichkeiten immer größer werden, wobei die Folgen immer weniger absehbar bleiben. Die Gesellschaft hat sich in einen „Technischen Galopp" (Jonas) [*hoppe, hoppe, der schreiter*] begeben, in dem der Techniker nicht noch zusätzlich für sein Handeln die Folgen überblicken kann.

Immer globalere Strukturen der Information und der Kommunikation bringen positive (z.B. Unterstützung der Putschgegner in der UdSSR) und negative Folgen (Zunahme des Verkehr mit allen ökologoschen Konsequenzen) mit sich, alle Vorgänge werde komplexer und damit unüberschaubarer („organisierte Unverantwortlichkeit"). Aus dieser Beschreibung kann sich nur die Forderung nach Erweiterung des Horizonts der Informatiker in Hinblick auf die Gesellschaft ergeben, die nicht in einen möglichen Ethikcode für eine Berufsschicht (eben den Informatiker) pressen lassen. Zudem sollte Ethik allgemein gültig sein. Diese Forderung wiederum führte zu einer Abschaffung des Informatikberufes, wie er bisher bekannt ist.

Inhalt der anschliessenden Diskussion

In jedem Falle gibt es keinen weltweit gültigen Ethikcode, zu unterschiedlich sind die Kulturen. Eine Ethik sollte auch allgemein gültig bleiben. Die „zehn Gebote" dürften in jedem Falle nur Diskussiongrundlage bleiben, kein Standardwerk. Allerdings wäre ein Handbuch fuer die Praxis immerhin ein Fortschritt gegenüber der bisherigen Situation. Außerdem besteht die Möglichkeit, daß andere (z.B. der Staat gesetzgebend) regulativ eingreifen, was zumindest schlechter ausfallen könnte.

alex

Protokolliert, gefangen und verurteilt!

Erläuterungen zur Auswertung von Btx-Sessions durch die DBP-Telekom.

Das Knacken und Ausspähen, sowie die Fremdbenutzung von Btx- Teilnehmerkennungen scheint immer noch ein verbreitetes Hobby einiger Btx-Freaks zu sein. Besonders betroffen und geschädigt werden durch derartige Aktivitaeten in erster Linie die Dialog-Dienst-Anbieter. Bei den Inhabern mißbrauchter Btx-Kennungen summieren sich zeitweise Kosten bis zu 6000,- DM monatlich!

Kürzlich verhandelte das Amtsgericht Berlin-Tiergarten einige solcher Fälle. Verhängt wurden dabei Geldstrafen zwischen 700,- und 1600,- DM. Offengelegt wurden in der Verhandlung auch die derzeitigen Protokollmöglichkeiten der DBP-Telekom.

Bei jeder Verbindung zur Btx-Zentrale werden während der Sitzung mehrere Datensätze angelegt. Insgesamt werden sieben wesentliche Faktoren je Datensatz festgehalten.

IN SPALTE 1 wird die Btx-Vermittlungsstelle protokolliert, über die die betreffende Btx-Sitzung durchgeführt wurde. Hierbei wird der Standort der Vermittlungsstelle mit der Postleitzahl des Ortes festgehalten. Dieses ermöglicht auch eine Fangschaltung im betreffenden Ortsnetz - jedoch noch manuell.

IN SPALTE 2 werden Rechnernummer und Zugangsport aufgezeichnet. Diese Daten werden dem Btx-Teilnehmer übrigens „verdeckt" beim Verbindungsaufbau auf der Identifizierungsseite (oberste Zeile) in der Reihenfolge: Rechnernummer, Zugangsport, Anschlußnummer und Zugangsseite angezeigt. Es kann zeitgleich immer nur eine Verbindung über einen bestimmten Port durchgeführt werden. Anhand der Portnummer sollte sich auch die Übertragungsgeschwindigkeit ermitteln lassen.

IN SPALTE 3 verzeichnet die Post die Sitzungsart. Innerhalb einer Btx-Sitzung können hierzu mehrere Datensätze angelegt werden. Definiert sind:

SE; der Sitzungs-Endesatz der gesamten Sitzung mit der Angabe der Zeitdauer der Gesamt-Sitzung.

Die Beweislast dieser Protokolle ist gerichtlich noch nicht abschließend geklärt. Zwar behauptet die DBP-Telekom durch diese Protokolle den Beweis zu erbringen, welcher Btx-Teilnehmer mit seiner eigenen Anschlußkennung fremde freizügig deklarierte Teilnehmer mißbrauchte. Besonders wenn dieses von einer DBT-03 Anschlußbox aus erfolgte.

ER; jeweils eine Externe-Rechner-Session, je kostenpflichtiger Nutzung eines externen Rechners. Bei Nutzung mehrerer externer Rechner wird jede ER-Nutzung einzeln abgeschlossen und verzeichnet.

EG; der Entgeltsatz der innerhalb einer Btx-Sitzung erzeugt wurde. Je Anbieter, bei dem Kosten verursacht wurden, kann ein eigener Datensatz erzeugt werden. Diese Daten sind auch Grundlage der Anbieterabrechnungen.

IN SPALTE 4 wird die Btx-Teilnehmernummer einschließlich des Mitbenutzer-Suffix registriert, zu dessen Lasten die Verbindung aufgebaut wurde.

IN SPALTE 5 wird die system-interne Teilnehmer-Nummer festgehalten. Diese dient der Zuordnung der im System auflaufenden Datensätze, sie ist extern ohne Bedeutung.

IN SPALTE 6 dokumentiert die Post die Anschlußnummer über welche die Verbindung aufgebaut wurde. Die Anschlußnummer wird ebenso auf der Seite *74# und auf jeder Zugangsseite in der ersten Zeile (neben anderen schon erwähnten Daten) verdeckt angezeigt. Über die Anschlußnummer lässt sich die genutzte Anschlußkennung ermitteln. Die aufgezeigte Anschlußnummer ist von Spalte 4 immer abweichend, wenn im Falle der Freizügigkeit über fremde Anschlüße Btx-Verkehr abgewickelt wird. Ferner wird in dieser Spalte festgehalten, welche Leitseiten abgerufen und welche Entgeltsätze (als Summe) dabei erzeugt wurden.

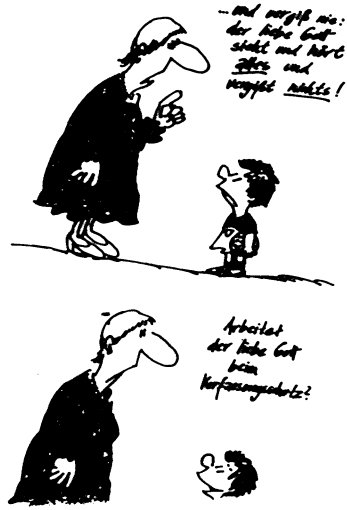
IN SPALTE 7 erfolgt die Speicherung der Zeitdauer der einzelnen Sitzungen. Werden mehrere Datensätze (siehe Spalte 3) angelegt, wird jeder einzeln mit der Zeitdauer festgehalten. Die Speicherung erfolgt in der Reihenfolge ihres Abschlußes. Es lassen sich somit die Daten mehrerer zeitgleicher Sitzungen unter einer Teilnehmernummer immer jeder einzelnen Verbindung zuordnen.

Es sollte davon ausgegangen werden, daß auch fehlerhafte und falsche Verbindungsaufbauten (z.B. zu nicht freizügig deklarierten Teilnehmern) verzeichnet werden.

Die Anschlußkennungen aus DBT-03 Anschlußboxen werden in einem anderen Datenformat (7e1, stat 8n1) innerhalb eines Zeitfensters übertragen. Dieses läßt sich jedoch mit einem seit Jahren verbreiteten PD-Decoder simulieren. Btx-Freaks, welche sich auf diesem Wege zum Beispiel als „öffentliches Btx-Gerät" identifizieren, sparen so die Gebühren für den Mitteilungsdienst (Strafbar!).

Diese Beweisform der DBP-Telekom führte in der Vergangenheit sogar dazu, daß gegen Btx-Teilnehmer Durchsuchungsbeschlüße erwirkt wurden, deren Anschlußkennungen ausgespäht oder sogar freiwillig an Btx- Agenturen weitergegeben wurden! Es empfiehlt sich daher, sich die Weitergabe der Anschlußkennung (auch an Btx-Agenturen) quittieren zu lassen.

Das nun in den jüngsten Gerichtsverfahren teilweise eindeutige Urteile zustande kamen, hat einen weiteren Hintergrund. Nachdem ein Teilnehmer die „Fremdbenutzung" seines Anschlußes bemerkte, wurde dieser aus dem Btx-System gelöscht. Nach einigen Tagen wurde jedoch festgestellt, daß unter der gelöschten Kennung immer noch eine Btx-Verbindung aktiv war und weiterhin Datensätze protokolliert wurden. Daraufhin wurde eine Fangschaltung veranlaßt. Ergo sum: Wer sich 13 Tage ununterbrochen unter einer fremden Kennung im Btx-System aufhält, ist selber schuld(ig)!



Den Btx-Teilnehmern sei empfohlen, die von der DBP-Telekom im Btx- System erläuterten „Sicherheitshinweise" (*10414114013#) ernsthaft zu studieren. Noch immer geben Btx-Teilnehmer auf von Btx-Anbietern simulierten Passwortabfragen freiwillig ihre Daten preis. Selbst das Kennwort eines Landeskriminalamtes gelangte so in fremde Hände.

NETZWERKER//CCC-Btx-Redaktion//LS23

S. Wernery

Kinder des Donners

Vom Autor des Schockwellenreiter, John Brunner, ist ein neues Buch erschienen. „Kinder des Donners" heißt es und ist bei Heyne als SF4683 für 1480 Pfg erhältlich.

Wem das als Empfehlung noch nicht genügt, dem sei gesagt, daß der Herausgeber Wolfgang Jeschke ist. Und der ist auch gut. Nach den 511 Seiten Roman kommt noch ein Nachwort von Ernst Petz. „Ich wünschte", erklärte John Brunner einmal, „ich würde nicht so viele Menschen kennen, die nicht begreifen wollen, wie wichtig es ist, an der Zukunft interessiert zu sein. Schließlich werden wir dort den Rest des Lebens verbringen!" beginnt EP und verweist auf das ahnbare, vorhersehbare Morgen, wo sich die Menschheit weiter treiben läßt von Geschäftemachern, korrupten Führern, einer feilen Presse, mittelalterlich-restaurativer Borniertheit, hochbezahltem, nicht mehr abwählbarem Großgaunertum.

Die endlose Wiederholung der Geschichte Brunnerscher Welten beschreibt EP so:

Aus Bücklingsregierungen werden solche „Revolutionärer Parteien", aus diesen die Regierungsform, die nur dank „öffentlicher Apathie" überlebt - wem diese vertraut vorkommt, der irrt sich nicht.

Im ersten Stadium ist ein Arbeitsplatz Glückssache, im zweiten staatlich gelenkt, im dritten gibt es individuelle Arbeitsverträge - der Mensch ist endlich freier als frei: vogelfrei.

Informiert wird die Bevölkerung im ersten Stadium auf Amateurbasis, im zweiten durch Nachrichtenagenturen der Regierung und schließlich zuletzt vermittels „durch Vetternwirtschaft und politische Trägheit verkommene Sprachrohre" der Führung. Psychodelika sind zuerst unerschwinglich, dann nachdrücklich bekämpft - und schließlich toleriert: es wird wünschenswert, daß sich die Untertanen zufrieden aus der Wirklichkeit des Big Business wegträumen, daß sie ihr zutiefst deprimierendes Sein nicht mehr empfinden.

Soweit aus dem Nachwort, das wegen der geplanten Einführung der Steuerpflicht für THC-Produkte aktuell ist. Denn viele Kiffer sind nicht an der dumpfen Nutzung der verschiedensten Hanfpflanzenteile interessiert, sondern an wachem Leben. Wer Denkanstöße haben will gegen die heutige Drogenwelt von staatlich genehmen Betörungsmitteln, sollte das Buch lesen. Für den schnellen Lesetest hier Seitenzahlen mit Stichworten, wie ich sie im Buch notiert habe: Senderoulett am Knopf der Fernseherfernbedienung: 36, Bildschirmjunkmail: 37, Jesuiten - Kinder: 246, Atompest: 317, polizeiliches Wertebewußtsein: 320, Tut-mir-Leid-Unfug: 371, Affenliebe: 397, Stempel: 402, Gratis-Rechtsbeistand berufswidrig: 408, Schwarz-Schillings Alterssitz in Kanada: 422, Gotteskrieg: 439 und Fahrgastrationierung auf Seite 469. Weil ich es schätze, wenn Autoren bestimmte Dinge kurz und knapp formulieren und sowas schnell wiederfinden will, schreibe ich mir so einen Kurzindex in mir wichtige Bücher.

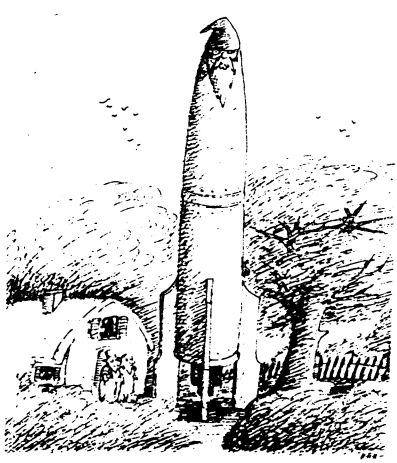
„Kinder des Donners" ist ein mir wichtiges Buch.

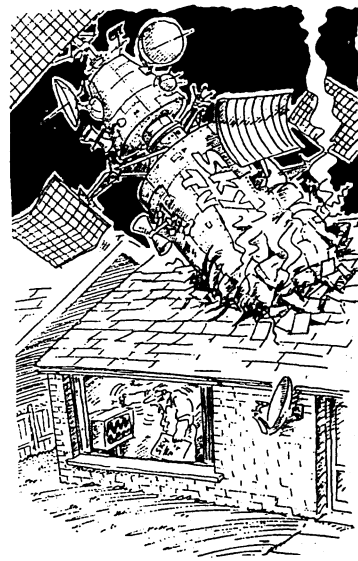
wau

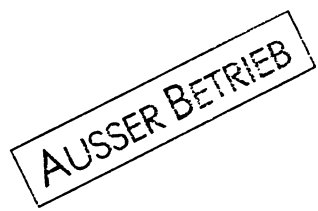
Dr. Wau's Sammelsorium

Ariane Panne Nummer 5

In Kourou, dem französischen Kolonialgebiet am Satellitenäquator, passierte wieder eine Panne. Kourou, wo Frankreich früher Gefangene hielt, ist wegen der Bedeutung als Raketenstartplatz besser gesichert als einst die Berliner Mauer. Trotzdem gab es einen weichen Fehler bei den 26 Meter langen Feststoff-Hilfsraketen. Dabei wird in 10 Meter lange Rohre eine zähflüssige Treibstoffmasse gefüllt, die mit einem Härter versehen wird. Davon wurde nicht genug zugegeben und die Suppe blieb weich. Deshalb verschiebt sich der für März 1992 vorgesehene Test der Feststoff-Hilfsraketen um mehr als ein halbes Jahr. So ein komplexes Projekt durchzuziehen, ist nicht einfach. Ein andermal wurde ein Stofflappen, der zur Reinigung gedacht war, in der Ariane vergessen. Das ist sowas ähnliches wie eine bei einer Operation im Bauch vergessenen Zange eines Arztes. Insgesamt ist die Zuverlässigkeit von Arianes jedoch recht hoch.







Wanderfeldröhren

Als beim Satellit OLYMPUS eine Wanderfeldröhre den Geist aufgab, wurde auf die Ersatzröhre umgeschaltet. Das geschah im Oktober 1989. Nun wird eine Fernheilung der Ersatzröhre versucht, weil die auch nicht mehr will.

Auch bei Intelsat VI-FI spukt eine Wanderfeldröhre. Nach dem Start am 29.11.91 bemerkten Techniker Störungen des Spotbeams. Ursache scheint ein lockeres Metallteilchen in der Röhre zu sein. Die Leitstelle will nun durch Beschleunigung und Abbremsen des Satelliten das Klappern beseitigen.

ariane.tex wau

CHAOS-HH - CCC Hamburg
Treffen jeden Dienstag ab 19 Uhr.
Mailbox CHAOS-HH unter 040 / 491 10 85
Voice: 040 / 490 37 57
Fax: 040 / 491 76 89
Briefpost: CCC-HH, Schwenckestraße 85, 2000 Hamburg 20

CHAOS-HL - CCC Lübeck
Treffen am ersten und dritten Freitag im Monat, 19 Uhr in der Röhre (gerade von der Mengstraße ab).
Mailbox CCC-HL unter 0451 / 316 42
Voice: 0451 / 86 55 71
Briefpost: CCC-HL, Lachswehrallee 31, 2400 Lübeck

CHAOS-RH - CCC Recklinghausen
Treffen alle zwei Wochen oder so.
Voice: 02364 / 163 49
Fax: 02361 / 65 27 44
Mailbox: LITB unter 02363 / 663 78 und LIVETIMES unter 02361 / 37 32 14

CHAOS-RM - CCC Rhein-Main
Treffen finden statt oder auch nicht
Voice: 06103 / 41 00
Mailbox BITMAIL vielleicht unter 06103 / 452 87
Briefpost: CCC-RM, c/o E.Engelter, Postfach 1201, 6073 Egelsbach

SUECRATES - Stuttgarter Computerrunde mit Zeitschrift D'Hacketse
Garantiert keine Satzungsdebatten - Mitglied im Bundesverband gegen Vereinsmeierei e.V.
Kontakt: T. Schuster, Im Feuerhapt 19, 7024 Filderstadt 3
E-Mail: norman@delos.stgt.sub.org

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

Hack-Tic
P.B. 22953
NL-1100 D1 Amsterdam
Voice: +31-20-6001480
Fax:+31-20-6900968

CHAOS-RN - CCC Rhein Neckar
Treffen jeden Dienstag 20 Uhr im "Vater Rhein" in HD.
Wegbeschreibung von der Stadthalle: "Gehe über die Fußgängerampel. Gehe nicht über LOS. Durchquere den Minipark. Gehe halb links. Jetzt stehst Du davor. Begib Dich in den linken Flügel der Gaststätte. Hinten rechts siehst Du einen Haufen Leute mit Schlepptops, Funkgeräten und ähnlichem Kram. Das sind wir. Trau Dich zu fragen, wir beißen nicht. (Nur farg nicht, ob wir verrückt sind, Du könntest eine Antwort bekommen...)"
Mailbox CHAOS-RN unter 06221 / 90 47 27
Briefpost: CCC-RN, Postfach 10 40 27, 6900 Heidelberg

FoeBuD-BI - Verein zur Förderung des öffendlichen bewegten und unbewegten Datenverkehrs e.V., Bielefeld
Treffen jeden Dienstag, 19 Uhr im Cafè "Spinnerei", Heeperstraße 64.
Monatliche "Public Domain" Veranstaltung jew. am 1.Sonntag im Monat, im Bunker Ulmenwall, Kreuzstraße 0, 4800 Bielefeld 1. Termine siehe BIONIC.
Voice: 05211 / 752 54
Mailbox BIONIC unter 05211 / 711 88
Briefpost: FoeBuD, c/o Art de Ameublement, Marktstraße 18, 4800 Bielefeld 1

CCC-Ulm
Treffen jeden Mittwoch, 19.00 Uhr im Cafè "Einstein", Uni-ULm
Kontakt: Framstag, framstag@rz.uni-ulm.de (Ulli Horlacher, Landfiedbühl 5, 7900 Ulm) und Deep Thought, brenner@tat.physik.uni-tübingen. de (Martin Brenner) oder CCC-Ulm, ccc-ulm@sol.zer und ccc-ulm@sol.north.de

Chaos Bestellfetzen

Chaos Computer Club

Schwenckestraße 85
D-2000 Hamburg 20
Tel : 040 / 490 37 57
Fax: 040 / 491 76 89
Box: 040 / 491 10 85
Postgiro Hamburg
(BLZ 200 100 20)
Konto 59 90 90 - 201

Postvertriebsstück, Gebühr bezahlt - C 11301 F

Name:

Adresse:

Mitgliedschaft im CCC e.V. - Schließt Datenschleuder-Abo mit ein.

____	*evvw*	20,00 DM	Einmalige Verwaltungsgebühr bei Eintritt
____	*evnm*	120,00 DM	Normalmitgliedschaft (Jahresbeitrag)
____	*evsoz*	60,00 DM	Sozialmitgliedschaft für Studenten, Schüler, Arbeitslose etc. (Jahresbeitrag)

Reine Datenschleuder Abos - Ein Abo gilt für 8 Ausgaben.

____	*nabo*	60,00 DM	Normalabo der Datenschleuder
____	*sabo*	30,00 DM	Sozialabo der Datenschleuder s.o.

Chaos-Literatur (auch im Buchhandel erhältlich)

____	*habi1*	33,33 DM	Die Hackerbibel, Teil 1 (260 Seiten A4)
vergriffen	*habi2*	33,33 DM	Die Hackerbibel, Teil 2 (260 Seiten A4)
____	*wund*	28,00 DM	Das Chaos Computer Buch (250 Seiten A5)
vergriffen	*mosk*	26,00 DM	Hacker für Moskau (unzensierte 1. Auflage)

Chaos-Literatur (im Buchhandel eher nicht erhältlich)

____	*stud*	7,50 DM	Studie für die Grünen über politischen Computereinsatz im Bundestag -- und überhaupt
____	*mutst*	10,00 DM	Mensch-Umwelt-Technik Studie: Elektronische Informationssysteme für den Umweltschutz
____	*kamj*	10,00 DM	Der elektronische Kammerjäger / Über Wanzen, Abhörmethoden und Erkennung derselben
____	*doku*	5,00 DM	Dokumentation zum Tode von Hagbard (Karl Koch)
____	*frnk*	7,50 DM	Perspektiven einer neuen Kommunikationsmoral für das Zeitalter der Kybernetik, von Prof. G. Frank

Infopakete / Software / Hardware & Co. - Diskettenformat angeben !

____	*vir*	25,00 DM	Infopaket Computerviren (inkl. MS-DOS Demovirus)
____	*pcd*	25,00 DM	PC-DES für MS-DOS: Private Verschlüsselung von (Text-) Dateien Gewerbliche Version bei BrainON!
in arbeit	*ts-plan*	10,00 DM	"Taschen-Synthi", Schaltplan und ASM-Listing / Dokumentation
____	*pc-syn*	20,00 DM	"PC-Synthi" für blaue Töne, Schaltplan, Quälcode, Dokumentation

Aufkleber PVC, wassergeschützt / gestanzt, wenn nicht anders angegeben.

____	*3ks*	3,33 DM	3 Stück "Kabelsalat ist gesund" mit Chaos-Knoten
____	*ah*	3,33 DM	Bogen mit 64 Stück "Achtung Abhörgefahr", Papier, zum Selbstausschneiden, postgelb
____	*ooo*	5,00 DM	Bogen mit 18 x "Außer Betrieb", 8 x "Out of Order" und 1 x "Guasto"
____	*post*	5,00 DM	Bogen mit Post-Totenkopf-Klebern in versch. Größe
____	*zula*	5,00 DM	Bogen Zulassungszeichen zum Fummeln, wie Muster

Ganz Wichtig: gedenkt unserer irren Portokosten! Mindestens Rückporto !!

____	*pvst*	??,?? DM	Porto / Verpackung / Spende / Trinkgeld / "Haste mal ne Mark?"

Summe: DM ____.__ ◯ bar ◯ V-Scheck ◯ Überweisung

Chaos E BE ERL