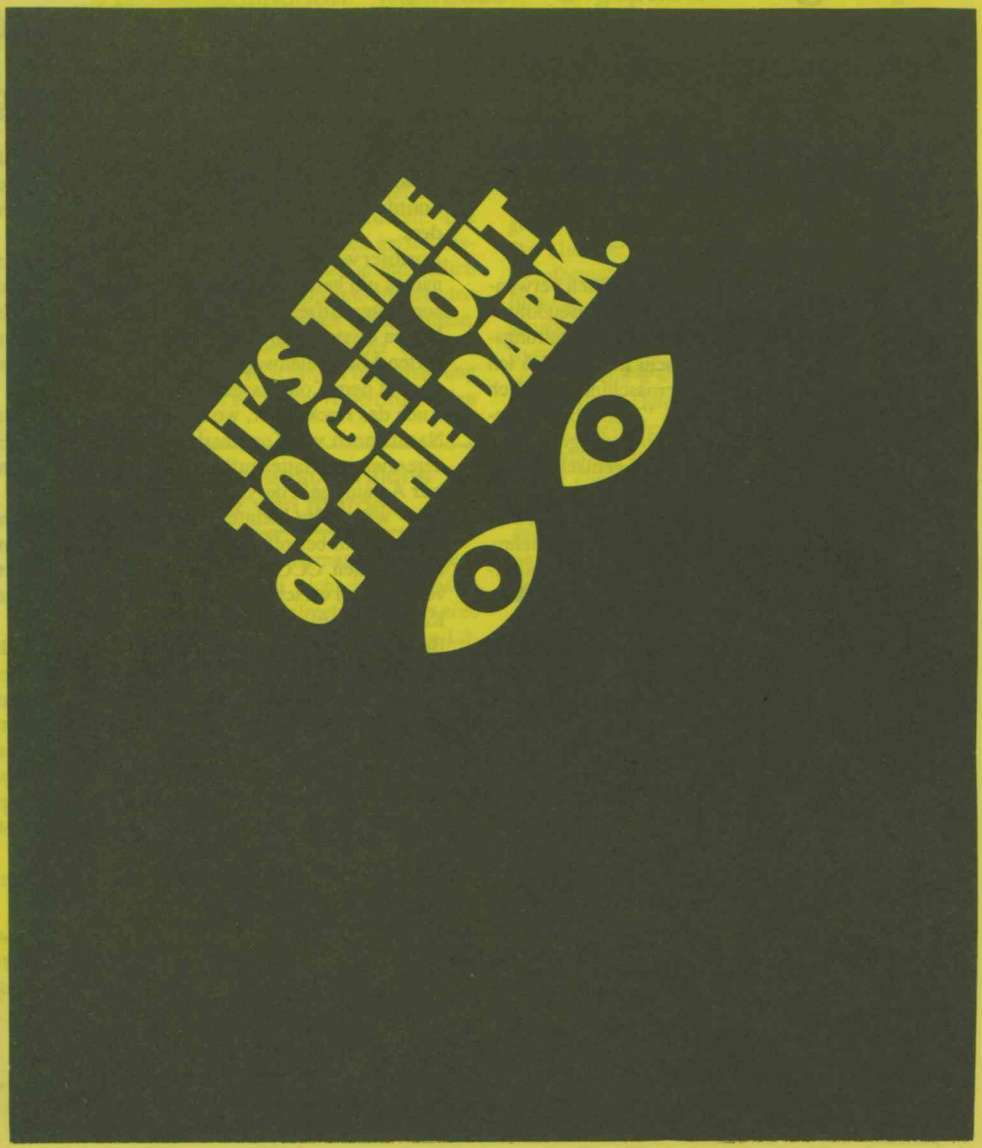
DM 3,00

Nummer 25 | Mærz 1988

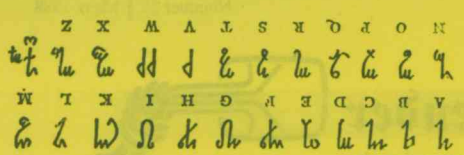
Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende

Ein Organ des Chaos Computer Club



~~Der~~/ Die Beschuldigte ist / ~~xxx~~ aufgrund der bisherigen Ermittlungen verdächtig,
anderen geholfen zu haben.



Congräßlich

Den Hackern sind die Nächte lang

Congress Critic

Hacker im Beamtenstatus?

Hallo CCC'ler. Ich bin nun schon seit zwei Tagen auf'm CCCongress. Und was fällt mir auf? Die Sprache.

Diese Sprache, die hier fast ausschließlich verwendet wird, stößt mir sauer auf. Nur noch pseudojuristische Spitzfindigkeiten und Verwaltungs-Sprachgehabe. Selbst wenn Uschi möchte, daß ich ihr beim Umstellen der Kaffeemaschine behilflich bin, faselt sie irgendetwas von 'Zuständigkeitsbereich' und von 'Projektleitung'. Nichts gegen Uschi. Auf ihr Sprachgebaren aufmerksam gemacht, meinte sie, daß sie sich halt anpasse.

Der CCC als Schulungsorganisation für Verwaltungsabläufe? Sicherlich ist es ganz angenehm, wenn einige Sachen geklärt sind und ein Mindestmaß an Handshake-Protokoll gewährleistet ist. Aber was zuviel ist ist zuviel!

Es gab wohl bereits intern eine Menge an Diskussion über das verzweifelte Bemühen, das Chaos in den Griff zu kriegen. Fein. Aber was hier auf dem CCCongress am Rande der 'galaktischen Vereinigung ohne feste Strukturen' als Ordnungsstruktur mitläuft, ist nicht neu, sondern uralt. Ich bemerke tiefprovinzielle, urdeutsche Rotes Kreuz- und freiwillige Feuerwehr-Allüren.

Sicher ist es schön, die Infrastrukturen von o.g. Diensten mitbenutzen zu können. Aber lassen wir bitte den Verwaltungs- oder gar Kasernenton weg. 'Wir Proleten' werden nicht dadurch salonfähig, daß wir geschraubt schwafeln. Das wirkt so peinlich wie Frau Dr. Elisabeth Müller-Mayer im Kleinen Schwarzen.

Lieber ungewaschen als parfümiert. Denn blöde Computerclubs gibt's schon genug.

padeluun

Hamburg (ccc) - Nach wortgewaltigen Strukturdebatten über nächtliche Kongressaktivitäten konnte der Hausfrieden wiederhergestellt werden.

Auslöser war die resolute Räumung des Hackcenters nachts um halb drei. Die nächtliche Schichtleitung sorgte gewaltfrei und resolut mit Unterstützung der letzten Gäste für die Einhaltung der vorher vereinbarten Maximalanwesenheitsquote von vier Personen auf dem Kongressgelände.

Auch das Hackcenter, wo aus aktuellem Anlaß des Nachts noch vor Kongressbeginn eine unangemeldete wichtige Plattenaufbauaktion stattfinden sollte, war Anlaufpunkt der Schichtleitung.

Mit - wie einige meinten - berechtigter Empörung reagierte ein betroffener Hacker: er warf seine von ihm für den CCC87 mitentworfene Eintrittskarte von sich und verschwand im Dunkel der Nacht. Zum Kongress ward er nicht mehr gesehen.

Beinahe wäre auch die Nachtaufsicht des Hackcenters von der rigiden Quotenregelung betroffen worden. Ursache dieser nächtlichen Beschränkungen waren verschiedene nicht druckreife Erfahrungen in den Kongressnächten des Vorjahres. In einer längeren Organisationsdebatte über Chaos und Hamburger Preussentum wurden auch andere empfindliche Stellen der Kongressorganisation getroffen.

Zwar wurde die Festlegung genau eines resoluten Nacht-Verantwortlichen allgemein akzeptiert, *sefehler Diskette..)* *(..Le-*

Der Vorschlag für das weitere Vorgehen: Außer notwendigen festgelegten Verantwortungen mehr konstruktive Anarchie.

wau

CCC'87/CCCONGRESS/PRESSESTELLE/28.12.87/07:52

BKA macht mobil

Nach kurzer Pause weitere Durchsuchungen in der Hackerszene

Beamte des BKA haben sich erneut in die praktische Ausbildung begeben. Am Dienstag Morgen gegen sechs wurden drei Hacker unsanft aus dem wohlverdienten Schlaf gerissen. Mitarbeiter des BKA luden sich zum morgentlichen Kaffee ein und durchsuchten alles was irgendwie nach Technik aussah.

Die jüngsten Ermittlungen beziehen sich auf ein Telefonbüchlein, daß bei vorherigen Durchsuchungen im November in den Räumen des CCC beschlagnahmt wurde.

Nach BKA-Angaben hat ein Hacker am 20. November 1986 eine `Datenunterhaltung` mit dem für die Systempflege verantwortlichen Systemmanager geführt. Danach wurde der ungebetene Gast vom Systemmanager aus dem System herausgeworfen. Der Sysop unterbrach sämtliche Zuleitungen und verhinderte damit jeglichen Zugang zum Rechner. Der Hacker sei nun über einen anderen Rechner in das System eingedrungen und habe dem Systemmanager sämtliche Nutzungsrechte entzogen. Der Sysop hatte keine Möglichkeit mehr, auf sein System zuzugreifen.

Gegen 16.00 kristallisierte sich heraus, daß das BKA in sechs Orten der Bundesrepublik gleichzeitig eine konzertierte Aktion durchführte. Nach bisher vorliegenden Informationen sind dies:
1)6.00 - 11.30 eine Privatwohnung in Ellerbek (Kreis Pinneberg)
2) 6.15 - 17.00 eine Privatwohnung in Karlsruhe
-Betriebsräume der Universität Karlsruhe
-Privatwohnung der Eltern des Durchsuchten in Bad Bramstedt.
3) 6.30 - 18.00 Eine Privatwohnung in Hamburg-Harburg
-ebenfalls Betriebsräume des Arbeitgebers

Ergebnisse dieser Ermittlungen liegen derzeit noch nicht vor. Nach neuesten Informationen sind an den Durchsuchungen der Privatwohnung in Hamburg-Harburg auch drei Beamte der Deutschen Bundespost beteiligt. Sie interessieren sich für Verstöße gegen das Fernmeldeanlagengesetz.

Nachdem die Durchsuchungen gegen 12.00 dem diensthabenden Leiter der Hackerseelsorge bekannt wurden, sind erste Maßnahmen eingeleitet worden. Bereits gegen 12.30 stand ein Mitarbeiter von Radio Hamburg vor der Tür. Ein Durchsuchter gab erste Interviews. Auf die Stellungnahmen der anderen Durchsuchten wird noch gewartet. Laut Hackerseelsorge habe inzwischen fast jeder Hacker das Prädikat `staatlich geprüfter Hacker` erworben - eine Auszeichnung, die in der Szene einen hohen Stellenwert besitzt.

Bei der jüngsten Hausdurchsuchung in Hamburg wurde ein selbstgebauter Akkustikkoppler, rund 25 Spieledisketten sowie diverse Programmausdrucke beschlagnahmt. Ausserdem nahmen die Beamten die jüngste Ausgabe der CCC-eigenen Publikation Datenschleuder mit.

Mitglieder des Chaos Computer Clubs sind angesichts der jüngsten Durchsuchungen eher enttäuscht. Wie Vorstandsmitglied Steffen Wernery erklärte, wurde Wochen vor der Veröffentlichung des NASA-Hacks der Verfassungsschutz informiert, mit der Bitte, die

amerikanischen Geheimdienste über den schwerwiegenden Softwarefehler in Kenntnis zu setzen. Nach Angaben der Hacker wollte man mit dieser Informationspolitik auf vorhandene Sicherheitsrisiken aufmerksam machen. Nachdem sowohl die Digital Equipment Corporation (DEC) als betroffener System- und Netzhersteller als auch die betroffenen wissenschaftlichen Institute informiert waren, ging der Chaos Computer Club mit der Story an die Öffentlichkeit. Nachdem die Wogen der Erregung abflauten, stellten die Computerfreaks fest, das trotz ihrer Informationspolitik die Computer der NASA nach Wochen immer noch offen und die Sicherheitsmängel nicht beseitigt waren.

Wie Reinhard Schrutzki gegenüber der Presse erklärte, zeige der Vorfall, wie wenig man sich auf die Sicherheitsbehörden verlassen könne . Man habe sich wirklich bemüht, eine Schadensbegrenzung einzuleiten. Jetzt wird man vom BKA verfolgt. Schrutzki: `Wer wirklich als Betroffener von Computerkriminalität auf die Hilfe der Polizeibehörden angewiesen ist, der hat schlechte Karten.

CLINCH / CRD 19880301 1903

Bestellfetzchen 01/88

Die Datenschleuder (@ 8 Ausgaben)

Sozialabo für Schüler pipapo	DM	30.00
Standardabo	DM	60.00
Förderabo ab	DM	120.00

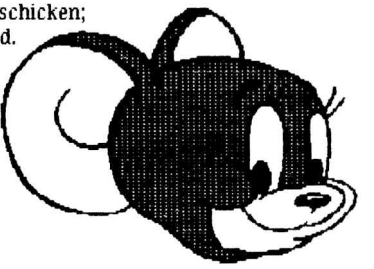
Mitgliedschaft im CCC e.V. für 1 Jahr		
Aufnahme-/Verwaltungsgebühr	DM	20.00
Schüler, Studenten etc	DM	60.00
Otto-Normaluser	DM	120.00
Fördermitglieder ab	DM	240.00

Die Hackerbibel Teil 1	DM	33.33
Parlacom - Studie	DM	7.50
Der elektronische Kammerjäger	DM	10.00

Aufkleber `Kabelsalat ist gesund`,
Superluxussonderausführung mit
unbeschränkter Haftung 3 Stück-Set
DM 5.00

Summe DM


```
program Personenbogen;
uses CCC;
begin
readln(stift,Vorname);
readln(stift,Name);
readln(stift,Strasse );
readln(stift,Ort);
if neues Mitglied then begin
 readln(stift,Telefon);
 readln(stift,Geburtsdatum);
  repeat
   readln(stift, Zahlweise);
  until Zahlweise in [ bar v-scheck
überweisung ];
end;
repeat
 readln(stift, Zahlweise);
until Zahlweise in [ bar v-scheck
überweisung ];
bezahlen;
eintüten;
abschicken;
end.
```



Ess Di Ai

Lichtblitze zucken lautlos über dem Horizont von Capistrano. Hell aufleuchtend explodiert im selben Augenblick eine Rakete.

Ursache war der Lichtblitz einer chemisch gepumpten Wasserstoff-Flour Laserkanone. Licht ist zur Waffe geworden. Dies ist nicht Science Fiction einer fremden Welt, sondern Alltag der Bewohner des kalifornischen Badeortes San Juan Capistrano . *Seit 1977 werden hier Hochenergielaser in militärischen Geheimprojekten als Strahlenwaffen erforscht,* und das nicht erst seit Reagans SDI-Plänen. Für das US-Navy Projekt „Sea Lite", zur Strahlenverteidigung von atomgetriebenen Flugzeugträgern, testete die Firma TRW hier ihre chemischen Laser mit einer Leistung von mehr als zwei Megawatt. Im Jahre 1981 erprobten die USA den MIRACL (Mid-Infrared Advanced Chemical Laser). Dieser Laser hätte bei Leistungsteigerungen auf über zwanzig Megawatt die Potenz, sowjetische Atomraketen bereits in der Startphase über Distanzen von mehreren tausend Kilometern zu vernichten. Das Ziel ist der Erfolg des „Alpha"-Projekts. Den chemischen Laser samt Treibstoff (H,F), Optik und Steuerungsrechner so kompakt zu fertigen, daß er im Orbit stationiert werden kann. Das Projekt ist ein wesentliches Element der strategischen Verteidugungsinitiative Präsident Reagans.

Röntgenlaser und EMP

Die Fletcher-Studie des ehemaligen US-Weltraumchefs, James Fletcher, kam zu dem Ergebnis, daß neue Technologien verfügbar werden, die einen Kraftakt der USA zur Verwirklichung der Defensiv-Strategie rechtfertigen. Initiator dieser neuen Technologien ist der als Vater der Wasserstoffbombe geltende Physiker Dr. Edward Teller. Unter seiner Anleitung wird der Röntgenlaser entwickelt. Aus einer Höhe von 80 km über dem Erdboden soll der Röntgenlaser durch die Energie einer Atombombe gespeist, feindliche Raketen auf tausende Kilometer Entfernung zerstören. Die Atomexplosion des Lasers wird neunmal stärker sein als die Atombombe, welche auf Hiroshima fiel.

Eine Studie des Pentagon kritisiert hingegen die Bemühungen des US-Militärs, Waffen und Nachrichten-Elektronik vor dem gefürchteten elektromagnetischen Puls (EMP) zu schützen. Noch immer, so die Studie, könnten „einige Atomexplosionen" in großer Höhe gewaltige EMPs auslösen und das nachrichtentechnische Nervensystem zerstören. Die Bemühungen der Militärs die Informationstechnologien des C3I (Command-, Control-, Communication-Intelligence) vor dem Chaos-Faktor zu schützen, gelten den Wissenschaftlern schon wegen des „unzureichenden Verständnisses" des EMP-Phänomens als nicht aussichtsreich. Die biologischen Konsequenzen eines EMP sind ebenfalls noch unkalkulierbar.

Tellers nuklear gepumpter Röntgenlaser paßt somit nicht in ein Konzept wie SDI. Heinar Kipphardt charakterisiert Edward Teller „In der Sache J. Robert Oppenheimer" als einen Wissenschaftler der meint, „daß Entdeckungen weder gut noch böse sind, weder moralisch noch unmoralisch, sondern nur tatsächlich". Teller ist überzeugt, „daß sie erst dann politische Vernunft annehmen, wenn sie wirklich tief erschrecken. Erst wenn die Bomben so groß sind, daß sie alles vernichten können, werden sie das tun". Bertold Brecht wertet die Einstellungen von Wissenschaftlern mit den Worten seines Galilei: „Wer die Wahrheit nicht weiß, der ist bloß ein Dummkopf. Aber wer sie weiß und sie eine Lüge nennt, der ist ein Verbrecher. Wenn Wissenschaftler, eingeschüchtert durch selbstsüchtige Machthaber, sich damit begnügen, Wissen um des Wissens willen aufzuhäufen, kann die Wissenschaft zum Krüppel gemacht werden, und eure neuen Maschinen mögen nur neue Drangsale bedeuten. Ihr mögt mit der Zeit alles entdecken, was es zu entdecken gibt, und euer Fortschritt wird doch nur ein Fortschreiten von der Menscheit weg sein. Die Kluft zwischen euch und ihr kann eines Tages so groß werden, daß euer Jubelschrei über irgendeine neue Errungenschaft von einem universalen Entsetzensschrei beantwortet werden könnte."

S. Stahl

Keine Chance für Hacker (hche)

VAX-Encryption

Als in den ersten Januar Tagen der neue Software-Katalog von DIGITAL Equipment Corporation (DEC) in die Briefkästen der Kunden flatterte, bot sich auch das Software-Produkt VAX-Encryption zum Erwerb an. VAX-Encryption ist ein Software-Tool für die Verschlüsselung von Dateien zum Schutz gegen unerwünschtes Lesen.

VAX/VMS Encryption wurde nach den Empfehlungen der US-Normenbehörde National Bureau of Standards (NBS) entwickelt und erfüllt die Anforderungen des Data Encry ption Standard (DES). Die Verschlüsselung erfolgt nach dem ANSI DEA-1 Algorithmus auf der Grundlage der FIPS-46 Spezifikation des NBS. Neben dem Cipher Block Chain Mode DESCBC ist sowohl der Electronic Code Book Mode DESECB als auch der 8- Bit Cipher Feedback Mode DESCFB anwendbar.

Wünscht ein VAX/VMS Benutzer die Verschlüsselung einer Datei, so geschieht dies direkt aus der Digital Command Language (DCL). Zuerst wird einmal der Encryption Key value definiert:

```
$ ENCRYPT/CREATE-KEY KEYNAME "Key value"
```

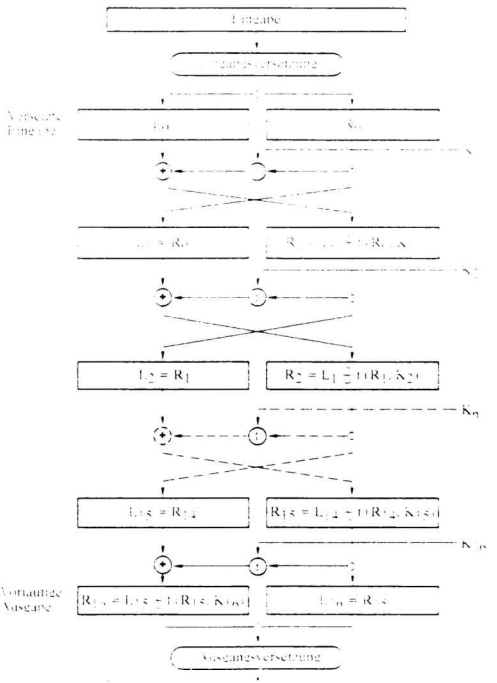
Der Key value ist das Codewort nachdem der Algorithmus die Datei verschlüsselt. Das Codewort sollte aus beliebig vielen Zahlen und Buchstaben bestehen, so z.B.:

```
$ ENCRYPT/CREATE-KEY GAGA "13 Affen haben
71 Bananen gern"
```

Encryption legt das Codewort wie folgt in der eigenen Proccess-Table ab:

```
ENCRYPT$KEY$GAGA = "Verschlüsselter Key
value"
```

Systemweite Codewörter werden durch den Zusatzparameter `/SYSTEM` in die SYSTEM-TABLE definiert und sind so für jeden Benutzer erreichbar.



Dieses erfordert jedoch das SYSNAM-Privileg. Durch den Parameter `/ALGORITHMUS=` können die verschiedenen oben erklärten Verschlüsselungsmodes gewählt werden. Die Standarteinstellung ist DESCBC. Dateien werden nun wir folgt verschlüsselt:

```
$ ENCRYPT FILENAME KEYNAME !Also so:

$ ENCRYPT FILENAME GAGA
```

Hierdurch werden die gesamten Inhalte der Datei sowie separat gespeicherte Zusatzinformationen wie Satzstruktur, ursprüngliches Erstellungsdatum und ursprünglicher Dateiname kodiert. Dies ist allerdings nur der Fall, wenn mit dem Parameter `/OUTPUT=FILENAME` die gleiche Datei mit der gleichen Versionsnummer angesprochen wird, ansonsten wird eine völlig neue Datei erzeugt. Die Dateiattribute werden ebenso wie die ursprünglichen Dateiinhalte bei der Entschlüsselung wiederhergestellt.

Abbildung rechts: Schema der Verschlüsselung beim DES-System. Dabei bedeutet L die linke Blockhälfte, R die rechte Blockhälfte, als K_1 bis K_{16} sind die sechzehn Unterschlüssel bezeichnet, die aus dem Gesamtschlüssel abgeleitet werden, der aus 56 Dualzeichen besteht. Die Abkürzung f deutet den Verrechnungsprozeß an. (Nach G. Herrmann »Datensicherheit durch Verschlüsselung«, IBM

```
$ DECRYPT FILENAME KEYNAME
```

Der Eintrag des verschlüsselten Keyvalues in die Proccess-Table wird durch dieses DCL Kommando gelöscht:

```
$ ENCRYPT/REMOVE-KEY KEYNAME
```

Zur Installierung dieses Software-Produkts werden folgende Dateien benötigt:

```
SYS$SHARE: ENCRYPSHR.EXE 85 BLOCKS;
SYS$SYSTEM: ENCRYPFAC.EXE 16 BLOCKS;
SYS$MANAGER:ENCRYPT-START.COM 3 BLOCKS;
```

sowie die VMS-HELP-Library ENCRYPT.HLP, welche in das VMS-HELP integriert wird.

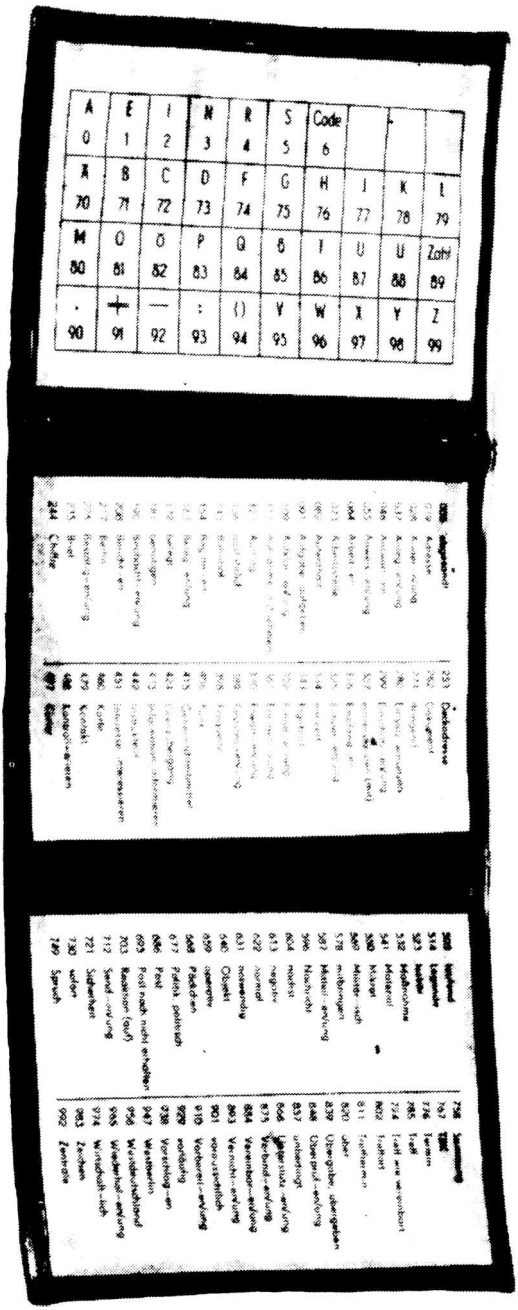
Bedauerlich an diesem faszinierenden Software-Tool ist jedoch die Tatsache, dass es für normal Sterbliche nicht zu haben ist. Schon die Preisliste des DEC-Katalogs verrät, daß dieses „Produkt nur im Rahmen von Projekten angeboten" wird.
Ein DEC-Vertreter bezog zu dieser Produktpolitik auf dem letzten DECUS-LUG Treffen in Hamburg Stellung: VAX-Encryption ist eine für das Militär gedachte Entwicklung, welche nicht in die Hände des Ostblocks fallen darf. Daher wacht der CIA über den Anwenderkreis dieses Tools. DEC ist verpflichtet nur Kunden mit ENCRYPT zu beliefern, die keine potentiellen Verbindungen in den Ostblock besitzen.

Ein weiterer Grund ist laut DEC-Vertreter die Gefahr, daß Hacker mit VAX-Encryption Unsinn treiben könnten und die Sicherheit von Systemen und Datenbeständen in Frage stellen würden.
Sicherlich ist die Verschlüsselung von Daten nur so sicher, wie die Aufbewahrung des geheimen Schlüssels sicher ist. Aufgefallen ist bei VAX-Encryption, daß das geheime Codewort zwar verschlüsselt in der Proccess-Table steht, jedoch auch in Klartext im Recall-Buffer zu finden ist. Für Hacker also kein Problem über den VMS SYSTEM-ANALYSER die Codewörter anderer Benutzer in Erfahrung zu bringen.
Sicherlich sollte DEC seinen Werbeslogan „Keine Chance für Hacker" nochmal überdenken.

S.Stahl

CLINCH/DS-RED/STAHL/28.01.88/11:38/4065 Z.

Im Zentrum der Spionage



Geheime Nachrichten-Technik

Im Kampf um die Information

Neu im Medienarchiv der DATENSCHLEUDER ist das „Handbuch für den privaten Nachrichten-Schutz". „Nachrichtenwaffen" prangt rot auf dem schwarzen Umschlag. Das Inhaltsverzeichnis weist mehrere Symbole für den Schwierigkeitsgrad auf. Schließlich sind außer allgemein verständlichen Verfahren wie zwei Seiten alltagstaugliche Geheimtintenauflistung und Postfallenbeschreibungen auch moderne mathematische Chiffrierverfahren erklärt.

Die Privatstudie mit © by Reb Harbinger von 1986 umfaßt gut 300 Seiten. Mengenmäßig wäre das – nur als Maß für die gegenwärtig verfügbare Datentechnologie, keine Bestellungen bitte, da nicht vorhanden – eine geschrumpft volle 720 Kilobyte-Diskette für die übliche kleine Tasche in Jacke oder Hemd (nicht auf die Daten setzen!).

Ein Einleitungs-Abschnitt: „Die USA"

Der erste Absatz wird jetzt unverändert zitiert, danach werden verschiedene Informationen aus der Studie assoziativ aktualisiert:
In den Vereinigten Staaten ist für die verschlüsselte Datenübertragung im „privaten" Bereich (z. B. für Banken) von Gesetz wegen das sog. „DES-System" (Data Encryption System) vorgeschrieben. Es wurde von der Firma IBM, ursprünglich unter der Bezeichnung „Lucifer", entwickelt.
Lucifer bezeichnet historisch den gefallenen Engel, der den Menschen das Licht (Erleuchtung?) brachte.
Die „National Security Agency" (NSA) – der größte technische Nachrichtendienst der westlichen Welt, über den LeserInnen der oben genannten Privatstudie im Selbstverlag weiteres erfahren können – hat die Annahme dieses Systems für den zivilen Sicherheitsgebrauch durchgesetzt. So geschehen, weil das „DES-System" noch unterhalb der Grenze der für die NSA überwindbaren liegt.
DES verschlüsselt mittels eines 64 Bit-Blocks und benutzt vom Schlüssel 56 Bit.
Auf dem Chaos Communication Congress Ende 1987 dienten übliche Domestos-Maschinen als Rechenknechte für das dort vorgeführte in der BRD entwickelte DES-Programm. DES wurde dort nur als sicher in Verbindung mit einem zusätzlich gesicherten als Public Domain erhältlichem Datenschrumpfprogramm erachtet.

Bezeichnenderweise wurde es zu DES-Planungszeiten IBM untersagt, einen Computer mit einer längeren und damit noch schwieriger zu überwindenden Schlüssellänge als 64 bit herzustellen (ein 128 bit Gerät lief im Versuch). Hätte IBM sich nicht an diese Auflage gehalten, der Export dieser Computer wäre untersagt worden, mit Hilfe der „ITAR"-Gesetze („International Traffic in Arms"), mit denen auch die Ausfuhr von Computertechnologie und Software geregelt wird.
Die Überlebensdauer von „DES" scheint abgelaufen, da Fachleute sie auch im kommerziellen Bereich mit fünf, höchstens acht Jahren angeben.
Vergleichsweise könnten schon entsprechend viele über Transputer europäischer Technologie verschaltete Heimcomputer von sonstwoher in den Gigaflop-Bereich dringen, der zu praktikabler DES-Analyse wohl benötigt würde.
In früheren Jahren wurden sogar Veröffentlichungen über Entwicklungen von „sicheren" Schlüsselsystemen – wie z. B. dem „Public Key", von Hellman und Diffie – nach dem Kriegsgeräte-Kontrollgesetz („Munition Control Act") zunächst von staatlicher Genehmigung abhängig gemacht. Inzwischen wurden diese Bestimmungen gelockert, so daß dieses System im Vertragsdruck in der BR Deutschland ausführlich behandelt werden kann.

Ein paar weitere Infos aus dem Werk

... Am 1. Juli 1948 gab der Nationale Sicherheitsrat der USA mit seiner „Intelligence Directive" (NSCID) die ersten Richtlinien für den gesamten Sicherheitsbereich heraus, in denen auch die Überwachung aller derjenigen europäischen Nachrichtenverbindungen festgelegt wurde, in denen sicherheitsrelevante Meldungen mit militärischem, politischem, wissenschaftlichem oder wirtschaftlichem Inhalt enthalten sein „könnten" („..which *may* concern information..").
... Durch die Unterschrift unter ein Codewort (einer muß es ja wissen) besiegelte am 24. Oktober 1952 ein amerikanischer Präsident die „Geburtsurkunde" der National Security Agency (NSA).
...Sämtliche „Ziele" der US Nachrichtenaufklärung sind aktuell in TEXTA, einer Art „Bibel", vernetzt

erfaßt.
...Lt. einiger hier zugänglicher Untersuchungen betreibt jedoch „die Sowjetunion heute die größte Nachrichten-Aufklärungs-Organisation der Welt".
...Seit Mitte der 70er Jahre sind brieftaschengroße Heimatfunkstellen im Einsatz, deren frequenzhüpfenden Signale in örtlichen Radiosendungen der Gegenseite verborgen (sub carrier) und wieder herausgefiltert werden konnten und umgekehrt via Satellit.
...In der BRD unterliegen Hersteller bei ihren Entwicklungen keinen Baubeschränkungen. Die Inlandsüberwachung von Nachrichtenverbindungen wird über die Einrichtungen bei den Knotenämtern der Deutschen Bundespost durchgeführt (siehe auch das Kapitel „Postkontrolle").
...In Österreich ist die Situation entspannter. Geräte zur Erzeugung von Schlüsseln der höchsten Sicherheit werden produziert.
...Die Schweiz stellt seit längerer Zeit Nachrichtenhöchstsicherungsgeräte her. Zu Zeiten des 2. Weltkrieges gab es nur in der Schweiz keine Beschränkungen für den Nachrichtenschutz. Bitte sich vorzustellen: Die DDR als Demokratie nach Schweizer Vorbild bis 1990.

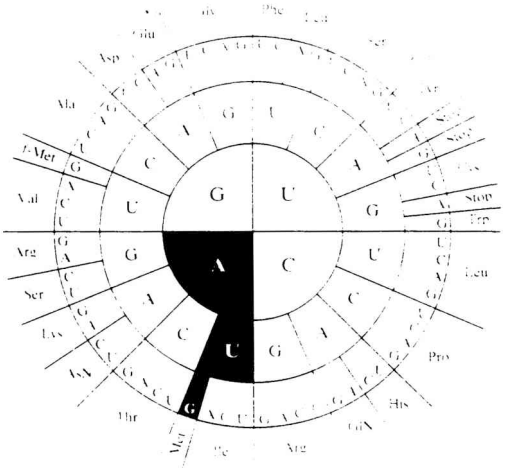
Verschlüsseln mit Zettel und Stift

Einen wichtigen Ausblick schildert der Autor: Schutzmaßnahmen im Privatbereich könnten so selbstverständlich wie das Verschließen eines Briefumschlages werden. Zu kurz kommt, daß für die neuen Datendienste fast jeder handelsübliche Computer entsprechende Sicherungsmöglichkeiten bietet.
Die verschiedensten Verschlüsselungsverfahren mit Zettel und Stift werden vorgestellt. Die meisten sind zwar gut beschrieben, aber recht kompliziert im Vergleich zu dem einfachen, im Buch „Im Zentrum der Spionage" (ISBN 3-7758-1141-9) abgebildeten Verfahren des MfS (DDR): die häufigen Buchstaben AEINRS werden durch eine einzige Ziffer (0..5) dargestellt, die 6 steht für Code. Drei Ziffern markieren einen Begriff der hundertstelligen Jargon-Liste und die anderen Zeichen werden durch zwei Ziffern dargestellt. Die Zahlenverteilung zwischen ein-, zwei- und dreistelligen Zahlen bei der Schlüsselvergabe sollte für Rauschen im Chi-Text sorgen (siehe Abbildungen).
Da die hundert häufigsten Wörter knapp die Hälfte eines Textes ausmachen und die häufigsten Buchstaben durch eine Ziffer dargestellt werden, verkürzt und verschlüsselt dieses Verfahren zugleich.
Das modernste in der Studie für privaten Nachrichtenschutz geschilderte teilautomatisierte Verfahren ist dagegen die Grundkonzeption eines Verschlüsselungsprogrammes mithilfe eines Taschenrechners ab Generation TI 57.
Ein PC oder HC mit Transputer dran und die Nutzung der Rechenkapazität zum Hufman-Coding oder der Schlüsselbildung aus vereinbarten Bitwürfelregionen von Mandelbrotzufällen u.a.m. fehlen.
Aber die veraltete Mikropunktherstellung wird erklärt.
Die vom Ostblock ausgeführte Mikrat-Kamera ist 25 mm kurz, 15 mm schmal und 5 mm flach. Die etwa 2 mm starke (Öl-)Linse verkleinert bis 1:1000. Dahinter die 15er Rundkassette. Das bringt gut beleuchtete Objekte etwa im Meterabstand auf den knapp mm-grossen schwarzen Punkt.
Hierzulande kann nach dem – fast traditionellen – ersten Schritt MINOX–Verkleinerung von 8„*11" auf 8*11 mm mit handelsüblicher Mikrofilmtechnologie (z. B. FUJI 850 Linien/mm) punktuell weiterverkleinert werden.
Zum Vergleich: Laserdrucker bieten derzeit theoretisch 12 Linien/mm (300 dpi); oft ist der Toner grober (der SLM804 ist fein). Die besprochene Privatstudie würde gerade noch lesbar im A6-Format auf 40 doppelseitig belaserte A4-Blätter passen.
Auch groschengrosser Mehrfach-Druck ist möglich.

Im Kapitel „Postüberwachung" schließlich...

...wird geschildert, wie es gemacht wird und was mensch dagegen tun kann.
Neben den Trocken-Naß-Dampf-Öffnungsverfahren wird auch das einfache Abziehen und Wiederaufkleben von als Postfalle aufgebrachten Klarsichtklebestreifen mittels Tetrachlorkohlenstoff (scheitert bei dehn/reißbarem Matt-Acetatband) beschrieben. Lehrreich sind geschilderte kleine Dienst-Pannen, wenn etwa im verposteten sorgfältig wiederverschlossenen Umschlag nur die Kontrollkopie lag und der Empfänger sich wunderte.
Die Studie beschließt mit dem heiklen Thema „Längstwellen". Gehirn-Manipulation vermittels langsam gepulster Funkwellen?
Der Leiter der Forschungsabteilung am Pettis Memorial Veterans Hospital in Kalifornien hatte Versuche mit einem aus der UdSSR stammenden „LIDA-Gerät" durchgeführt. In der UdSSR wurde schon seit Jahren das „LIDA-Gerät" zur „Ruhigstellung von Patienten, anstelle von Tranquilizern,

angewandt und dabei deren unerwünschte pharmakologische Nebenwirkung vermieden." Die gepulsten Radiowellen des „LIDA" regen die elektromagnetischen Gehirnströme an und rufen einen tranceähnlichen Zustand hervor. Lt. Gebrauchsanleitung wird das Gerät in der UdSSR „zur Beruhigung



bei Schlafstörungen und Spannungszuständen, sowie bei neurotischem Fehlverhalten" eingesetzt.
Über starke niedrigfrequente Impuls-Sender ließen sich nichtoperative Ferneingriffe in die Gehirnstruktur vornehmen („surrogate lobotomies at long distance"), um Gruppenverhalten zu beeinflussen.
Beschrieben werden hilfreiche Forschung und Nutzung der Erkenntnisse auf der einen Seite und gewarnt vor dem Mißbrauch „Geheimer Nachrichtentechnik", zum Nachteil der Freiheit der Menschen unserer Zeit.
In den vierseitigen Literaturhinweisen gibt es ausreichend Stoff für Neugierigere.

Die Studie für den privaten Nachrichtenschutz „Geheime Nachrichtentechnik" ist mit 80 DM für „normale" DV-AnwenderInnen nicht gerade billig, aber „Preis-Wert". Sollte sie im örtlichen DV-Kleinhandel nicht erhältlich sein: Sie wird vertrieben von Utilisation Est, PF 856, FL-9490 Vaduz und
beim Recon-Verlag, Postfach, 2000 Hamburg 73.

Wau 19.2.88 22:35

Einladung
an den Polizeipräsidenten

Hamburg (ccc) - Der Chaos Computer Club hat am 23. Dezember 1987 den Hamburger Polizeipräsidenten in einem Telex zum Congress eingeladen. Die Einladung im Wortlaut:

Sehr geehrter Herr Präsident,

wie Sie sicherlich aus der Presse erfahren haben, veranstaltet der Hamburger Chaos Computer Club e.V. auch in diesem Jahr seinen inzwischen traditionellen Chaos Communication Congress im Eidelstedter Bürgerhaus. Der Congress findet am 27. und 28. Dezember statt.
Im Mittelpunkt der diesjährigen Veranstaltung steht unter anderem eine Bewertung des sogenannten NASA-Hacks. Wir möchten Sie aus Anlaß des Kongresses zu einem persönlichen Gespräch einladen, in dem es Gelegenheit gibt, über die Probleme der Computertechnik in verschiedenen Bereichen zu sprechen. Wir gehen davon aus, daß ein solches Gespräch für alle Beteiligten von Interesse ist.

Für den Vorstand des Chaos Computer Club e.V., mit freundlichem Gruß

Reinhard Schrutzki

Geschenk-Abos gen Osten

Nachdem die HACKERBIBEL Teil 1 (das Erscheinen des zweiten Teils ist derzeit noch durch BKA-Fremdeinwirkungen behindert) schon seit Jahren in die DDR verschenkt werden darf, konnte der Verschenkdienst aktuell erweitert werden.
Jetzt können auch komplette DATENSCHLEUDER-Abos, bis Nummer xx sogar rückwirkend, formlos in die DDR verschenkt werden!
Einfach die DDR-Empfängeradresse, ab welcher Nummer der DS-Versand gewünscht wird und einen entsprechenden Scheck (8 Ausgaben DM yy) schicken. HACKERBIBEL DM 33,33 extra.
Auslandsaufschlag ist nicht erforderlich!

Modem-Workshop auf dem CCC 87

Entwicklung eines zulassungfähigen galvanisch gekoppelten Modems

Der CCC plant, eine Arbeitsgruppe ins Leben zu rufen, die im Lauf des ~~nächsten~~ Jahres bis zur engültigen Festlegung der Zulassungsbedingungen für teilnehmereigene Modems ein zulassungsfähiges, galvanisch gekoppeltes Modem entwickelt.

Galvanisch gekoppelt bedeutet, daß das Modem im Gegensatz zu einem Akustikkoppler elektrisch mit der Telefonleitung verbunden ist. Für dieses Modem soll eine Seriezulassung beantragt werden; die Finanzierung derselben soll eventuell eine Zeitschrift übernehmen. Das Modem soll (von selbiger Zeitschrift) als Bausatz ausgeliefert und dann zur Endkontrolle nach Hamburg geschickt werden. In Hamburg wird beim CCC getestet, ob das Modem der Serienzulassung entspricht, und mit dem FZZ-Aufkleber versehen. Die Käufer des Bausatzes sind also die „Fertigung"; der CCC übernimmt gegen geringe Gebühr lediglich die Endkontrolle.
In den nächsten Wochen soll geprüft werden, ob ein solches Vorgehen rechtlich möglich ist. Die Kosten für eine Serienzulassung liegen bei etwa 20.000 DM. Dieser Betrag müßte von einer Firma oder Zeitschrift aufgebracht werden, die dafür die Vertriebsrechte an den Modembausatz erhält.

Modemminimalversion

Die größten Probleme liegen bei der „Zulassungsfähigkeit" des Modems. Die Post wehrt sich mit Händen und Füßen gegen alles, was in dieser Richtung von privaten Anwendern unternommen wird. Die entgültigen Zulassungsbedingungen sind nicht bekannt, lediglich vorläufige Richtlinien sind verfügbar. Zunächst soll eine „Minimalversion" des Modems entwickelt werden, die möglichst wenige Streitpunkte, die bei der Zulassung entstehen könnten (Hayes-Befehlssatz etc), streift. Sie soll zum legalen, kostenkünstigen Betrieb einer Mailbox ausreichen.
Die Enwicklungszeit hängt im wesentlichen davon ab, wie schnell die rechtliche Lage und die Bedingungen für eine Zulassung vor dem Europäischen Gerichtshof und bei der Bundespost endgültig geklärt sind. *TRE/PKY*

Bitnapping Party V1.0

Die Ermittlungen gegen Art d'Ameublement und Teile der Bielefelder Scene sind abgeschlossen. Das Verfahren wurde eingestellt, die Kosten werden von der Staatskasse getragen. Schadensersatzforderungen wegen der Beschlagnahme (=Anwaltskosten) werden ebenfalls von der Staatskasse getragen. Quot erat - nochmal - quod erat expectaum!

CLINCH/CHAOS/PADELUUN/07.02.88/22:43/324 Z.

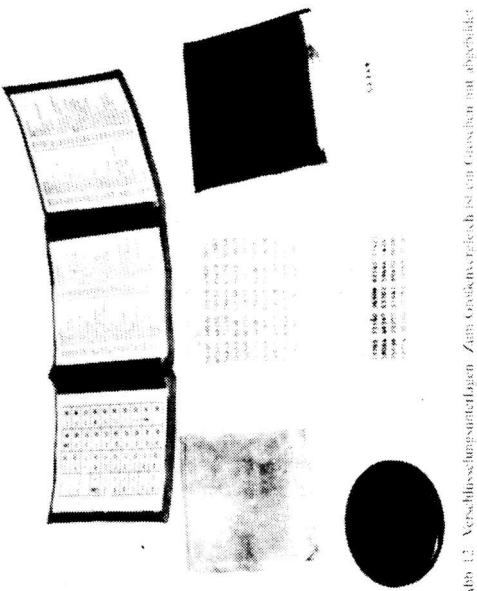


Abb. 12: Verschlüsselungsmethoden. Zum Glück ist ein Gerät mit abgebildet.

Kurzmeldung

Während des letzten Pariser „Salon du Livre" bildete sich eine Gruppe, die den Kampf gegen die Zensur aufnahm: „informel Renvoyons la censure". Das erste Bulletin mit Nachrichten aus der nicht nur französischen Welt gewisser großer Brüder:
Difpop, 14, rue de Nanteuil, F 75015 Paris.

EARN
oder das Erste Außerirdische Regional Netz

Vor einigen Wochen entdeckte ich, daß an meiner Universität ein Anschluß an EARN existiert. Ein Bekannter lieh mir sein Login samt Passwort und los ging es.

Als erstes stürzte ich mich auf das Terminal, eine Siemensanlage unter dem VM/CMS Betriebssystem. Nach dem Einloggen tippte ich erstmal SETUP NETZE um das Netz zu aktivieren. Ab da begannen die Schwierigkeiten. Mein erster Befehl, den ich an den EARN-Knoten absendete war /signup Vorname Nachname. Damit meldet man sich bei DEARN als Benutzer des InterChat an. Nach meinem Handbuch hätte jetzt die Meldung kommen müssen, daß man sich freut, mich bei InterChat begrüßen zu dürfen. Darauf seelisch eingestellt, war die Meldung 'You banned from this Relay' ein Schock. Unter Relay versteht man die einzelnen Knoten der Datennetze, die so aufgebaut sind wie EARN bzw. das US-Gegenstück BITNIC.
Nach Anfragen beim Operator bekam ich zu hören, daß ich wohl gegen die EARN-Richtlinien verstoßen habe. Mit diesem Aha-Erlebnis wurde ich bei dem Besitzer des Login vorstellig. Er war genau einmal bei EARN gewesen, und da hatte er nichts getan. Eine suspekte Angelegenheit. Glücklicherweise bekam ich zwei Tage später durch eine Vorlesung ein eigenes Login für die Siemens.
Ein weiterer Versuch, mich bei DEARN einzuloggen brachte den gewünschten Erfolg. Auch der nächste Befehl - /signon Nickname channel - klappte hervorragend. Dann brach das Chaos auf meinem Bildschirm aus. Irgendwie sah es aus, als würden hunderte von Leuten gleichzeitig in einer Mailbox miteinander reden. Nun, es waren etwa 30 Leute, die sich eingeloggt hatten.

Something about EARN

EARN ist ein europäisches Datennetz zum Austausch von Informationen und Programmen. Praktisch heißt das, man kann auf dem Netz direkt mit anderen Leuten chatten. Nicht nur mit Leuten, die sich bei EARN-Relays einloggen, sondern mit jedem, der sich an einem Relay einloggt, da zu anderen Netzen Querverbindungen existieren, weltweit etwa 1300. Neben Europa und USA auch Exoten wie Canada, Mexiko, Israel und Japan.
Allerdings ist das zu einem gewissen Maße Theorie, da die Netze eine nette Eigenschaft haben: Sie brechen gern zusammen. Zwischen den Relays liegen die Kabel bzw. Satellitenverbindungen, die allseits bekannten Links, und die beliebteste Fehlermeldung lautet 'Link Failure on xxxxx to yyyyy path' (Kurz LF). Wer einen EARN-Anschluss benutzen kann, sollte sich von EARN die Hilfsliste schicken lassen. Auf gut VM/CMS heißt das: 'Tell Relay at DEARN /help'.
Zum Beispiel kann man mit /who abfragen, wer sich gerade auf EARN aufhält. Diese Informationen sind sehr strukturiert. Jemand von 'TAUrelay' kommt aus Israel. Jemand von 'Germany' kommt aus Deutschland (oder auch nicht). Jemand mit der Meldung 'Geneva' kommt meistens aus Irland. Zum Reden stehen die 'Public Channels' zu Verfügung. Das sind die Kanäle 0 bis 99. Will man privater reden, wechselt man zu einem Kanal zwischen 100 und 999. Diese werden bei Abfragen von /who nicht angegeben. Es gibt noch die Kanäle zwischen 1000 und 9999. Aber die sind nur besonderen Leuten vorbehalten.

Die Anstandsregeln

Es gibt auch Richtlinien zur Benutzung von EARN:
- man darf nicht auf einen privaten Kanal wechseln, wenn dieser besetzt ist
- man darf keine Zeichensatz-Bilder schicken
- man darf nicht hart fluchen und schmutzige Witze erzählen
- man sollte Englisch reden
- man darf nicht hacken.

Es gibt noch andere Möglichkeiten auf EARN. Zum Beispiel kann man sich auch an andere Relays wenden. Man darf sich zwar nicht einloggen, aber man kann erfragen, wer sich dort so tummelt. Möchte man jemanden anchatten, kann man ihn dann über BITNIC/UNINET rufen. Dafür tippt man einfach 'Tell UserId at Standort'.
Auf diese Weise erreicht man auch Leute, die normalerweise nicht in EARN sind. Derzeit ist das z.B. die einzige Möglichkeit, das Wetter in Tokyo zu erfragen. Aber man kann natürlich auch Mailbox-ähnliche Systeme erreichen. Das bekannteste ist da wohl CSNEWS at MAINE. Dort kann man sich alles schicken lassen, von PD-Software bis zum Gedicht des Tages. Ein andere Box ist UH-INFO, mit den Subservern Arpanet und Atarinet.

Anfang Dezember '87 wurde der Deutsche Hauptknoten von Darmstadt nach Bonn verlegt. Außerdem wurde die Leitungen von 2400 Baud auf 9600 Baud erhöht. Nachdem DEARN wieder aktiv war, merkte man das sofort: Die LF kamen viel schneller.
Geschwindigkeit ist bei EARN so eine Sache. Man kann Glück haben, und die Anwort ist vor der Frage wieder da. Nachmittags dauert es 5 Minuten, bis man eine Antwort bekommt. Dafür hat man morgens ein reines Vorort-Gespräch. Nur Deutsche, Bayern und Holländer.

Der XMAS-Virus

In der zweiten Dezemberwoche kan es auf dem Relay zum ersten GAV (Größter Anzunehmender Vireneinsatz). An einem kalten Donnerstagmorgen

bekam ich ein File names XMAS. In meinem jugendlichen Leichtsinn startete ich es. Erst sah ich einen Weihnachtsbaum und dann zirka 30 Fileende-Befehle. Das Programm ging meine Namensliste (diese existiert auf allen VM/CMS Rechnern und kann erweitert werden) durch und sendete sich selbst an die Leute.

Es gibt zwei Möglichkeiten, mit XMAS umzugehen. Entweder man läßt ihn gewähren und hat dann eine formatierte Platte. Oder man drückt Reset, dann braucht man eine Stunde, bis man durch einen Operator wieder Zugang zu seinem Rechner hat. 24 Stunden später konnte man sich einloggen wo man wollte, egal ob Europa oder USA, alles redete über XMAS und wünschte dem Programmierer wenig Nettes. Die Variablennamen waren übrigens Deutsch.
In den folgenen Tagen mußte man das Relay in Ruhe lassen, da durch das ständige Übertragen von XMAS das Netz stark verlangsamt wurde. Interessant zu bemerken: Eine Warnung in die USA hat die Operatoren dazu veranlaßt, in die Header der Relay-Messages eine Warnug einzubauen. Eine Warnung an den Deutschen Operator brachte keine Reaktion.

Wer gEARN möchte

Der Zugang zu EARN wird in Deutschland ziemlich unterschiedlich gehandhabt. In Hannover und Hamburg wird dieser Zugang generell nicht erlaubt. In Heidelberg und Oldenburg kann jeder Student ans Netz. Sinnlos ist EARN sicher nicht. Man lernt Leute kennen und man bekommt Informationen. Wer allerdings auf billige Software hofft, hat keine Chance. Der normale Chatter ist ein Student der Naturwissenschaften ohne Computer. Sie kennen zum Teil nicht mal den Unterschied zwischen Bit und Byte. Aus manchen Universitäten und Instituten schalten sich zu mehr als 80% nur Mädchen zu. Komisch, wenn man bedenkt, wie selten diese an Computern zu finden sind.
Falls ihr mehr über EARN wissen wollt: Ich bin ganz einfach zu erreichen: Tell 98B030 at DOLUNI1 Text. Dann habt ihr mich meistens am Hörer. Es sei den ihr bekommt wieder ein LF on DHVRRZN1 to DOLUNI1 path. Dann habt ihr Pech gehabt.

Terra

TOPNEWS NEU! Digital UNTERHALTUNG

BKA unter Fahndungsdruck

CCC (Hamburg/Wiesbaden) - Über vier Monate sind vergangen, seitdem das Bundeskriminalamt (BKA), mit in der Bundesrepublik beispielosen nächtlichen Hausdurchsungen, die Jagd auf vermeintliche Hacker beim Hamburger Chaos Computer Club e.V. (CCC) eröffnete.

Mitte September trat der Club mit Informationen an die Öffentlichkeit, die ein eklatantes Sicherheitsloch in einem Großrechnerbetriebssystem der Firma Digital Equipment belegten. „Hacker" hatten sich an den Club gewandt, nachdem es ihnen gelang, in circa 135 Computersysteme des wissenschaftlichen Informationsnetzes der Luft- und Raumfahrt sowie der Hochenergiephysik einzudringen.
Mittels sogenannter „Trojanischer Pferde" untergruben sie die Sicherheitsroutinen und installierten unter anderem Programme, die die Kennworte aller Nutzer auskundschafteten. Betroffen von diesem „Hack" waren neben der amerikanischen Raumfahrbehörde NASA führende Institute im neun westlichen Ländern.

Raubkopien auf Großrechnern

Bei der durch den Club sofort nach Bekanntwerden eingeleiteten „Schadensbegrenzung" wurde neben dem Hersteller auch der amerikanische Geheimdienst CIA informiert. Man wollte, so ein Clubsprecher, vermeiden, daß der Club sich aufgrund der Brisanz der betroffenen Systeme zum Spielball der Geheimdienste entwickelt. So war es selbstverständlich, daß vor einer Veröffentlichung die betroffenen Systeme wieder „gesichert" werden mußten.
Beim Vergleich der von den „Hackern" angefertigten Liste der betroffenen Computer mit der Liste des Herstellers ergaben sich jedoch zahlreiche Unstimmigkeiten. So wurden an führenden Forschungseinrichtungen, auch im Bundesgebiet, auf dem second hand Markt erworbene Großrechner ohne Lizenz betrieben. Gemeinhin wird soetwas als „Raubkopie" bezeichnet.
Als Folge der Veröffentlichung dieses „Hacks" besannen sich die Wiesbadener Polizeispezialisten einer Anzeige der französichen Niederlassung der Philips AG. Diese hatte im Herbst 1986 - nachdem der Gesetztgeber in der Bundesrepublick das Ausspähen und Verändern von Daten unter Strafe stellte - Anzeige erstattet. Nach Angaben von Philips waren Hacker in die Fertigungssteürung eingedrungen.

Die Ermittlungen der französischen Behörden führten in die Schweiz zum Genfer Kernforschungszentrum CERN. Dieses beklagt schon seit 1984 ständig Einbrüche durch Hacker. Unter den Hackern selbst gilt CERN als die „Europäische Hackerfahrschule" in der sich die Hacker „die Klinke in die Hand geben". Die schweizer Systemspezialisten äußerten den Ermittlungsbehörden gegenüber den Verdacht, daß der Hamburger Chaos Computer Club Verursacher dieser Einbrüche sei.
So erwirkte die Staatsanwaltschaft, einen Tag nach Veröffentlichung des Nasa-Hacks, die ersten Durchsuchungsbeschlüsse. Inzwischen wird gegen sieben „Computerfreaks" aus dem Umfeld des CCC, inzwischen auch wegen des publiziertem NASA-Hacks, ermittelt. Begleitet wurden die Ermittlungen durch ebensoviele Hausdurchsuchungen, bei denen umfangreiches Material sichergestellt wurde.

MegaChip
NETWORKING

Hart getroffen wurden durch die Ermittlungen die beiden Vorstandsmitglieder des Clubs. Beide sind auch journalistisch tätig. Steffen Wernery unterhält seit 1984 einen Informationsdienst im Bildschirmtextsystem der Post. Bei den Durchsuchungen wurde das Redaktionssystem sichergestellt, so daß der Dienst nicht mehr fortgeführt werden konnte. Zwei Monate allein benötigten die Spezialisten vom BKA, um eine Kopie der für die Fortführung des Dienstes benötigten Daten anzufertigen. Inzwischen sind auch Computerteile zurückgegeben worden. Dabei wurde festgestellt, daß die Ermittlungen durch unsachgemäßen Umgang mit den Gerätschaften und einem daraus resultierenden Geräteschaden verzögert wurden.

hoffnungslose Bestrebungen

Seit der letzten Durchsuchung sind knapp vier Monate vergangen. Bis zum heutigem Tage wird den Anwälten der Beschuldigten die Akteneinsicht verwehrt. Das BKA und die Staatsanwaltschaft tun sich

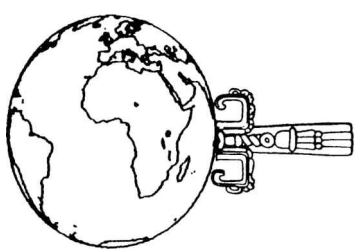
schwer Licht in das Dunkel dieses Falles zu bringen. Mag auch das sichergestellte Material an Umfang zwar zugenommen haben, so scheinen die Spezialisten vom BKA nicht in der Lage zu sein ihre Vorwürfe zu präzisieren und zu belegen.

Die Hoffnungslosigkeit der Bestrebungen des BKA wird ersichtlich wenn man Hintergründe eines weiteren Verfahrens miteinbezieht. So wird gegen den Pressesprecher des Clubs, welcher nach internen Informationen einer der Hauptverdächtigen sein soll, seit eineinhalb Jahren wegen des Verdachts auf Verstoß gegen das Fernmeldeanlagengesetz ermittelt. Normalerweise werden geringfügige Verstöße, bei gleichzeitig erhobenen schwereren Vorwürfen, eingestellt. So jedoch nicht in diesem Fall. Denn in der Ermittlungsakte findet sich ein Vermerk, daß eine Anklage oder Verurteilung in den Ermittlungen des BKA kaum zu erwarten sei. So ist es zu erklären, daß die Hamburger Staatsanwaltschaft zunächst das geringfügige Verfahren weiterverfolgt.

Doch mit einer baldigen Einstellung des Hackerfalles ist nicht zu rechnen. So ist zu vermuten, daß gerade die französichen Ermittlungsbehörden die Deutschen kräftig unter Druck setzen, jetzt endlich einen mutmaßlichen Täter zu präsentieren und zu überführen. Der Fahndungsdruck wird weiter erhöht - Insider bezweifeln allerdings den Erfolg.

So stellten schon die Hamburger Hacker fest: Der Gesetzgeber hat es versäumt, mit Einführung der Straftatbestände auch für die nötige Ausbildung der Ermittlungsbehörden zu sorgen. So fehlt es dem BKA an Kompetenz und Augenmaß in dieser Sache. Eine Chance, so die Hacker, der wirklich gefährlichen Computerkriminalität Herr zu werden, haben die Computerspezialisten des BKA vertan.

S.Wernery 062106 Feb 88 BEREICH RED BKA DRUCK CLINCH/DS-RED/S.WERNERY/07.02.88/15:51/5614 Z.



Modemanschluß

Die Modem-Anleitung sagt über den Anschluß nichts Wichtiges aus, sondern ist (wegen der USA-Normen) eher etwas konfus.

Es reicht aber der 2 Draht-Anschluß, wie er bei den meisten Hauptanschlüssen auch verwirklicht wird, jedenfalls bei den „alten" (neu heißt: Spezialstecker für ISDN, darüber weiß ich nix, dürfte aber nur neuer Stecker sein). Dort gehen aus der Wand 4 Drähte raus, entweder steckbar (4 Pin-Stecker) oder so, daß man einen Deckel abschrauben muß und (z.B.) ein 10-Meter-Kabel mit den Poststeckern (flach, rechteckig, durchsichtig) einfach angeschlossen werden kann. Wenn man sich den Stecker ansieht, sind dort nur 3 Kabel drin. Davon sind bei einer „normalen" Anlage (1 Hauptanschluß, keine Nebenstelle) nur 2 Kabel wirklich angeschlossen: die beiden, die direkt nebeneinander liegen. Nur diese beiden sind auch wirklich wichtig, das Modem erkennt Klingeln - das deutsche Besetztzeichen usw. erkennt es leider nicht. An dem Modem ist ein einfaches, 4-poliges Kabel. Es werden nur die rote und die grüne Leitung gebraucht, die anderen kann man abschneiden. Jetzt stellt sich die Frage, ob man immer umstecken will (oh wei!) oder umschalten oder alles (Teflon und Co.) immer dranlassen will. Das Modem hat noch einen zweiten Anschluß, an dem ein USA-Telefon (Stecker-Norm) so angeschlossen werden kann, daß immer, wenn das Modem aus ist, von dort aus telefoniert werden, und außerdem mit den Modem-Befehlen auf Telefon (Voice) und zurückgeschaltet werden kann. Dazu eignet sich gut ein ganz einfaches Telefon vom Conrad-Electronic-Grabbeltisch für ca. 20 DM (ohne den Stecker!).

Ich habe es etwas anders gemacht: Ich habe 2 Umschalter (2 pol & 1 pol) so mit dem ganzen Kram verlötet, daß ich entweder *nur Post* (2 pol!!) also normales Teflon dranhabe, oder Nicht Post, d.h. entweder Modem oder Ami-Phone (s.o. von Conrad), über den 1-poligen Umschalter, der andere Pol liegt bei Modem & Phone gleichzeitig an. In das Ami-Phone hab ich außerdem noch einen Schalter eingebaut, mit dem sich das Mikro ausschalten läßt. Dadurch, daß das das Ganze steckbar gemacht wurde (6 M-Kabel vom Conrad), ist die Chose höllisch schnell abbaubar: Wandsockel auf, Kabel raus, Gehäuse des Umschalters auf, Stecker (Original-Post-Teflon!) raus, diesen Stecker in den Wandsockel, Deckel anschrauben - fertig. Das 10 M-Kabel kann die Pest m.E. nicht messen, der Rest ist immer nur dran, wenns gebraucht wird. WABE

Legalize private Modems!

Im folgenden ein Artikel aus LA RAZON - (argentinische Tageszeitung, vor 76 Jahren gegründet, 3 Ausgaben täglich (?), eine der drei wichtigsten Zeitungen des Landes) - gefunden von Stefan Weirauch, übersetzt von Rena Tangens.

La Razon
Freitag, 25.September 1987

Interpol argentinischen Hackern auf der Spur

Laut Bericht von Alberto A. Antonucci, einem der Direktoren, wurde die Firma SISCOTEL S.A. (S.A. = Aktiengesellschaft), in unserem Land Eigentümerin von DELPHI - Anbieterin von Datenbank, Telekommunikation und anderer Dienste - wurde also seine Firma über einen Zeitraum von sechs Monaten Opfer einer Aktion von Hackern und dabei um einige zehntausend Dollar geschädigt. Mittlerweile sei Interpol eingeschaltet und die Untersuchungen weit fortgeschritten, da bereits die Empfänger der Plaudereien von Computer zu Computer entdeckt worden seien, die via Telefon und unter der Benutzung des geheimen Passwortes, das ENTEL (örtliche Telefongesellschaft) an DELPHI als Benutzer dieser Dienstleistungen vergeben hatte. „Die letzte Rechnung, die wir bekamen, belief sich auf über 10.000 US Dollar", bestätigte Antonucci, nachdem er die Praktiken der staatlichen Firma erläutert hatte.

Der Schakal

Andererseits kommentierte er den Artikel, der in einer anderen Tageszeitung erschienen war und in dem ein einheimischer Hacker porträtiert wurde, der auf den Decknamen 'Schakal' hört. Er berichtete, daß er und seine Kollegen im Besitz der persönlichen Passworte von vielen Benutzern von DELPHI seien und damit heimlich von allen Diensten Gebrauch machen könnten „und damit ahnungslosen Benutzern ungeheure Rechnungen aufbürden."
Antonuccis Widerspruch ist ganz grundsätzlich: „Lassen Sie uns bitte nicht in den Bereich von Science Fiction oder irgendeiner anderen Art von Aberglauben gehen. Dieser Typ Hacker, den einige Veröffentlichungen, nicht nur in unserem Land, entwerfen, existiert nicht. Wissenschaftlich gesehen kann er gar nicht existieren. Unser System hat zwei 'Eintrittskarten': der Name, den der Teilnehmer verwendet - das kann der richtige Name oder auch ein Deckname sein - und das Passwort. Das erste ist nicht schwierig zu ermitteln, da einer Benutzerliste existiert. Das zweite ist eine Kette oder eine Folge von Buchstaben und Zahlen zwischen 6 und 33 Stellen. Ein eingetragener Benutzer kann obendrein das Passwort alle fünf Minuten ändern, wenn es ihm paßt. Außerdem bricht DELPHI die Verbindung ab, wenn jemand es ausprobiert und das System dreimal hintereinander nicht das richtige Passwort erkennt. Wenn beim fünften Anruf, also dem fünfzehnten Versuch, nicht die richtige Kombination kommt - mathematisch gesehen gibt es Millionen möglicher Kombinationen - legt das System nicht nur auf, sondern sperrt auch gleich den Account und fordert den Benutzer zu einer Erklärung auf bzw. zeigt ihm an, daß irgendjemand versucht, einzudringen."

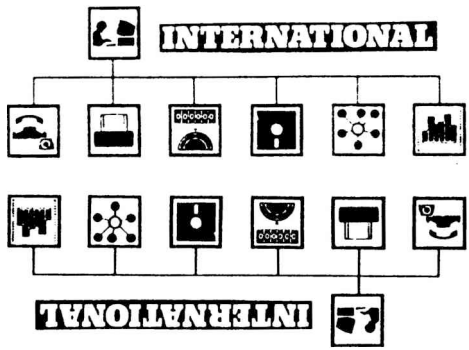
Zwei junge Deutsche aus Hamburg

Das Thema der Informationspiraten genannt 'Hacker' wurde sofort wieder aktuell, als vor einigen Tagen zwei junge Deutsche aus Hamburg einem deutschen Wochenmagazin ein Interview gaben und erzählten, daß sie, ebenfalls via Telefon, in das Telekommunikationsnetz der NASA, das insgesamt 135 Knotenrechner in Europa und Asien umfaßt, eingedrungen seien. Das nordamerikanische Unternehmen, ein japanisches und DIGITAL - eine der Firmen, die das größte Ansehen genießt in der Entwicklung von sicherer und leistungsfähiger Software für diese Art der Telekommunikation - haben das Eindringen bestätigt. „Seit Betriebsaufnahme von DELPHI haben wir hier vier Fälle gehabt", räumte Antonucci ein, „und bei allen gab es - unglücklicherweise für den jeweiligen Teilnehmer, glücklicherweise für uns - leicht zu entdeckende Fehler bei der Benutzung dieser Dienste. Wenn gesagt wird, daß das Passwort geheim ist, wollen wir damit sagen, daß es geheim sein *muß*, es darf nur einer wissen und sonst niemand."

unbegreifliche Rechnungen

Danach erzählte er LA RAZON, daß demgegenüber der Betrug, der jetzt entdeckt wurde, seinen Ursprung in einer Computer- und Telekommunikationsausstellung letzten Jahres hat, die jährlich in einem ruhigen

Hotel durchgeführt wird. „Wir brauchten eine spezielle Telefonleitung für unseren Messestand, um Dienste vorführen zu können, die DELPHI USA dort anbieten," erklärte Antonucci, „Dieser Telekommunikationsservice wurde uns im Mai eingerichtet und zwei Monate später hörten wir auf, ihn zu benutzen und die Ausstellung war beendet. Ab Dezember letzten Jahres und fortschreitend bis März diesen Jahres gab es dann einige unbegreifliche Rechnungen. An diesem Punkt erstatteten wir Anzeige. Zum Beispiel schien es so, als ob wir am 1. Januar dieses Jahres die Leitung nach Kanada von 11.30 h bis 15.00 h benutzt hätten. Aber von 12.00 h bis 14.00 h desselben Tages gab es eine andere



Verbindung von uns, und zwar mit der Schweiz und schließlich eine weitere ab 13.00 h bis 17.00 h mit einem anderen europäischen Land. Ganz offensichtlich sind Zuschauer während der Ausstellungen am Messestand gewesen, die die Fingerbewegungen des Vorführenden auf der Tastatur beobachtet haben, denn das Passwort ist nicht auf dem Bildschirm zu sehen, und haben auf diese Weise den Code herausgefunden. Auf der anderen Seite müssen wir zugeben, daß die Handhabung dieser Passworte nicht gerade vorbildlich war. Sie wurden einem Angestellten xy anvertraut, der sie daraufhin in einem Buch notierte, zu dem jeder andere Angestellte Zugang hatte; ein so wenig geheimer Dienstweg macht Passworte nutzlos. Der Typ 'Hacker', der die Informationen auf diese Weise ausfindig macht, existiert tatsächlich. Hingegen ist der Mythos vom Hacker, der die Passworte allein herausfindet und dem kein System widerstehen kann, sympathisch, aber mehr nicht. DELPHI zählt auch weiterhin auf die Technologie von DIGITAL, die eine der besten der Welt ist."

CLINCH/PADELUUN/PADELUUN/22.01.88/16:36/5754 Z.

Unglaublich aber wahr

Geschichten aus DATEX-P

Gut ein Jahr ist's her. Ich will anmerken, daß ich zum Zeitpunkt des Vorfalls im Vollbesitz meiner geistigen Kräfte war. Ich habe grade mal wieder 'ne Public Domain-NUI in die Hände bekommen und will mich mal 'n bißchen im DX umschauen. Zwei der frei belegbaren Funktionstasten meines Terminalprogrammes sind mit Teil A und B der NUI belegt, auf einer dritten habe ich die - wie sich später rausstellte fehlerhafte - NUA irgend eines britischen Rechners gelegt.

Ich klingle den PAD HH an, ein Ferngespräch. Ich wohne in der Provinz, eine Fangschaltung o.ä. ist damit wohl ausgeschlossen. Der PAD piept, ich lege den Teflonhörer in meinen wunderbaren postzugelassenen (!) Akustikkoppler, gebe das Dienstanforderungszeichen ein, der PAD meldet sich. Teil A und B meiner Tlkng werden akzeptiert, in froher Erwartung drücke ich auf meine dritte Funktionstaste. Der PAD antwortet mit "Kein Anschluß unter dieser Nummer" oder so.

Sekundenbruchteile später, ohne weitere Meldung, schickte der PAD die Zeile "Hallo Hacker!" auf meinen Bildschirm, gefolgt von einer nicht enden wollenden Sequenz aus BELs!! Bleich vor Schreck fiel ich fast von meinem Bürostuhl. Als ich mich Sekunden später wieder gefaßt hatte, hechtete ich in Richtung Teflon und drückte mit einem karateähnlichen Handkantenschlag auf die Gabel. Etwas später, als der Schreck verflogen war, rief ich den PAD noch mehrmals an, um den Vorfall zu reproduzieren. Ohne jeden Erfolg.

Der Vorfall liegt schon länger zurück. Hat vielleicht dennoch jemand irgend eine Erklärung? Neben der naheliegensten (Hallus etc.) fällt mir nur noch die sehr unwahrscheinliche ein, daß jemand mein Telefon angezapft und sich in die Leitung reingeschaltet haben könnte. Das würde ich zwar der Post und Komplizen sofort zutrauen - sie machen's ja auch des öfteren - nur würden sie sich nicht freiwillig derartig preisgeben. WAS IST DA BLOSS PASSIERT?

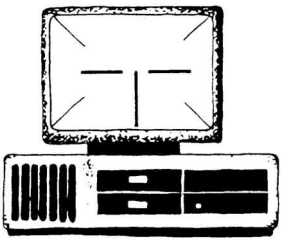
Ein mit DX befaßter befreundeter Postler erklärte mir übrigens, daß so etwas nicht möglich sei, beeilte sich aber hinzuzufügen, daß Unmöglichkeit kein Grund dafür sei, daß es nicht dennoch passiere. In DX sei allerhand Unmögliches möglich....

CLINCH/SYSOP/GAST/26.10.87/21:30/2885 Z.

Sicherheitsrisiken von Computersystemen

Hacker schleichen sich in Datensysteme ein

Hamburg (clinch) - In der Wissenschaft ist es längst üblich, Informationen elektronisch unter Angabe der richtigen Passwörter von Computer zu Computer zu verschicken. Besonders die Kernphysiker in Forschungszentren mit ihrem extrem hohen Datenaufkommen sind auf Computerkommunikation angewiesen.



Zudem lassen sich Daten und Programme an der einen Stelle aufbewahren und von außerhalb abrufen. Nur so ist die Zusammenarbeit über Grenzen hinweg möglich. Doch das dafür geschaffene Netz ist hackerfreundlich: Es wurde mit dem Ziel gegründet, wissenschaftlichen Einrichtungen den Zugang zu den Weltraumbehörden NASA (USA) und ESA (Europa) zu verschaffen. Das Rückgrat bildeten die DEC-Systeme (Digital Equipment) der NASA. Dabei wurde ein Computertyp eingesetzt, der unter Hackern besonders beliebt ist, weil er sich auf Billigcomputern besonders gut nachmachen läßt.

Und prompt ist es passiert

Im August dieses Jahres warnte Greg Chartrand, Computermanager des amerikanischen Kernforschungszentrums Fermilab in Batavia nahe Chicago seine Kollegen in aller Welt: „Hacker haben im Juli ihre Spuren in Europa hinterlassen und breiten sich nun in den USA aus". Und es waren deutsche Hacker, die mit „Trojanischen Pferden" Rechenzentrum um Rechenzentrum eroberten, besonders in der europäischen und amerikanischen Raumfahrtforschung. Betroffen sind Computer des Typs VAX der Fa. Digital Equipment (DEC). Die Hacker konnten jedes Programm und jede Datei eines angegriffenen Systems öffnen. Keine Sicherheitsschranke hielt sie auf. Der jüngste „Superhack", der zunächst nur stückweise bekannt wurde, gilt als der erfolgreichste seit der Existenz von Computern und übertrifft alle Befürchtungen der Experten. Zwar handelt es sich bloß, wie sich herausstellte, um den elektronischen Abfallkorb der NASA, in den man vorgedrungen war, aber immerhin.
Der Einsteig in das Netz der DEC-Anlagen war nach dpa verblüffend einfach. „Beim Spielen mit den Computern ohne böse Absicht waren die Hacker in ein Software-Loch gefallen", erklärte ein Sprecher des Hamburger Chaos Computer Clubs. Die Hacker meldeten sich mit dem bereits bekannten Passwort als Besucher beim Computer an und riefen die Liste mit den verschlüsselten Informationen über die Zugriffskontrolle auf. Das Ergebnis war - wie erwartet - eine Fehlermeldung. Diese wurde jedoch einfach ignoriert und die bereits offene Datei geändert. Die Hacker trugen sich ebenfalls in die Liste ein und gaben sich damit die Zugriffsrechte des Systemmanagers.

Wie inzwischen bekannt wurde...

...sind auch Teile des Computersystems der Deutschen Forschungs-und Versuchanstalt für Luft- und Raumfahrt (DFVLR) in Oberpfaffenhofen bei München betroffen. Es handelt sich dabei um Systeme des Typs VAX 4.4, 4.5, wie der Pressesprecher in der Kölner Zentrale auf Anfrage einräumte. 135 Einheiten dieser Art seien insgesamt in neun Ländern von Hackern „geknackt worden". Andere Programme wurden manipuliert, um sich „unsichtbar" zu machen. Auf dem Bildschirm und in den Ausdrucken erschien kein Hinweis auf die Eindringlinge. Wie einst die alten Griechen im Inneren eines hölzernen Pferdes in die belagerte Stadt Troja gelangt waren, so hatten sich jetzt die Hacker in fremden Computern eingenistet.

(aus: Polizeispiegel 11/87, S.245)

CLINCH/CHAOS/REDAKTION/26.01.88/11:49/3370 Z.

Grundlagen für den Einsatz neuer Technologien in den Geisteswissenschaften

Prof. Dr. Ekkehard Martens und Peter Matussek, Universität Hamburg, Arbeitsgruppe „Neue Technologien, Philosophie und Bildung"

Kurzdarstellung des Projekts einer „Hermeneutischen Interessen angepaßten Technologie" (HIAT)

Das Projekt HIAT stellt sich die Aufgabe, ein bisher ungenutztes Wirkungspotential neuer Technologien für die geisteswissenschaftliche Forschung zu erschließen.

Deren immer noch äußerst geringe Akzeptanz gegen den Einsatz computergestützter Hilfsmittel ist auf ein Akzeptabilitätsproblem zurückzuführen: Die verfügbaren Technologien werden den geisteswissenschaftlichen Forschungsinteressen grundsätzlich nicht gerecht. Sie sind auf die empirisch-erklärenden Verfahren der Naturwissenschaften zugeschnitten. Der hermeneutisch-verstehende Ansatz der Geisteswissenschaften aber setzt einer Formalisierung sowohl ihrer Inhalte als auch ihrer Arbeitsmethoden prinzipielle Grenzen.

Der geisteswissenschaftliche Arbeitsplatz von morgen

Die Anerkennung dieses paradigmatischen Gegensatzes muß und darf jedoch nicht in resignative Technikabstinenz münden. Vielmehr enthält er eine produktive Spannung, aus der technologische Lösungen für die geisteswissenschaftliche Forschung zu gewinnen sind.

Unter dieser Prämisse konzipiert das hier vorgestellte Projekt die Gestaltung des geisteswissenschaftlichen Arbeitsplatzes von morgen. Durch eine praxisorientierte Grundlagenforschung im interdisziplinären Dialog zwischen Geisteswissenschaftlern und Informatikern will es die zukunftsorientierten Anforderungen an neue Technologien im Sinne geisteswissenschaftlicher Problemstellungen formulieren und experimentell realisieren.

Als Pilotstudie soll eine Software mit Expertensystemfähigkeiten entwickelt werden, die drei Grundtypen hermeneutischen Arbeitens gerecht wird und sie forschungsintensivierend vereinigt: interpretative Phänomenkonstitution, sinnorientierte Recherche und praktische Darstellung. Diesen Vorgaben entspricht das zu konstruierende „Personal Indexing and Retrieval plus Editor" (P.I.R.E.).

P.I.R.E.

Es bietet dem Geisteswissenschaftler einen individuell angepaßten Zugriff auf eine Volltextdatenbank, der über drei kooperierende Anwenderprogramme für hermeneutisches Arbeiten zu nutzen ist: Der „Indexer" hilft bei der Ideenfindung und Problemformulierung durch eine interaktive Dialogführung und strukturiert entsprechend den Wissensbestand der Datenbank vor. Das Retrieval-System, der „Knowledge-Navigator", gestattet eine somit auf die jeweiligen Forschungsinteressen zugeschnittene Datenselektion. Der „Editor" ist ein Textverarbeitungsprogramm, das die Gestaltung und Konzeption auch nicht hierarchisch gegliederter Texte unterstützt, wobei es sich den jeweiligen Indizierungs- und Selektionspräferenzen „intelligent" anpaßt. Die drei Teilkomponenten arbeiten parallel im Multitasking-Verfahren, so daß z.B. der Schreibvorgang durch die Indizierungsdialoge unterstützt werden kann und der „Knowledge Navigator" jeweils adäquates Informationsmaterial bereitstellt.

Das Knowledge Engineering für das P.I.R.E. bedarf als Voraussetzung einer kriteriologischen Klärung hermeneutischer Arbeitstechniken. Sie soll durch wissenschafts- und medientheoretische Untersuchungen zur geisteswissenschaftlichen Methodologie erbracht werden. Ansätze für deren informationstechnische Umsetzung bieten neuere Trends der KI-Forschung, die das Design von Zugangssystemen nach dem (hermeneutischen) Modell offener Dialogstrukturen konzipieren.

Der Prototyp des P.I.R.E. ist schließlich in einer größeren Feldstudie zu forschungsrelevanten Problemstellungen daraufhin zu überprüfen, ob er den Kriterien von HIAT genügt und ggf. entsprechend zu modifizieren.

Ziel des Gesamtprojekts ist die Erarbeitung von Rahmenrichtlinien für die sinnvolle Verwendung neuer Technologien in den Geisteswissenschaften.

Wenn unzustellbar
Anschriftenausschnitt bitte
mit neuer Adresse zurück

Nasa-Hack

Daten raus umsonst und sofort!

Unverschämtheit! Der CCC fordert seit langem die ominöse „Freedom of Information". Anstatt mit gutem Beispiel voranzugehen, zockt er der (meistens armen) Hackerbasis einen Hunni für die Dokumentation des NASA-Hacks ab. Information also nur für die, die sich's leisten können (Presse, Bullen, VS etc.).

Damit keine Mißverständnisse aufkommen: Wir haben nichts dagegen, wenn Ihr versucht, eure Kosten wenigstens teilweise wieder reinzubekommen. NUR: zockt die Kohle gefälligst denen ab, die sie haben! Also z.B. DEC, den SPANNET-Betreibern, IBM, Gorbi oder sonstwem. Wir fordern also:

Sofort die gesamte Dokumentation des NASA-Hacks in einen öffentlich zugänglichen Teil der CLINCH-Mailbox!

Wer Freiheit der Information fordert und seiner eigenen Basis Kohle abnimmt, macht sich UNGLAUBWÜRDIG. Ihr denkt kommerzieller als die großen Kommunikationsdealer wie Bertelsmann. Im Übrigen: bildet euch nicht ein, von nichts und niemanden abhängig zu sein. Auch ihr seid auf die Kooperationsbereitschaft der „Szene" oder „Basis" angewiesen. Wenn ihr euch weiter so verhaltet, ist es Essig damit. *Daten raus, zack, zack!*

(für die CLINCH-Mailbox ist das Zeug wohl zuviel Müll auf einem Haufen, der Sätzer)

Die Bildschimschänder,
Sektion Passau

CCC'87/CCCONGRESS/CONGRESS/28.12.87/21:39/1184 Z.

Hallo Sysop,

Wir wollen gerene informationen tauschen. In die Niederlande gibt es ein hackverein, dass ihre mitglieder communicieren lasst durch ein bbs system in amsterdam. wir sind sehr interessiert was der CCC vom holländishe hacker weist, und wir wollen gern korrespondieren mit die CCC. verzeihe wen was ich schreibe nicht richtig Deutsch ist. Ich bin ja ein Hollender. Bitte schreibe an die holländische hacker, postfach 12894, 1100 AW Amsterdam. Die Niederlande.

Wir hoffen auf eine gute zusammenarbeit.

P.S: wir hacken diverse systeme und sind beschäftigt mit datex und phreaking. auch die sociale aspekten von computermisbrauch ist unseres thema.

CLINCH/SYSOP/GAST/18.01.88/20:44/651 Z.

Impressum	†
Die Das für	**Datenschleuder™** **wissenschaftliche Fachblatt** **Datenreisende**
Ein Organ des	©haos ©omputer ©lub e.V.
Nummer 25	Mærz 1988
Schwenckestraße 85	D-2000 Hamburg 20
Tel.:	(040) 490 37 57
f. Presse:	(040) 48 37 52
BTX:	*CHAOS#
Clinch / Geo1:	Chaos-Team
Herausgeber:	©haos ©omputer ©lub e.V.
ViSdP:	Reinhard Schrutzki
Mitarbeiter (u.a.):	DDT, A. Eichler, P. Franck,
Herwart Holland-Moritz,	JWI,H. Køpke, M. Kühn,
Andy M.-M., J. Nicolas,	Rudolf Schrutzki, padeluun,
Poetronic, S. Stahl,	S. Werněry.S. Weirauch
Nachdruck für bei Quellenangabe	nichtgewerbliche Zwecke erlaubt.
Layout &Grafik:	Streßtop Publishing
Satz:	**BuchMaschine**
Unterdruck	im Selbstverlach.